

# WELLNOMICS INFORMATION SECURITY POLICIES & PROCEDURES

## Contents

WELLNOMICS INFORMATION SECURITY POLICIES & PROCEDURES .....	21
Overview.....	21
Purpose.....	21
Scope .....	21
Policy elements.....	21
Actions .....	22
Roles .....	22
Requirements under this Policy .....	25
Policy Compliance.....	25
Management Approval .....	26
Definitions and Terms.....	26
Revision/Approval History.....	26
POLICIES .....	28
PRODUCT & SOFTWARE DEVELOPMENT - Policies .....	29
Secure Development Lifecycle (SDLC) - Policy.....	30
Related Standards, Policies and Processes .....	32
Revision History.....	33
Software Development Tools - Policy .....	34
Overview.....	34
Policy .....	34
Compliance Measurement.....	34
References .....	34
Related Standards, Policies and Processes .....	34
Revision History.....	34
Privacy Legislation & GDPR - Policy .....	36
Data Classification - Policy .....	37
Data Classification .....	37
Data Privacy.....	37
Data Confidentiality.....	38
Data Classification Examples.....	39
Application of data classification.....	39
Policy Compliance.....	40
Related Standards, Policies, Processes and Forms .....	40
Revision History.....	40
Product Security Risk Assessment Matrix - Policy .....	41
Unauthorized access to data or application functionality.....	41

- Loss of data or server/application functionality .....41
- Effort required for security breach .....42
- Considerations when evaluating security risks.....42
- Priority for addressing an issue.....42
- Resolution priority.....43
- Related Policies.....43
- Policy Compliance.....44
- Revision History.....44
- Third Party Components - Policy .....45
- Purpose.....45
- Policy.....45
- Maintain Inventory of 3rd party components.....45
- Perform Security Analysis.....45
- Keep 3rd party Components Up to Date .....45
- Maintain a security response process.....45
- Decision process for updating components .....45
- Policy Compliance.....46
- Compliance Measurement.....46
- Exceptions .....46
- Non-Compliance.....46
- Related Standards, Policies and Processes .....46
- Revision History.....46
- Product Threat Modeling - Policy .....48
- Requirements for updating threat models .....48
- Policy Compliance.....48
- Related Documents .....48
- Revision History.....48
- Static Analysis Security Testing (SAST) - Policy .....50
- Policy.....50
- Policy Compliance.....50
- Related Documents .....50
- Revision History.....51
- Dynamic Analysis Security Testing (DAST) - Policy .....52
- Policy.....52
- Policy Compliance.....52
- Related Documents .....52
- Revision History.....53

Security and Penetration Testing - Policy .....	54
Introduction.....	54
Policy for Security Testing of Client Apps .....	54
Policy for Penetration Testing of Server .....	54
Internal Penetration Testing .....	54
External Penetration Testing .....	54
Fixing vulnerabilities.....	55
Testing process & fixing failures or vulnerabilities found .....	55
Policy Compliance.....	55
Related Standards, Policies, Processes and Forms .....	55
Revision History.....	55
DEPLOYMENT & HOSTING - Policies.....	57
Customer Services Interactions - Policy.....	58
Introduction and Overview .....	58
General Principles.....	58
Proactive and Reactive Customer Interactions .....	58
The Day to Day Management of Support Tickets .....	59
The Handling of Support Tickets .....	59
Support Tickets – team approach.....	59
Destruction of Data Held on Equipment to be De-commissioned.....	60
Reporting and Recording of Incidents Relating to Customer Data .....	60
Review & Revision History.....	60
Management of Hosting - Policy.....	61
Overview.....	61
Purpose.....	61
Scope .....	61
Policy.....	61
General .....	61
Support.....	61
System upgrades .....	62
Backups .....	62
Roles Matrix and Permissions.....	62
Server patches & hardening.....	62
Operating system (Windows Server) .....	62
Notifications and Communication .....	63
Policy Compliance.....	63
Compliance Measurement.....	63

Exceptions.....	63
Non-Compliance.....	63
Related Standards, Policies and Processes.....	63
Definitions and Terms.....	63
Revision History.....	64
Receipt, Storage and Deletion of Customer Data - Policy .....	65
Overview.....	65
Purpose.....	65
Scope .....	65
Policy.....	65
Data Anonymization, Retention and Destruction .....	66
Destruction of Data Held on Equipment to be Commissioned.....	66
Termination of Contract.....	66
Policy Compliance.....	66
Compliance Measurement.....	66
Exceptions.....	67
Non-Compliance.....	67
Related Standards, Policies and Processes.....	67
Revision History.....	67
Access Security - Hosting - Policy.....	68
Overview.....	68
Purpose.....	68
Policy.....	68
Logical Security .....	68
Physical Security - Hosted servers (Microsoft controlled premises - Azure).....	69
Physical Security - Wellnomics access to Hosted servers.....	70
Compliance and Measurement .....	70
Exceptions.....	71
Non-Compliance.....	71
Related Standards, Policies and Processes.....	71
Revision History.....	71
Threat Modeling - Hosting - Policy .....	73
Requirements for updating threat models .....	73
Policy Compliance.....	73
Related Standards, Policies, Processes and Forms .....	73
Revision History.....	73
Disaster Recovery and Business Continuity - Hosting - Policy .....	75

Information Technology statement of intent.....	75
Recovery Objectives.....	75
Related documentation .....	75
Glossary.....	75
INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Policies .....	77
Risk Assessment - Internal - Policy.....	78
Overview.....	78
Purpose.....	78
Scope .....	78
Risk Assessment Policy .....	78
The Form .....	78
Guidance on the Completion of the Risk Assessment Form .....	78
The Risk Assessment Form .....	79
Related Standards, Policies and Processes.....	79
Revision History.....	79
Incident Management Process - Policy .....	81
Background .....	81
Scope .....	81
Policy.....	81
Definitions.....	81
Exclusions .....	82
Process .....	82
Investigation.....	82
Policy Compliance.....	83
Compliance Measurement.....	83
Exceptions.....	83
Non-Compliance.....	83
Related Standards, Policies and Processes.....	83
Revision History.....	84
Disaster Recovery and Business Continuity - Internal - Policy.....	85
Glossary.....	85
User Management - Employees & Contractors - Policy .....	87
Overview.....	87
Purpose.....	87
Scope .....	87
Policy.....	87
General Requirements .....	87

Policy Compliance.....	88
Compliance Measurement.....	88
Exceptions.....	88
Non-Compliance.....	88
The Authorization Matrix for User Access Rights to Internal and Hosted Systems	88
Roles Matrix and Permissions 1 - Wellnomics internal systems .....	89
Related Standards, Policies and Processes.....	89
Definitions and Terms.....	89
Revision History.....	89
Passwords and Encryption - Employees & Contractors - Policy .....	91
Overview.....	91
Purpose.....	91
Scope .....	91
Policy.....	91
Password Creation.....	91
Password Change.....	91
Password Protection.....	91
Password Storage.....	92
Application Development .....	92
Use of Passwords and Passphrases .....	92
Policy Compliance.....	92
Compliance Measurement.....	92
Exceptions.....	92
Non-Compliance.....	93
Related Standards, Policies and Processes.....	93
Definitions and Terms.....	93
Revision History.....	93
Access Security - Internal security, Employees & Contractors - Policy .....	94
Overview.....	94
Purpose.....	94
Policy.....	94
Logical security.....	94
Physical security - Wellnomics controlled premises.....	94
Policy Compliance.....	94
Compliance and Measurement .....	95
Exceptions.....	95
Non-Compliance.....	95

- Related Standards, Policies and Processes.....95
- Revision History.....95
- Clean Desk - Employees & Contractors - Policy.....97
  - Overview.....97
  - Purpose.....97
  - Scope.....97
  - Policy.....97
  - Policy Compliance.....97
    - Compliance Measurement.....97
    - Exceptions.....98
    - Non-Compliance.....98
- Related Standards, Policies and Processes.....98
- Definitions and Terms.....98
- Revision History.....98
- Equipment De-Commissioning - Policy.....99
  - Overview.....99
  - Purpose.....99
  - Scope.....99
  - Policy.....99
    - Technology Equipment Disposal.....99
  - Policy Compliance.....99
    - Compliance Measurement.....99
    - Exceptions.....100
    - Non-Compliance.....100
- Related Standards, Policies, Processes and Forms.....100
- Revision History.....100
- Firewall - Internal Security - Policy.....102
  - Update records.....102
  - Permitted sites, white lists etc.....102
  - Revision History.....102
- Mobile Devices - Employees & Contractors - Policy.....104
  - Overview.....104
  - Purpose.....104
  - Scope.....104
  - Policy.....104
  - Procedures.....104
  - Roles & Responsibilities.....105



- Removable media ..... 105
- Encryption..... 105
- Policy Compliance..... 105
  - Exceptions ..... 105
  - Non-Compliance..... 105
- Related Standards, Policies and Processes ..... 105
- Revision History..... 106
- Change Management - Internal Processes - Policy ..... 107
- Background, Definitions and Roles ..... 107
  - Definitions..... 107
  - Roles ..... 107
- Scope ..... 108
- Process ..... 108
- Documentation..... 108
- Policy Compliance..... 109
  - Compliance Measurement..... 109
  - Exceptions ..... 109
  - Non-Compliance..... 109
- Related Standards, Policies and Processes ..... 109
- Definitions and Terms..... 109
- Revision and Update History ..... 109
- Wireless Communication - Employees & Contractors - Policy ..... 111
- Overview..... 111
- Purpose..... 111
- Scope ..... 111
- Policy..... 111
- Policy Compliance..... 112
  - Compliance Measurement..... 112
  - Exceptions ..... 112
  - Non-Compliance..... 112
- Related Standards, Policies and Processes ..... 112
- Revision History..... 112
- Wireless Communication Standard ..... 114
- Overview..... 114
- Purpose..... 114
- Scope ..... 114
- Standard ..... 114

General Requirements .....	114
Home Wireless Device Requirements .....	114
Policy Compliance.....	115
Compliance Measurement.....	115
Exceptions .....	115
Non-Compliance.....	115
Related Standards, Policies and Processes.....	115
Definitions and Terms.....	115
Revision History.....	115
Anti-Bribery & Corruption - Employees & Contractors - Policy .....	117
Purpose.....	117
Policy statement .....	117
Scope .....	117
Who is covered by the policy? .....	117
Bribes .....	117
Gifts and hospitality.....	117
Facilitation payments and kickbacks.....	118
Political Contributions .....	118
Charitable contributions .....	118
Your responsibilities.....	119
Record-keeping .....	119
How to raise a concern.....	119
What to do if you are a victim of bribery or corruption.....	119
Protection.....	119
Training and communication .....	120
Who is responsible for the policy?.....	120
Policy Compliance.....	120
Compliance Measurement.....	120
Non-Compliance.....	120
Revision History.....	120
Ethics - Employees & Contractors - Policy .....	122
Overview.....	122
Purpose.....	122
Scope .....	122
Policy.....	122
Executive Commitment to Ethics .....	122
4.2 Employee Commitment to Ethics.....	122

Company Awareness .....	123
Maintaining Ethical Practices .....	123
Unethical Behavior.....	123
Policy Compliance.....	123
Compliance Measurement.....	123
Exceptions.....	123
Non-Compliance.....	123
Related Standards, Policies and Processes.....	123
Definitions and Terms.....	123
Revision History.....	123
Email - Employees & Contractors - Policy .....	125
Overview.....	125
Purpose.....	125
Scope .....	125
Policy.....	125
Policy Compliance.....	125
Compliance Measurement.....	125
Exceptions.....	126
Non-Compliance.....	126
Related Standards, Policies and Processes.....	126
Definitions and Terms.....	126
Revision History.....	126
Acceptable Use - Employees & Contractors - Policy .....	127
Overview.....	127
Purpose.....	127
Scope .....	127
Policy.....	127
General Use and Ownership .....	127
Security and Proprietary Information .....	128
Unacceptable Use.....	128
Policy Compliance.....	129
Related Standards, Policies and Processes.....	130
Definitions and Terms.....	130
Revision History.....	130
Remote Access - Employees & Contractors - Policy .....	131
Overview.....	131
Purpose.....	131

- Scope ..... 131
- Policy ..... 131
- Requirements..... 131
- Policy Compliance..... 131
  - Compliance Measurement..... 132
  - Exceptions ..... 132
  - Non-Compliance..... 132
- Related Standards, Policies and Processes ..... 132
- Revision History..... 132
- Home Working - Employees & Contractors - Policy ..... 134
  - Purpose..... 134
  - Introduction..... 134
  - Key Points ..... 134
- IT Requests - Employees & Contractors ..... 135
  - Overview ..... 135
  - Purpose..... 135
  - Scope ..... 135
  - Policy..... 135
  - Requirements..... 135
  - Policy Compliance..... 136
  - Exceptions ..... 136
  - Revision History..... 136
- DOCUMENTATION ..... 137
- PRODUCT & SOFTWARE DEVELOPMENT - Documentation ..... 138
- Software Development Life Cycle - Documentation ..... 139
  - Introduction and Background ..... 139
  - Development Change Management Processes..... 139
    - Definition of Ready..... 140
    - Definition of Done..... 140
    - Details on Software Development ..... 140
- QA and Testing..... 140
  - Security and penetration testing ..... 141
- Releases..... 141
- Policy Compliance..... 141
  - Exceptions ..... 142
  - Non-Compliance..... 142
- Related Standards, Policies and Processes and Documents..... 142

Revision history .....	142
Logging & Diagnostics - SaaS - Documentation .....	144
Introduction.....	144
Data privacy .....	144
Error logging.....	144
Trace logging .....	144
Audit logging .....	144
Protection against deletion .....	144
Customer access to audit logs.....	145
Revision History.....	145
Logging - App - Documentation .....	146
Revision history .....	146
Third Party Components - WorkPace Classic App - Documentation .....	147
Third Party Components - App - Documentation .....	149
Third Party Components - SaaS - Documentation .....	150
Data Privacy Compliance - Documentation .....	152
Data Privacy Requirements.....	152
Health and Safety legislation and employee consent .....	152
How the Wellnomics solution supports data privacy .....	153
Guidelines for using the Wellnomics solution in accordance with data privacy requirements	153
Inform staff.....	154
Identify roles for managers .....	154
OH&S staff.....	155
Access to computer use statistics .....	155
EU-U.S. Privacy Shield Framework .....	155
Using the Wellnomics solution across multiple countries.....	156
The Data Privacy Legislation.....	156
Disclaimer.....	156
Privacy Policy - Default - SaaS - Documentation.....	158
1. Information we collect .....	158
2. Legal bases for processing .....	159
3. Collection and use of information.....	159
4. International transfers of personal information.....	159
5. Your rights and controlling your personal information .....	159
6. Cookies.....	160
7. Limits of our policy .....	161
8. Changes to this policy .....	162

Product Security and Best Practice - SaaS - Guidelines.....	163
Security Guidelines.....	163
Security Training.....	163
Log on and Authentication methods.....	164
Password security.....	164
Secure connection to server.....	165
Access security to server and data - server security model.....	165
Security against attacks.....	165
Brute force attacks.....	165
Cross-site scripting.....	165
Database access security & data flow.....	165
User accounts.....	166
Penetration Testing.....	166
Policy Compliance.....	166
Related Standards, Policies, Processes and Forms.....	167
Revision History.....	167
Product Security and Best Practice - App - Guidelines.....	168
Security References.....	168
Guidelines and Best Practice.....	168
File security.....	168
Communication Security.....	169
Checking Revocation Status.....	171
Policy Compliance.....	171
Related Standards, Policies, Processes and Forms.....	171
Revision history.....	171
Access Security - SaaS - Documentation.....	172
Log on and Authentication methods.....	172
Secure connection to server.....	172
Access security to server and data - server security model.....	173
Password security.....	175
Setting and Resetting Passwords.....	175
Security against brute force attacks.....	175
Database access security & data flow.....	176
User accounts.....	176
Policy Compliance.....	177
Related Standards, Policies, Processes and Forms.....	177
Revision History.....	177

Threat Modelling - App - Documentation.....	178
Threat Model.....	178
Threat Analysis and Mitigation.....	178
Related Standards, Policies, Processes and Forms.....	190
Threat Modelling - SaaS - Documentation.....	191
Threat Model.....	191
Threat Analysis and Mitigation.....	191
Related Standards, Policies, Processes and Forms.....	199
Software Development Tools - Documentation.....	200
Related Standards, Policies and Processes.....	201
Revision History.....	201
Static Analysis Security Testing (SAST) - Guideline.....	202
Overview.....	202
Best Practice - zero warnings.....	202
Fix Guide.....	202
Related documents.....	202
Revision History.....	203
Dynamic Analysis Security Testing (DAST) - Guidelines.....	204
Overview.....	204
Test Environment.....	204
Fix Guide.....	204
Related documents.....	205
Revision History.....	205
App Security Testing - Guidelines.....	206
Revision History.....	206
SaaS Security and Penetration Testing - Guidelines.....	208
Selection criteria.....	208
Revision History.....	210
DEPLOYMENT & HOSTING - Documentation.....	211
Microsoft Azure Security and Compliance - Documentation.....	212
Revision History.....	212
Access Security - Hosting - Documentation.....	213
Overview.....	213
Service features.....	213
Threat Modeling - Hosting - Documentation.....	214
Threat Model.....	214
Threat Analysis and Mitigation.....	214

Related Standards, Policies, Processes and Forms .....	215
Service Level Agreement and Security Statement .....	216
Definitions.....	216
Availability of service target .....	216
Downtime.....	217
Server and data security .....	217
Performance and availability .....	217
Data redundancy and disaster recovery.....	218
Software updates .....	218
Support and issue resolution.....	219
Incident resolution and escalation process.....	219
Related standards, policies and processes .....	219
Revision history .....	219
SaaS Service Level Agreement - Uptime Monitoring - Guideline .....	221
Monitoring - Hosting - Guideline .....	222
Web server availability.....	222
Network responsiveness.....	222
Discrete number of network connections .....	222
Success/failure of scheduled processes .....	222
System check.....	222
Disaster Recovery and Business Continuity - Hosting - Guide .....	224
Objective.....	224
Contacts.....	224
Business Critical Systems.....	224
Scenarios.....	224
Scenario - Unresponsive Agent .....	224
Scenario - System Failure .....	225
Scenario - Data Failure .....	225
INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Documentation .....	226
Critical Events - Guidelines.....	227
Purpose.....	227
List of Appendices.....	227
Key Points .....	227
Planned Critical Events .....	227
Pandemic.....	227
Tsunami, flood, storm, tornado etc.....	228
Unplanned Critical Events.....	228



Procedure - Business Critical Issues .....	228
Procedure - Planned Event - Pandemic .....	229
<b>Health Monitoring</b> .....	229
Procedure - Planned Event or Unplanned Event – Natural or Other Disaster .....	230
FAQ's .....	232
Revision History.....	233
APPENDIX 1 .....	233
Planning for a Critical Event – Personal Information Form .....	233
APPENDIX 2a.....	234
APPENDIX 2b.....	235
APPENDIX 3.....	235
APPENDIX 4 .....	236
APPENDIX 5 .....	236
APPENDIX 6.....	238
APPENDIX 7 .....	239
Monitoring - Internal - Guideline .....	241
Website availability.....	241
Wellnomics Status.....	241
Website Terms & Conditions (not Hosting).....	242
1. Terms.....	242
2. Use License .....	242
3. Disclaimer .....	242
4. Limitations.....	242
5. Accuracy of materials.....	242
6. Links.....	242
7. Modifications.....	243
8. Governing Law .....	243
Passwords & Encryption - Employees & Contractors - Guidelines.....	244
Overview.....	244
Purpose.....	244
Scope .....	244
Statement of Guidelines.....	244
Policy Compliance.....	245
Compliance Measurement.....	245
Exceptions.....	245
Non-Compliance.....	245
Related Standards, Policies and Processes.....	245

- Definitions and Terms.....245
- Revision History.....245
- Building Security - Documentation .....247
- Disaster Recovery and Business Continuity - Internal - Guide.....248
  - Objective.....248
  - Contacts.....248
  - Business Critical Systems.....248
  - Scenarios.....248
  - Scenario - 1 Loss of main office .....248
  - Scenario - 2 Loss of Main server .....249
  - Scenario - 3 Loss of Critical VM .....249
  - Related.....249
- Security & Privacy Training - Employees & Contractors - Guideline .....250
- Employee Agreement & Contract - Example .....251
  - Main employment contract.....251
  - Conditions of Employment.....251
  - Deed of Confidentiality .....251
  - Revision History.....251
- Employee Position Description - Example .....253
- Position Description - Wellnomics Consultant - Support and Implementation .....253
  - Purpose.....253
  - Qualifications & Experience.....253
  - Person Specifications .....253
- Revision History.....258
- Disciplinary Procedures - Employees & Contractors - Guidelines .....259
- Revision History.....259
- INTERNAL ONLY.....260
- Business Continuity (& Disaster Recovery Plan) - Guideline.....261
  - Overview.....261
  - Purpose.....261
  - Key Points .....261
    - Administration .....261
    - IT / Product Development .....262
    - Sales & Support.....262
- Procedures .....262
  - Procedure 1 – Preventative and Contingency Precautions.....262
  - Procedure 2 – Short Term Disruptions (less than five business days).....262

Equipment Failure (non-Critical Event).....	262
Staff Unavailability.....	263
Related Documents .....	263
Management Approval .....	263
Revision/Approval History.....	263
Backup of Wellnomics Company Data - Guideline .....	265
General Description of Backup Processes .....	265
Internal Systems.....	266
Hosted Systems .....	266
Revision History.....	266
RESOURCES & TEMPLATES - Due Diligence Checklists, Templates and Training Resources .....	268
PRODUCT & SOFTWARE DEVELOPMENT - Templates & Resources.....	269
Third Party Components Review - Template.....	270
Guide to updating form.....	270
App Security Testing Record - Template .....	271
Penetration Testing Record - Template.....	273
Findings .....	273
Dynamic Analysis Security Testing (DAST) Record - Template .....	275
Findings .....	275
DEPLOYMENT & HOSTING - Templates & Resources.....	276
Disaster Recovery Report - Hosting - Template .....	277
Hardening Checklist - Windows Server OS - Template .....	281
Hardening Checklist - SQL Server - Template .....	285
Hardening Checklist - IIS Server - Template .....	286
Appendix: Summary Table .....	286
IIS 8/8.5 Server Hardening Glossary of Information.....	288
5 IIS Logging Recommendations .....	288
7 Transport Encryption.....	288
INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Templates & Resources	298
Employee Leaving Checklist - Template .....	299
Further actions if employee had support or IT Admin Access .....	299
Information Security Policy Acknowledgment and Agreement - Employees & Contractors - Template.....	301
Risk Assessment - Template.....	303
Application for Access to Non Anonymised Customer Data - Employees & Contractors - Template.....	307
Change Request Form - Internal - Template.....	308

Equipment De-Commissioning Form - Internal - Template .....	309
Disaster Recovery Report - Internal - Template.....	311
Incident Investigation Form - Internal - Template .....	315
COMPLETED RECORDS - EXTERNAL - Due Diligence Checklists & Templates	316
PRODUCT & SOFTWARE DEVELOPMENT - Records - External .....	317
Externally available records.....	317
Internal only records .....	317
Dynamic Application Security Testing (DAST) - Records Summary .....	318
Static Application Security Testing (SAST) - Records Summary .....	319
Independent Penetration Testing - Records .....	320
Independent Penetration Testing - Record - SaaS Version 4.12.0, August 2022	321
Independent Penetration Testing - Record - SaaS Version 4.5.0, July 2021 .....	323
Independent Penetration Testing - Record - WRM Version 3.4.5, May 2019 .....	325
DEPLOYMENT & HOSTING - Records - External .....	327
Externally available records.....	327
Internal only records .....	327
INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Records - External	328
Externally available records.....	328
Internal only records .....	328
Summary of COMPLETED RECORDS - INTERNAL - Due Diligence Checklists and Templates, etc .....	329

# WELLNOMICS INFORMATION SECURITY POLICIES & PROCEDURES

**Review frequency:** Annual

## Overview

Wellnomics is a software development company that develops ergonomics software. The software products developed and sold by Wellnomics are:-

- Wellnomics SaaS - a server based application utilizing a SQL database and a MS IIS web application user interface. Previously known as Wellnomics Risk Management.
- Wellnomics Client App - a desktop multi-platform application (support mobile OS's in the near future as well)
- Wellnomics WorkPace - legacy version of the Wellnomics Client App that will be phased out longer term

In addition to developing software Wellnomics also provides a hosting service for the Wellnomics SaaS . The servers used for hosting are provided by a hosting provider with whom Wellnomics Ltd has a service level agreement covering server provision, availability, maintenance, backup and security. Hosted servers, each hosting a varying number of customer and Wellnomics systems are located in the US, Ireland (for UK and EU) and Australia.

Only limited Wellnomics staff have access to Hosting servers and systems. No Wellnomics software development staff have access to any of these hosting servers or hosted systems and none of these servers is used for any development or testing processes

## Purpose

The purpose of this policy is to provide guidance and a framework for reference to the related data and systems security policies that exist in Wellnomics and to ensure that all relevant policies and procedures are adhered to and enforced in accordance with this policy (See Section 5 below). This policy is the "umbrella" policy under which all other policies are created, managed and referenced.

This policy sets out the general roles and responsibilities of Wellnomics staff pertaining to data and systems security and covers all aspects covered under terms such as:-

- data security
- system security
- data protection
- data privacy

## Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Wellnomics, including all personnel affiliated with third parties. It covers internal Wellnomics systems, interfaces to external systems and customer hosted systems.

This policy provides an over-arching policy document to the specific related policies and procedures set out in the relevant Section below.

## Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

## Actions

To exercise data protection and the protection of privacy Wellnomics Management and staff are committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyber attacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

## Roles

### Roles and Responsibilities For Policies and Procedures

Wellnomics Ltd has a variety of policies related to data and systems protection and privacy. To oversee the enforcement of, and adherence to these policies and procedures, Wellnomics has identified the following roles and appointed the following individuals to those roles:-

<b>Roles</b>	<b>Person Appointed</b>	<b>Appointment Effective from (Date)</b>
Privacy Officer 1	Kevin Taylor, CEO	January 2015
Privacy Officer 2	Wayne Owens, Principal Consultant	January 2015
Data Security Officer	Corinne Wright, Customer Success Manager	April 2021

Data Security Officer	Ian Bartram, Systems Administrator & Support Engineer	May 2021
-----------------------	---	----------

On behalf of Wellnomics Ltd:-

- The Privacy Officers have a responsibility to periodically remind staff of their responsibilities as they relate to data privacy and security and to record the fact that it has been done.
- The Data Security Officer (equates to Data protection Officer as it relates to GDPR requirements) is responsible for applying and auditing the conditions and procedures set out in the Wellnomics Information Security Policy

## Logical Access - Role Specific Responsibilities for Internal Wellnomics IT Infrastructure and Systems

With reference to internal IT systems, the individuals detailed below have Administrator access to the key infrastructure components, the maintenance of which are necessary for Wellnomics to function efficiently, securely and safely.

Infrastructure Area	Role	Person Appointed	Appointment Effective from (Date)
Internal File Server	Administrator	Ian Bartram, Systems Admin & Support Engineer	May 2021
		Feng Zhou, Software Engineer	September 2022
Firewall	Administrator	Ian Bartram, Systems Admin & Support Engineer	May 2021
		Feng Zhou, Software Engineer	September 2022
Routers and Switches	Administrator	Ian Bartram, Systems Admin & Support Engineer	May 2021
Wireless Networks	Administrator	Ian Bartram, Systems Admin & Support Engineer	May 2021
		Feng Zhou, Software Engineer	September 2022
Broadband ISP	Administrator	Kevin Taylor, CEO	September 2015
		Ian Bartram, Systems Admin & Support Engineer	May 2021
Domain Controller	Administrator	Ian Bartram, Systems Admin & Support Engineer	May 2021
		Feng Zhou, Software Engineer	September 2022
VPN Service	Administrator	Ian Bartram, Systems Admin & Support Engineer	May 2021
		Feng Zhou, Software Engineer	September 2022
Virus and Malware Signatures	Administrator	Ian Bartram, Systems Admin & Support Engineer	May 2021
Hosted server management dedicated workstation	Administrator and authorized users	Ian Bartram, Systems Admin & Support Engineer	May 2021
		Kevin Taylor, CEO	September 2015

For the purposes of this policy and day to day work, Wellnomics employees not listed above are deemed to be "end users" and as such do not have any elevated access or administration rights to any of the internal systems or to the network infrastructure

For the specific policies surrounding the access to customer hosted systems see document [Management of Hosting - Policy](#)

## Logical Access - Role Specific Responsibilities for Wellnomics Hosting of Wellnomics SaaS

The servers running the Wellnomics SaaS software are provided under contract by a hosting provider with servers located multiple regions. The services provided by the hosting provider are under the terms of a contract and associated Service Level Agreement and these cover safety and security of data along with data privacy. Notwithstanding the hosting providers responsibilities there are also specific responsibilities for Wellnomics Support staff whose role may give them direct access to customer data held in Wellnomics SaaS systems. In addition, Support staff may also be given access to customer data through support requests and in order to provide customer support e.g. emails containing user records, database backups etc. The requirements to anonymize data where possible is contained within the document [Receipt, Storage and Deletion of Customer Data - Policy](#) . The handling of such data should only be done by those roles set out in the document [User Management - Employees & Contractors - Policy](#)

## Individual Responsibilities

All Wellnomics staff have individual responsibilities for adherence to this policy and the related policies and procedures detailed in Section 5 above. Notwithstanding the specific provisions relating to these policies, staff also have general responsibilities contained within a number of documents including, but not limited to:-

- Conditions contained within Contracts with customers and related Service Level Agreements (SLAs)
- Obligations and responsibilities set out for all employees under various employment documents including Employment Contracts, Individual Employment Agreements (IEAs), Position Descriptions and related employment guidelines. Examples of these documents and related provisions can be found in [Employee Agreement & Contract - Example](#)
- Related Wellnomics Policies and Procedures - see relevant Section below

**Training** - from time to time and at least annually, Wellnomics Ltd undertakes to provide refresher and reminder training, to all staff, on the subject of data and systems security and privacy. Wellnomics staff undertake to attend such training whenever possible. A record of staff training, both general and specific (for specified roles) will be kept in [Security & Privacy Training - Employees & Contractors - Records](#)

## Application of the "4 Eyes Principle"

This policy and all related policies and procedures listed under Section 6 below will be subject to the "4 eyes principle". This means that :-

- All policies must be reviewed by at least 2 members of the Wellnomics Management Team prior to formal adoption
- The review of all ongoing policy adoption and the results of all policy enforcement exercises and resulting corrective actions will be carried out and agreed by at least 2 members of the Wellnomics Management Team
- Specific security sensitive tasks may require the attendance and/or agreement of 2 people before being carried out. Where this is the case it will be detailed in the specific policy to which it relates.
- The Change Management processes specifically utilize the "4 eyes Principle" as a control and moderating factor in determining the requirements for change within the Wellnomics organization. See - [Software Development Life Cycle - Documentation](#) and [Change Management - Internal Processes - Policy](#)

## Physical Security - General requirements

Unauthorized access to Wellnomics equipment, infrastructure and hosted sites is controlled through a number of physical controls including but not limited to:-

- A lockable and locked external security door
- a requirement for all visitors (non employees) to book into the building and to be accompanied by a member of staff at all times whilst in the building
- Lockable door so all offices (locked when not occupied)
- Locked and secure access to all sensitive network equipment including servers, routers, network switched, wireless access points, patch panels, power supplies etc. Keys to these areas are issued only issued to those individuals listed in 6.2, that require access to execute their responsibilities under this policy.



- Log-in lockout after 10 minutes of non use on all workstations and server terminals.
- Limiting the access to hosted servers through the use of "white listed" (by IP Address) dedicated workstations accessible only to individuals specified in [Management of Hosting - Policy](#)
- Role Based Access Control and Multi-Factor Authentication of approved Staff, restricting access to the hosted servers - see also [Management of Hosting - Policy](#)

## Requirements under this Policy

### Periodic Risk Assessment

This policy requires the Wellnomics Management team to carry out a periodic risk assessment of all Wellnomics data handling and infra-structure systems in order to identify areas of potential risk (to business operations and Wellnomics and customer data security and privacy, and to take steps to mitigate against any identified areas of risk.

The format of the risk assessment is set out in the document [Risk Assessment - Internal - Policy](#) . This document sets out the format of the required risk assessment along with guidance on its completion and the frequency with which it must be completed. Completed Risk Assessment Forms detailing follow up action will be stored under [Risk Assessments - Internal - Completed Records](#)

### Periodic Review and Updating of Associated Policies, Procedures and Guidelines

This umbrella document will be subject to review as and when required, but at least annually.

Legislation and other changes may impact this document or any of the policies made under it - it shall be the duty of the Chief Executive to ensure that any changes in legislation both locally and internationally (where applicable) are properly reflected. Where applicable, changes that may affect software licences, agreements or contracts, shall be communicated for consideration for relevant changes.

### Demonstration of Due Diligence

In order to satisfy interested 3rd parties that the policies and procedures under this document are fully active and subject to inspection, enforcement and corrective action, due diligence records will be kept detailing:-

- The policy that as been subject to inspection
- When the inspection was completed and the nature of the inspection
- Who carried out the inspection
- Observations resulting from the inspection
- Corrective action identified and completed, along with completion date or target date for completion
- Any required changes to existing policy and related procedures

## Policy Compliance

### Compliance Measurement

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

As a company Wellnomics Ltd reserves the right, where criminal activity in relation to a security incident is known or suspected, to report such an incident, or suspicion of such an incident to the relevant enforcement authorities. In the case of New Zealand, this would be to the local police. The Wellnomics CEO is the person responsibility for determining whether any behaviour, whether or not resulting in a breach of security, should be reported to the relevant enforcement authority.

Any security breaches that result in the loss or inadvertent (or deliberate) release of customer data to unauthorized parties shall be communicated to the relevant customer

### Exceptions

Any exception to the policy must be approved by the Wellnomics management team in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Management Approval

Originally approved by management on 6th December 2013. Subject to management approval on an annual basis. This approval covers this header policy and all policies and procedures made under this header policy.

## Definitions and Terms

None

## Revision/Approval History

Date of change	Responsible/Updated by	Summary of change	Date of Next Revision
6th December 2013	Wayne Owens, Principal Consultant	Updated and converted to new format.	December 2014
12th December 2014	Wayne Owens, Principal Consultant	Annual management re-approval	December 2015
9th January 2015	Wayne Owens, Principal Consultant	Updated to make reference to new policies that have been created and auctioned	January 2016
10th December 2015	Wayne Owens, Principal Consultant	Annual management re-approval	December 2016
3rd February 2016	Wayne Owens, Principal Consultant	Updated and Linked new policies and procedures under Section 5	February 2017
November 2016	Wayne Owens, Principal Consultant	Updated and linked new policies under Section 5, removed proposed ones from Section 6	15 Nov 2017 <a href="#">Wayne Owens (Unlicensed)</a>
6th December 2016	Wayne Owens, Principal Consultant	Annual management re-approval	December 2017
10th April 2017	Wayne Owens, Principal Consultant	Created new document <a href="#">User Management Policy</a> and transferred authorization matrix from this document to the new document	13 Apr 2018 <a href="#">Wayne Owens (Unlicensed)</a>
29 November 2017	Wayne Owens, Principal Consultant	Updated to reflect Tony Galbraith leaving permanent role and Chris Mackay starting + Annual Management approval from Kevin Taylor CEO	<a href="#">Chris MacKay (Deactivated)</a> 09 Feb 2018
13 Feb 2018	Chris Mackay	Updated and Linked new policies and procedures under Section 5	15 May 2018 <a href="#">Chris MacKay (Deactivated)</a>
4 Mar 2019	Kevin Taylor	Reviewed and combined contents of separate general Privacy Policy into this overarching document	<ul style="list-style-type: none"> <li>01 Jun 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>

13 Mar 2019	Wayne Owens	Edited for typos and consistency. No material changes	<ul style="list-style-type: none"> <li>19 Jun 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
11 Jun 2019	Chris Mackay	No changes required	<ul style="list-style-type: none"> <li>17 Sep 2019</li> </ul>
19 Sep 2019	Chris Mackay	No material changes required	<ul style="list-style-type: none"> <li>17 Dec 2019</li> </ul>
19 Mar 2020	Chris Mackay	No material changes required	<ul style="list-style-type: none"> <li>25 Jun 2020</li> </ul>
17 Aug 2020	Angeli Arino	Reviewed and updated	<ul style="list-style-type: none"> <li>17 Nov 2020 <a href="#">Angeli Arino (Deactivated)</a></li> </ul>
01 June 2021	Corinne Wright	Replaced Chris Mackay and Angeli Arino with Ian Bartram and Corinne Wright	<ul style="list-style-type: none"> <li>20 Dec 2021</li> </ul>
17 May 2022	Wayne Owens	Minor corrections to typos and previously numbered sections	<ul style="list-style-type: none"> <li>17 May 2023 <a href="#">Corinne Wright</a> <a href="#">Corinne</a></li> </ul>
28 Sep 2022	Corinne Wright	Replaced Mitchell Denton with Feng Zhou	<ul style="list-style-type: none"> <li>28 Sep 2023 <a href="#">Corinne</a></li> </ul>

**Notifications Record - All Staff Data Security and Privacy Requirements, Policies and Procedures and Related Training**

- 08 Jan 2014 - creation of this page notified to all staff
- 12 Feb 2014 - addition of revised document Data Security and Privacy Requirements, Policies and Procedures
- 16 Apr 2014 - addition of Role Specific responsibilities and matrix
- 17 Dec 2014 - Reminder note to all staff regarding responsibilities re data privacy and security. Updated Roles matrix and permission
- 26 Mar 2015 - Reminder note to all staff regarding responsibilities re data privacy and security. Updated Roles matrix and permission
- 15 Dec 2015 - Reminder note to all staff regarding responsibilities re data privacy and security. Updated Roles matrix and permission
- 07 Jun 2016 - Reminder note to all staff regarding responsibilities re data privacy and security. Updated Roles matrix and permission
- 07 Aug 2016 - Updated policies to reflect Robert Groenestein leaving Wellnomics
- 13 Nov 2017 - Updated to reflect Chris Mackays role and responsibilities
- 17 Aug 2020 - Updated to reflect Angeli Arino's roles and responsibilities
- 01 June 2021 - Updated to reflect Chris Mackay and Angeli Arion leaving Wellnomics and the addition of Corinne Wright and Ian Bartram

For all future notifications and training of staff - see [Staff Training Record - Data and Systems Security and Privacy](#)

For all reviews of authorization matrices see [Authorizations Review Record](#)

- Communicated informally

# POLICIES

- [PRODUCT & SOFTWARE DEVELOPMENT - Policies](#)
- [DEPLOYMENT & HOSTING - Policies](#)
- [INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Policies](#)

# PRODUCT & SOFTWARE DEVELOPMENT

## - Policies

- Secure Development Lifecycle (SDLC) - Policy
- Software Development Tools - Policy
- Privacy Legislation & GDPR - Policy
- Data Classification - Policy
- Product Security Risk Assessment Matrix - Policy
- Third Party Components - Policy
- Product Threat Modeling - Policy
- Static Analysis Security Testing (SAST) - Policy
- Dynamic Analysis Security Testing (DAST) - Policy
- Security and Penetration Testing - Policy

# Secure Development Lifecycle (SDLC) - Policy

**Review Period:** Annual

As part of Wellnomics **Information Security Policies & Procedures** we follow the **Microsoft Security Development Lifecycle** (see [MSDL](#)). This consists of a set of 12 practices shown below:



**Provide Training**  
Ensure everyone understands security best practices.



**Define Security Requirements**  
Continually update security requirements to reflect changes in functionality and to the regulatory and threat landscape.



**Define Metrics and Compliance Reporting**  
Identify the minimum acceptable levels of security quality and how engineering teams will be held



**Perform Threat Modeling**  
Use threat modeling to identify security vulnerabilities, determine risk, and identify mitigations.



**Establish Design Requirements**  
Define standard security features that all engineers should use.



**Define and Use Cryptography Standards**  
Ensure the right cryptographic solutions are used to protect data.



**Manage the Security Risk of Using Third-Party Components**  
Keep an inventory of third-party components and create a plan to evaluate reported vulnerabilities.



**Use Approved Tools**  
Define and publish a list of approved tools and their associated security checks.



**Perform Static Analysis Security Testing (SAST)**  
Analyze source code before compiling to validate the use of secure coding policies.



**Perform Dynamic Analysis Security Testing (DAST)**  
Perform run-time verification of fully compiled software to test security of fully integrated and running code.



**Perform Penetration Testing**  
Uncover potential vulnerabilities resulting from coding errors, system configuration faults, or other operational deployment weaknesses.



**Establish a Standard Incident Response Process**  
Prepare an Incident Response Plan to address new threats that can emerge over time.

Below is a high level overview of how Wellnomics implements each of these practices, together with links to the relevant practice policies, guidelines, documents and examples.

A full copy of Wellnomics current **Information Security Policies & Procedures** containing many of these documents can be provided on request.

	Practice	Wellnomics processes	Relevant Policies & Guidelines	Examples of completed processes
1	Provide Training	Wellnomics provides training on security to all staff, including specialized training on security best practices covering customer data, hosting and software development to technical support staff and development staff.  Refresher training is provided on a regular basis and training materials reviewed and updated regularly.	<ul style="list-style-type: none"> <li><a href="#">Security &amp; Privacy Training - Employees &amp; Contractors - Guideline</a></li> <li><a href="#">Information Security Policy Acknowledgment and Agreement - Employees &amp; Contractors - Template</a></li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Security &amp; Privacy Training - Employees &amp; Contractors - Records</a></li> </ul>

2	Define Security Requirements	<p>Wellnomics maintains a set of best practice coding guidelines that meet OWASP (<a href="#">Open Worldwide Application Security Project</a>) principles and as well as global legislative requirements regarding data sovereignty and data privacy.</p> <p>As a result of the above a range of features are implemented as standard in our products in order to maintain high security. For example, CAPTCHA, TLS 1.2, hashing and salting of all passwords, protection against brute force attacks, no default accounts, etc.</p> <p>Specific features are also built to meet data privacy requirements, such as data classification, data retention policies, data minimization, data access control, in country data residence.</p>	<ul style="list-style-type: none"> <li>• <a href="#">Product Security Risk Assessment Matrix - Policy</a></li> <li>• <a href="#">Product Threat Modeling - Policy</a></li> <li>• <a href="#">Product Security and Best Practice - SaaS - Guidelines</a></li> <li>• <a href="#">Product Security and Best Practice - App - Guidelines</a></li> <li>• <a href="#">Privacy Legislation &amp; GDPR - Policy</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">How Wellnomics solutions support full compliance with GDPR - A Detailed Analysis</a></li> </ul>
3	Define Metrics and Compliance Reporting	<p>Wellnomics has defined processes and criteria for evaluating, prioritizing, tracking and resolving potential or identified security risks.</p>	<ul style="list-style-type: none"> <li>• <a href="#">Product Security Risk Assessment Matrix - Policy</a></li> <li>• <a href="#">SaaS Security and Penetration Testing - Guidelines</a></li> <li>• <a href="#">App Security Testing - Guidelines</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">Product Security and Internal Penetration Testing - Records</a></li> </ul>
4	Perform Threat Modelling	<p>Wellnomics maintains up-to-date threat models for both the desktop Wellnomics App software, mobile Wellnomics App and SaaS solutions using the best practice Microsoft Threat Modelling Tool. The threat models are reviewed and updated regularly and all threats identified by the model are reviewed and assessed using a security evaluation metric and then actioned as appropriate, with all decisions and resolutions documented.</p>	<ul style="list-style-type: none"> <li>• <a href="#">Product Threat Modeling - Policy</a></li> </ul>	<ul style="list-style-type: none"> <li>• Refer "<b>Access security to server and data - server security model</b>" and "<b>Database access security &amp; data flow</b>" in <a href="#">Product Security and Best Practice - SaaS - Guidelines</a></li> <li>• <a href="#">Threat Modelling - SaaS - Documentation</a></li> <li>• <a href="#">Threat Modelling - App - Documentation</a></li> </ul>
5	Establish Design Requirements	<p>Wellnomics has established a set of security standards and security features that are required to be implemented in all Wellnomics products. This covers areas such as database encryption, internet communication, user authentication, data storage, etc.</p>	<ul style="list-style-type: none"> <li>• <a href="#">Product Security and Best Practice - SaaS - Guidelines</a></li> <li>• <a href="#">Product Security and Best Practice - App - Guidelines</a></li> <li>• <a href="#">Privacy Legislation &amp; GDPR - Policy</a></li> <li>• <a href="#">Data Classification - Policy</a></li> <li>• <a href="#">Data Privacy Compliance - Documentation</a></li> </ul>	
6	Define and Use Cryptography Standards	<p>Wellnomics products all use standard cryptography solutions and keep up to date with the latest standards, such as TLS 1.2 for all internet communication. Wellnomics follows <a href="#">Microsoft SDL Cryptographic Recommendations</a></p>	<ul style="list-style-type: none"> <li>• <a href="#">Product Security and Best Practice - SaaS - Guidelines</a></li> <li>• <a href="#">Product Security and Best Practice - App - Guidelines</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">Product Security Risk Assessment - SaaS (Sep 2020)</a></li> <li>• <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>

7	Manage the Security Risk of Using Third-Party Components	<p>Wellnomics maintains a list of all open source and 3rd party components used in desktop, mobile and SaaS applications. These are reviewed regularly to ensure they are up-to-date with respect to versions and security vulnerabilities.</p> <p>Regular Static Analysis Security Testing (SAST) and (Dynamic Analysis Security Testing) DAST is also performed to identify known security risks in 3rd party components. Any discovered vulnerabilities are then reviewed against the Product Security Risk Assessment Matrix Policy and resolved as required.</p>	<ul style="list-style-type: none"> <li>Third Party Components - Policy</li> <li>Third Party Components Review - Template</li> <li>Third Party Components - SaaS - Documentation</li> <li>Third Party Components - App - Documentation</li> </ul>	<ul style="list-style-type: none"> <li>Third Party Components Review - SaaS 4.14.0 (Nov 2022)</li> <li>Third Party Components Review - App 1.3.1 (Dec 2021)</li> </ul>
8	Use Approved Tools	Wellnomics uses only approved and industry standard development tools such as Microsoft Visual Studio and Qt	<ul style="list-style-type: none"> <li>Software Development Tools - Policy</li> </ul>	<ul style="list-style-type: none"> <li>Software Development Tools - Documentation</li> </ul>
9	Perform Static Analysis Security Testing (SAST)	Wellnomics uses static code analysis tools for desktop, mobile and SaaS applications as a standard part of our continuous integration. Any issues found are documented, reviewed against the Product Security Risk Assessment Matrix and then resolved before code can be committed.	<ul style="list-style-type: none"> <li>Static Analysis Security Testing (SAST) - Policy</li> <li>Static Analysis Security Testing (SAST) - Guideline</li> </ul>	<ul style="list-style-type: none"> <li>SAST Record - SaaS 4.15.0 (Jan 2023)</li> </ul>
10	Perform Dynamic Analysis Security Testing (DAST)	Wellnomics will use professional vulnerability scanning tools (such as Invicti/Netsparker) as a standard part of automated testing and every release must pass the Dynamic Analysis Security Testing successfully.	<ul style="list-style-type: none"> <li>Dynamic Analysis Security Testing (DAST) - Policy</li> <li>Dynamic Analysis Security Testing (DAST) - Guidelines</li> </ul>	<ul style="list-style-type: none"> <li>DAST Record - SaaS 4.14.0 (Nov 2022)</li> </ul>
11	Perform Penetration Testing	<p>Wellnomics uses both internal and external penetration testing for SaaS applications and internal security testing for desktop &amp; mobile Apps. This testing is designed to fully test products against all specified product security guidelines and test against all reasonable potential security vulnerabilities as specified in testing guides based upon industry standard best practice guides (such as OWASP)</p> <p>External penetration testing by a professionally qualified 3rd party provider is conducted regularly and reports on this testing are available to customers on request.</p>	<ul style="list-style-type: none"> <li>Security and Penetration Testing - Policy</li> <li>SaaS Security and Penetration Testing - Guidelines</li> <li>App Security Testing - Guidelines</li> <li>Penetration Testing Record - Template</li> <li>App Security Testing Record - Template</li> </ul>	<ul style="list-style-type: none"> <li>Penetration Testing - Independent - Records</li> <li>Security Testing - Record - WPC 5.5.5 (Nov 2020)</li> </ul>
12	Establish a Standard Incident Response Process	<p>Wellnomics has policies and processes for managing security incidents and for responding to other incidents reported by customers (e.g. server down) and taking action to resolve these.</p> <p>Wellnomics also maintains a 24/7 monitoring services on all SaaS applications to ensure up-time targets are met and provide escalation where needed. Customers can be provided with access to the live up-time monitoring and metrics for their hosting server on request.</p>	<ul style="list-style-type: none"> <li>Incident Management Process - Policy</li> <li>Customer Services Interactions - Policy</li> <li>Incident Investigation Form - Internal - Template</li> <li>Monitoring - Hosting - Guideline</li> <li>SaaS Service Level Agreement - Uptime Monitoring - Guideline</li> </ul>	

## Related Standards, Policies and Processes

- Software Development Life Cycle - Documentation



## Revision History

Date	Who	Summary	Next revision date
06 Nov 2020	<a href="#">Kevin</a>	Finished writing up based upon Microsoft SDLC	<ul style="list-style-type: none"><li>01 Nov 2021 <a href="#">Kevin</a></li></ul>
05 May 2022	<a href="#">Kevin</a>	Reviewed MS SDLC site and no changes to best practice.	<ul style="list-style-type: none"><li>05 May 2023 <a href="#">Kevin</a></li></ul>
17 Mar 2023	<a href="#">Kevin</a>	Updated descriptions and policy links prior to publishing a new version on website	<ul style="list-style-type: none"><li>01 Apr 2024 <a href="#">Kevin</a></li></ul>

# Software Development Tools - Policy

**Review period:** Annual

## Overview

Ensuring the use of consistent and high quality development tools helps ensure consistency and security of Wellnomics products.

## Policy

- Wellnomics will use industry standard development tools from well known vendors or tools that are well accepted and maintained by the industry (if open source tools are used).
- Tools should be maintained up-to-date ensuring we remain on the latest versions
- A balance should be maintained between upgrading to the latest versions in a timely manner (which can involve considerable rework sometimes due to incompatibilities between versions), and the urgency of upgrading in order to take advantage of improved security or vulnerability fixes in newer releases.
- Wellnomics will maintain a list of approved tools that are used for product development and the versions used.
- Wellnomics will maintain a list of the security checks available in such tools, such as compiler/linker options and warnings.
- If security features are available in tools Wellnomics development team members are expected to make use of these consistently.

## Compliance Measurement

At each annual review the current SDLC owner will verify that the [Software Development Tools - Documentation](#) has been reviewed recently and is up-to-date.

Jira will be used to track any required tools updates that have been identified.

## References

See below references for guide on selection of appropriate development tools and security analysis

- [Microsoft Recommended Tools, Compilers and Options for x86, x64 and ARM](#)

## Related Standards, Policies and Processes

- [Software Development Tools - Documentation](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
24 Aug 2020	<a href="#">Kevin</a>	Added policy based upon MS SLDC	<ul style="list-style-type: none"><li>• 24 Oct 2021 <a href="#">Ian Bartram</a></li></ul>
16 Dec 2021	<a href="#">Ian Bartram</a>	Reviewed, no changes needed	<ul style="list-style-type: none"><li>• 26 Jan 2023 <a href="#">Ian Bartram</a></li></ul>

26 Jan 2023	<a href="#">Ian Bartram</a>	Reviewed, no changes needed	<ul style="list-style-type: none"><li>• 16 Feb 2024 <a href="#">Ian Bartram</a></li></ul>
-------------	-----------------------------	-----------------------------	---

# Privacy Legislation & GDPR - Policy

## Review period: Annual

Wellnomics solutions are designed to comply with Privacy Legislation and Best Practice Privacy Guidelines in most countries. Specific reviews have been conducted of the following Privacy Legislation in the different countries:

- UK Data Protection Act 2018
- Australian Privacy Act 1998
- New Zealand Privacy Act 2020
- EU General Data Protection Regulations (GDPR) 2018

GDPR is generally regarded as the most stringent of these legislative requirements. This means that meeting GDPR means in almost all cases meeting the requirements for other privacy legislation.

For an analysis of the specific legal requirements of GDPR and their implications for the Wellnomics solution with regard to how data is collected, stored and accessed within the solution see [How Wellnomics solutions support full compliance with GDPR - A Detailed Analysis](#)

For a description of the features within the product that are designed to support Data Privacy Legislation see Wellnomics White Paper **Data privacy guidelines for using Wellnomics**

# Data Classification - Policy

**Review period:** Annual

This policy sets out the different classification levels for data sensitivity in Wellnomics products. These classifications are used to guide the security requirements and also user access levels. They also help guide compliance with Privacy Legislation such as the EU GDPR.

## Data Classification

### Data Privacy

It is firstly helpful to consider data classification from a data privacy point of view - as the requirements of privacy legislation are very prescriptive and legally binding. From this point of view we can consider four types of data.

Data Type	Description	Covered by Privacy Legislation
Personal Data	<p>The EU GDPR provides a useful definition of Personal data as</p> <p><i>Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</i></p>	Yes
Sensitive Personal Data	<p>Under the EU GDPR data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, <b>biometric data, data concerning health</b> or data concerning a natural person's sex life or sexual orientation is considered Sensitive Personal Data.</p> <p>Sensitive Personal Data has more restrictions on it's collection storage and usage than Personal Data. For example, it can never be collected without user permission (whereas normal Personal Data may be under the right circumstances).</p> <p>See <a href="https://www.burges-salmon.com/news-and-insight/legal-updates/gdpr-personal-data-and-sensitive-personal-data">https://www.burges-salmon.com/news-and-insight/legal-updates/gdpr-personal-data-and-sensitive-personal-data</a> for more on this.</p>	
Pseudonymized Data	<p>Pseudonymized data is data where parts that identify the user have been replaced with a number or text that doesn't identify the user, as 'pseudonym'. An obvious example of this is a GUID or a User ID as used in databases. Data can then be stored, viewed or transmitted in this form without identifying information such as name, email address or employee ID. However, pseudonymization is a reversible process as the GUID or User ID can still be used to link the data with the real person's identifying details if needed. Although access to this may be restricted.</p> <p>Pseudonymization provides a way to share data but reduce the chance of personal data being breached unintentionally. From the point of view of privacy legislation like the EU GDPR because the data can still ultimately be tied to an identifiable person its still considered personal data.</p> <p>Refer to <a href="https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/">https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/</a> for more details.</p>	Yes

<p>Anonymized Data</p>	<p>Refers to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable</p> <p>Effective data anonymization must be made up of two parts:</p> <ul style="list-style-type: none"> <li>• It is irreversible.</li> <li>• It is done in such a way that it is impossible (or extremely impractical) to identify the data subject.</li> </ul> <p>It should be noted that data anonymization is more difficult than it may at first appear. If you have a lot of data about someone (e.g. date of birth, sex, education level, salary, address, company they work out, etc) then it may require relatively little effort for someone to deduce the identities of the people and thus 'reverse' the anonymization. For this reason, simply removing someone's unique identifiers (email address, employee ID, name, social security number) may not actually be enough to anonymize the data.</p> <p>Refer to <a href="https://gdpr.eu/data-anonymization-taxa-4x35/">https://gdpr.eu/data-anonymization-taxa-4x35/</a> for more information</p>	<p>No</p>
<p>Group Anonymized Data</p>	<p>Group data is a form of Pseudonymization that is achieved by aggregating data from a group of people. For example, taking averages, or maximum and minimums. The group might be all staff belonging to an Organization, or a Department, Site or Region.</p> <p>Note that aggregating data doesn't necessarily stop it being personal data. For example, if the group has just a few people (in minimum case a group containing just 1 user) then if you know which people belong to the group you effectively still know information about those users.</p> <p>For this reason there must generally be a minimum group size (e.g. 10 people) to provide a level of 'anonymization'.</p> <p>Note also that if the group is defined by some criteria (e.g. all users who are high risk, or who have reported discomfort) then simply knowing which people are members of this group may reveal personal data about these people.</p> <p>For the above reasons Group data must be used carefully if we want to preserve the ability to consider it as non-personal data and therefore not subject to legal privacy legislation requirements.</p>	<p>No</p>

## Data Confidentiality

Not all data is covered by privacy legislation. However, data not covered by privacy legislation may still be considered confidential by the organization concerned. For example, the average employee salaries as at company, financial accounts or injury rates are not covered by privacy legislation, but may still be considered confidential. There are different levels of confidentiality and these will vary by organization of course, but a general guide can be provided below.

Confidentiality Level	Description	Group Data Examples	Personal Data Examples
High	Data considered sensitive and an organization would not want released publicly and will want access to tightly controlled.	Risk levels for departments. Top risk factors. Injury statistics. Average computer use levels and trends.	Injury or health information. Data on computer use or risk levels.  Any <b>Sensitive Personal Data</b>

Low	Data not intended to be released publicly, but is not considered sensitive and access does not need to be tightly controlled	HR data such as lists of departments, sites.  Some organization wide statistics such as overall risk levels, number of employees using Wellnomics software, etc.	Company address book info e.g. employee name, email address, department and job title.  Whether an employee has Wellnomics software installed, version they're using, what features they have enabled, status of completed training and assessments
None	Data an organization is happy to have released publicly.	Name of organization. Number of employees. Website address of Wellnomics software.	None

## Data Classification Examples

Below are some examples of the above classifications applied to specific data.

Data	Data Type	Confidentiality Level
User's email address, first and last name	Personal Data	Low
User's stretch-break settings	Personal Data	Low
User completion status of training and assessments	Personal Data	Low
User data on computer use, mouse use, number of breaks and applications used	Personal Data	High
User's answers to posture & workstation assessment	Personal Data	High
User's answers to discomfort assessment	May be considered Sensitive Personal Data	High
Organizational HR data	Personal Data	Low
Notes and attachments against a user record	Personal Data or Sensitive Personal Data	High
Group level data on number of users who've completed training and assessments or have unknown risks	Group data	Low
Group level data on risk levels or wellbeing scores, or top risk factors.	Group data	High
Website URL for Wellnomics hosted system	Group data	None

## Application of data classification

All data collected, stored, viewed or exported by Wellnomics products should be classified according to the above classification. This classification will then guide how the data is protected and the default access controls that are placed over it.

For example, High Confidentiality data will automatically by default require a higher level of access control.

Reporting of data will be designed so that different types of data, or data of different confidentiality levels can be restricted appropriately according to a user's access level.

For more information on this see [Wellnomics solution compliance with Data Privacy](#).

# Policy Compliance

## Compliance Measurement

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Wellnomics management team, in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Related Standards, Policies, Processes and Forms

- [Wellnomics solution compliance with Data Privacy](#)
- [Wellnomics Product Security Guidelines and Best Practice - Client](#)
- [Wellnomics Product Security Guidelines and Best Practice - SaaS](#)

# Revision History

Date of change	Responsible	Summary of change	Next revision date
20 Oct 2020	<a href="#">Kevin</a>	Created policy from existing internal documents	<ul style="list-style-type: none"><li>• 20 Oct 2021 <a href="#">Ian Bartram</a></li></ul>
13 Oct 2021	Kevin Taylor	No material change required	14 Oct 2022 <a href="#">Ian Bartram</a>



# Product Security Risk Assessment Matrix - Policy

**Review period:** Annual

For Wellnomics products there are two key types of risk:

1. Unauthorised access to data or application functionality
2. Loss of data or server/application functionality

For each type there is varying severity. We will also take into consideration the effort required for the security breach to occur.

## Unauthorized access to data or application functionality

Refer to [Data Classification - Policy](#) for definitions in bold below.

Severity	Description
None	No data or application access gained. No loss of application functionality
Minor	<p>Access to <b>Low Confidentiality Personal Data</b> about a single user e.g. HR info about a user such as email address, name, department.</p> <p>Access to <b>Low Confidentiality Group Data</b> such as statistics on training and assessment completion or number of users using the system</p> <p>Ability to create an unauthorized user account.</p>
Moderate	<p>Access to <b>High Confidentiality Personal Data</b> on a single user e.g. statistics on computer use, answers to workstation assessment, levels of discomfort, application use.</p> <p>Access to the ability to control/change settings for a single user (e.g. settings policy for one user or change settings)</p> <p>Access to <b>High Confidentiality Group Data</b> such as risk levels for departments, risk trends or top risk factors</p>
Major	<p>Access to <b>Sensitive Personal Data</b> for such as injury case data or personal health data for any user.</p> <p>Access to any <b>Personal Data</b> on multiple users at a time.</p> <p>Access to the ability to control/change settings for a multiple users at a time.</p> <p>Actions in this category carry a risk of significant legal liability (e.g. under privacy legislation), significant reputational damage (e.g. publicity about a large data breach), or a significant impact on business operation (e.g. many users having their stretch-break settings adjusted wrongly)</p>

## Loss of data or server/application functionality

Severity	Loss of data	Loss of application functionality
None	No loss of data	No affect on application or server function

<b>Minor</b>	Minor recoverable loss of data (e.g. loss of statistics data that can be easily re-synced from Wellnomics Client), or loss of data locally in client, but this data is already synced to the server.	Minor temporary loss of server performance, no application reinstall needed. Potential to affect server over time (e.g. blowing out log files or database size).  Minor temporary impact on client application functionality
<b>Moderate</b>	Major recoverable loss of data (i.e. can be replaced from backup) or minor irrecoverable loss of data (e.g. all data for a particular user lost, or user settings lost)	Temporary major loss of server performance, or server down temporarily.  Application needing to be re-installed, but configuration of system will be recovered as part of restore from backup for server
<b>Major</b>	Irreparable loss of customer data	Server failure plus backup failure meaning all configuration settings are lost upon re-install.

## Effort required for security breach

Effort	Description
<b>Accidental</b>	No effort required at all. Anyone could 'stumble' across this breach accidentally.  For example, clicking on a link takes them to somewhere they shouldn't see, or the privacy level restriction doesn't work correctly for some reports allowing the user to access them. This is pretty much the level of a bug.
<b>Easy</b>	Someone couldn't do this accidentally - they'd need to know the security hole existed, but no expert knowledge is required to do it.  For example, if they know the URL for a management report they can access it despite it not being on their menu, but they couldn't accidentally do this
<b>Expert</b>	Expert knowledge would be needed, or a large number of steps, but no special tools required or 'hacking' techniques.
<b>Hacker</b>	Hacker level. You'd have to be sniffing packets, or using advanced hacking skills and things like robots doing DOS attacks, etc.

## Considerations when evaluating security risks

As identified by Product Owner there are some additional considerations when deciding on the priority for the implementation of any Wellnomics functionality with security in mind.

1. How easily could a security breach occur?
2. What would happen if security was breached?
3. What would motivate a potential user to try?
4. What is best / common practice?

## Priority for addressing an issue

The priority for addressing an issue will be dependent upon a combination of the above. There will also be other factors at play too of course. For example, even if something is low risk, if we're not following common practice in an area then we may want to still address it.

We have to accept that someone can always hack into our system with enough effort. The key thing is to ensure Wellnomics is not negligent (through not following common or best practice) and ensuring that hacking in will not be easy. We can't necessarily expect to make things fool proof though.

A general guide to when we should take action can be come up with by combining the above lists.

	Effort required for security breach			
Unauthorised access to data or application functionality	Accidental	Easy	Expert	Hacker
None	Low Risk	Low Risk	Low Risk	Low Risk
Minor	High Risk	High Risk	Medium Risk	Low Risk
Moderate	High Risk	High Risk	Medium Risk	Medium Risk
Major	High Risk	High Risk	High Risk	High Risk
Loss of data or server/application functionality	Accidental	Easy	Expert	Hacker
None	Low Risk	Low Risk	Low Risk	Low Risk
Minor - Client App	High Risk	High Risk	Low Risk	Low Risk
Minor - Server	High Risk	High Risk	Medium Risk	Medium Risk
Moderate	High Risk	High Risk	Medium Risk	Medium Risk
Major	High Risk	High Risk	High Risk	High Risk

Risk level	Resolution Priority
Low risk	No strict requirement to resolve.
Medium Risk	Resolve in next release.
High risk	Resolve ASAP. Either fix before release, or provide a patch for already released product.

## Resolution priority

No product version should be released with a **High Risk** item present. If a High risk item is identified in a released version then a patch should be released as soon as possible (unless a new product release is about to be released within 1 week and the fix can be incorporated into it).

**Medium Risk** items should be scheduled to be fixed in next release.

Overall items should be scheduled as part of our product backlog according to the below guide.

1. **High Risk** security issue. **Fix in current release (or provide a patch)**
2. High impact bug fixes
3. **Medium Risk** security issue. **Fix in next release**
4. Features and enhancements with high market value
5. Medium impact bug fixes
6. **Low Risk** security issue
7. Other product features and enhancements
8. Low impact bug fixes

## Related Policies

- [Product Threat Modeling - Policy](#)
- [Product Security and Best Practice - SaaS - Guidelines](#)
- [Product Security and Best Practice - App - Guidelines](#)
- [Third Party Components - Policy](#)
- [Static Analysis Security Testing \(SAST\) - Policy](#)
- [Dynamic Analysis Security Testing \(DAST\) - Policy](#)
- [Security and Penetration Testing - Policy](#)

## Policy Compliance

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Revision History

Date	Responsible	Summary of change	Next revision due
20 May 2020	QA = <a href="#">Aarti</a>	New document needs review and finalization prior to publishing	<ul style="list-style-type: none"> <li>• 20 May 2020 <a href="#">Aarti</a></li> </ul>
24 Aug 2020	<a href="#">Angeli Arino</a>	Converted to a new page	
28 Sep 2020	<a href="#">Kevin Taylor</a>	Updated resolution priority and tidied up layout	
28 Oct 2020	<a href="#">Kevin Taylor</a>	Separated out 2014 security assessment and data classification	<ul style="list-style-type: none"> <li>• 28 Sep 2021 <a href="#">Ian Bartram</a></li> </ul>
05 Oct 2021	<a href="#">Corinne Wright</a>	Reviewed matrix with team and confirmed fit for purpose	<ul style="list-style-type: none"> <li>• 03 Oct 2022 2022 <a href="#">Corinne</a></li> </ul>
26 Jan 2023	<a href="#">Corinne Wright</a>	Reviewed matrix, no changes required	<ul style="list-style-type: none"> <li>• 26 Jan 2024 <a href="#">Corinne</a></li> </ul>

# Third Party Components - Policy

**Review Period:** Annual

## Purpose

To protect against the security risks that may be present in 3rd party commercial and open source components used in Wellnomics products.

## Policy

Wellnomics will follow [best practices for open source](#) as outlined in [Microsoft SDLC](#)

## Maintain Inventory of 3rd party components

A list of all 3rd party components including commercial and open source must be maintained for both client and server products. This list must be reviewed and updated with every release to include any additional components and update version numbers. The list must contain the following:

- Name of component
- Version
- Copyright
- License type
- Reference links to where the component comes from (e.g. source code repository for open source or commercial site for paid components) so that this site can be used to

## Perform Security Analysis

Wellnomics will use SAST and DAST tools that can scan for vulnerabilities such as out of date 3rd party libraries and components. See [Static Analysis Security Testing \(SAST\) - Policy](#) and [Dynamic Analysis Security Testing \(DAST\) - Policy](#). Manual penetration testing ([Security and Penetration Testing - Policy](#)) will also check for use of out of date components with known vulnerabilities.

## Keep 3rd party Components Up to Date

With each major new release or at least every 12 months a [Third Party Components Review Template](#) will be completed to identify the versions of each component used, their security importance, and how up-to-date they are compared to the latest versions available.

Any components that should be updated from a security perspective will be identified and a Jira ticket created to implement and track this change.

## Maintain a security response process

Wellnomics maintains a [Security Incident Response Plan](#) so that we can react to reported security issues. For example, if news of a new vulnerability is released (such as the [Heartbleed bug](#)) then Wellnomics will perform a risk evaluation to identify any product versions that may have this vulnerability, and then inform customers and provide a patch if needed, plus schedule an update of this component asap for next release.

## Decision process for updating components

If scanning or review identifies an out-of-date 3rd party component a risk analysis will be performed in order to make a decision whether the component needs be updated to latest version before product is released. The decision will be based upon taking into account:

1. How security critical is the component - High, Medium or None?
2. How much effort is it to update the component? Sometimes upgrading components can cause compatibility issues that take some work to be resolved.
3. If the component is of High security importance and the effort to update it is Low then the default position should be to update it to latest LTS.
4. If there is significant effort to update the component or good reasons to keep the older component then an analysis will be made to determine if the older component represents a security risk i.e. are there important vulnerabilities that have been identified in currently used version that are fixed in a newer version.
5. When it comes to updating a component we may not necessarily upgrade to the very latest version of the component, as this may cause compatibility issues. Instead a judgement will be made on which version will address any security vulnerability identified whilst also maintaining product compatibility.

## Policy Compliance

### Compliance Measurement

Copies of the component reviews will be recorded in [Third Party Components Reviews](#) and annual reviews will be conducted to verify these are being provided and updated.

Jira will be used to flag and track required component updates and verify they are implemented in next versions.

### Exceptions

Any exception to the policy must be approved by the Wellnomics management team in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

- [Third Party Components - Server Application](#)
- [Third Party Components - Wellnomics Client Application](#)
- [Third Party Components Review Template](#)
- [Third Party Components Reviews](#)

## Revision History

Date of change	Responsible	Summary of change	Date of next revision
17 Aug 2020	Angeli Arino	Reviewed and update due to changed staff permissions	<ul style="list-style-type: none"> <li>• 17 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
11 Aug 2021	<a href="#">Ian Bartram</a>	Reviewed and update due to changed staff permissions	<ul style="list-style-type: none"> <li>• 10 Aug 2022 <a href="#">Ian Bartram</a></li> </ul>
08 Sep 2022	<a href="#">Kevin</a>	Reviewed and no changes required	<ul style="list-style-type: none"> <li>• 08 Sep 2023</li> </ul>



# Product Threat Modeling - Policy

**Review period:** Annual

Threat Modeling is defined on the OWASP site here [https://owasp.org/www-community/Application\\_Threat\\_Modeling](https://owasp.org/www-community/Application_Threat_Modeling).

Wellnomics performs threat modeling on its client and server software using architecture diagrams that identify data flows and interfaces.

The [Microsoft Threat Modelling tool](#) may be used to build a threat model. This tool helps to identify areas of risk for further analysis.

## Requirements for updating threat models

Threat models for Gadget, App & SaaS software must be reviewed annually, or updated whenever a relevant change is made to the data flows, interfaces or security methods. For example, implementing a new technology or methodology for user authentication or adding a new data API.

A documented and up-to-date diagram and/or table must be maintained in Development documentation showing:

- Interfaces
- Data flow diagram
- Data classifications (types of data) involved in each part
- Data at rest (storage)
- Data in transit

The threat models for both client and server and any new products must be reviewed every 12 months to ensure they are still current, and updated where needed.

## Policy Compliance

### Compliance Measurement

A copy of the threat model and analysis will be saved as part of our completed evidence. Jira will be used to track changes that are identified as needing to be made and used to verify these changes/updates have been implemented in future releases. An annual review conducted by the current SDLC owner will verify that the processes have been followed and up-to-date evidence of such has been provided and saved in the correct locations.

### Exceptions

Any exception to the policy must be approved by the Wellnomics management team, in advance.

## Related Documents

- [Threat Modelling - App - Documentation](#)
- [Threat Modelling - SaaS - Documentation](#)
- [Product Security and Best Practice - App - Guidelines](#)
- See also "**Access security to server and data - server security model**" and "**Database access security & data flow**" in [Product Security and Best Practice - SaaS - Guidelines](#)

## Revision History



Date of change	Who	Summary of change	Next revision date
10 Oct 2020	<a href="#">Kevin</a>	Created policy to tie together existing work	20 Jul 2017 <a href="#">Ian Bartram</a>
05 May 2022	<a href="#">Kevin</a>	Reviewed policy, updated terminology and added requirements for Gadget	<ul style="list-style-type: none"> <li data-bbox="1238 365 1466 394">• 05 May 2023 <a href="#">Kevin</a></li> </ul>
09 May 2023	<a href="#">Kevin</a>	Reviewed policy, updated terminology and added additional requirements for Gadget	<ul style="list-style-type: none"> <li data-bbox="1238 465 1414 517">• 07 May 2024 @kevin</li> </ul>

# Static Analysis Security Testing (SAST) - Policy

**Review period:** Annual

## Policy

- Modern compilers also provide extensive warnings regarding coding issues and risky coding practices. Wellnomics will ensure all compiler warnings are enabled and endeavor to resolve all compiler warnings with the goal of eliminating all compiler warnings in released code. If warnings cannot be eliminated they will be reviewed and ensured they do not represent a security risk.
- Wellnomics will also use a minimum of one static analysis tool as part of the standard compilation or CI process for all developers to identify potential coding issues that could cause product security or stability issues.
- The tools used will be best practice market proven tools (refer <https://wellnomicsdev.atlassian.net/wiki/pages/resumedraft.action?draftId=523174072> ) and developers will be required to address and fix all errors that could affect security. Tools will be selected to be most effective for each development environment, likely meaning different tools may be used for Client and Server software code.
- The <https://wellnomicsdev.atlassian.net/wiki/pages/resumedraft.action?draftId=42868601> will be used to guide the priority for addressing any issues or warnings found.
- Once experience is gained using the above Risk Assessment Matrix for a new tool the [Static Analysis Security Testing \(SAST\) - Guide](#) will be updated and maintained for each tool clearly indicating what types of warnings or errors found should be resolved using **Must fix / Try to Fix / Ignore** ratings. As an example, refer to the recommended warnings to be fixed when using Visual Studio Code Analysis as outlined in [Microsoft Recommended Tools, Compilers and Options for x86, x64 and ARM](#).
- All **Must Fix** items must be fixed before code can be committed.
- Where possible commit and CI tools should be set to **automatically reject commits** that does not pass the static code analysis requirements. This ensures that the quality process and required standards are automatic and will always be applied..
- Although it is acceptable to ignore some low level warnings if they are rated as low risk using the Risk Assessment Matrix, the best practice goal is to aim for **zero warnings** if possible so that it's easy to spot new or important warnings. It is not acceptable to have hundreds of warnings that are always ignored.
- **Switches** may be used to hide low level warnings as long as this is documented and a risk based decision is made on this being acceptable.
- For currently used tools refer to [Software Development Tools - Documentation](#) or [Static Analysis Security Testing \(SAST\) - Guide](#)

## Policy Compliance

### Compliance measurement

**Every 6 months** a copy of the latest static analysis & compiler warnings report for each product will be attached in the [Static Analysis Security Testing \(SAST\) - Results](#). This can be compared against the [Static Analysis Security Testing \(SAST\) - Guide](#) to verify that no warnings or vulnerabilities of significance were found.

### Exceptions

Any exception to the policy must be approved by the Wellnomics management team, in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Documents

- [Software Development Tools - Documentation](#)
- [Static Analysis Security Testing \(SAST\) - Guide](#)
- [Static Analysis Security Testing \(SAST\) - Results](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
05 Nov 2020	<a href="#">Kevin</a>	Added new policy based upon Microsoft SDLC	<ul style="list-style-type: none"> <li>• 05 Nov 2021 <a href="#">Angeli Arino (Deactivated)</a></li> </ul>
30 May 2021	Kevin Taylor	Updated to include compiler warnings	<ul style="list-style-type: none"> <li>• 30 May 2022 2022</li> </ul>
08 Sep 2022	<a href="#">Kevin</a>	Reviewed and confirmed still current - no changed required	<ul style="list-style-type: none"> <li>• 08 Sep 2023 <a href="#">Kevin</a></li> </ul>

# Dynamic Analysis Security Testing (DAST) - Policy

**Review period:** Annual

## Policy

- Wellnomics will use a minimum of one DAST tool as part of the standard compilation or CI process for all developers to identify potential coding issues that could cause product security or stability issues.
- The DAST tools used will be best practice market proven tools (refer [Software Development Tools - Policy](#) ) and developers will be required to address and fix all errors that could affect security. DAST tools will be selected to be most effective for each development environment, likely meaning different tools may be used for Client and Server software code.
- The [Product Security Risk Assessment Matrix - Policy](#) will be used to guide the priority for addressing any issues or warnings found.
- Once experience is gained using the above Risk Assessment Matrix for a new tool the [Dynamic Analysis Security Testing \(DAST\) - Guide](#) will be updated and maintained for each SAST tool clearly indicating what types of warnings or errors found should be resolved using **Must fix / Try to Fix / Ignore** ratings. As an example, refer to the recommended warnings to be fixed when using Visual Studio Code Analysis as outlined in [Microsoft Recommended Tools, Compilers and Options for x86, x64 and ARM](#).
- All **Must Fix** items must be fixed before code can be committed.
- Although it is acceptable to ignore some low level warnings if they are rated as low risk using the Risk Assessment Matrix, the best practice goal is to aim for **zero warnings** if possible so that it's easy to spot new or important warnings. It is not acceptable to have hundreds of warnings that are always ignored.
- **Switches** may be used to hide low level warnings as long as this is documented and a risk based decision is made on this being acceptable.
- For currently used DAST tools refer to [Software Development Tools - Documentation](#) or [Dynamic Analysis Security Testing \(DAST\) - Guide](#) .

## Policy Compliance

### Compliance measurement

**Every 6 months** a copy of the latest DAST report for each product will be attached in the [Dynamic Analysis Security Testing \(DAST\) - Records](#) . This can be compared against the [Static Analysis Security Testing \(SAST\) - Guide](#) to verify that no warnings or vulnerabilities of significance were found.

### Exceptions

Any exception to the policy must be approved by the Wellnomics management team, in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Documents

- [Software Development Tools - Documentation](#)
- <https://wellnomicsdev.atlassian.net/wiki/pages/resumedraft.action?draftId=523469253>
- [Dynamic Analysis Security Testing \(DAST\) - Records](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
05 Nov 2020	<a href="#">Kevin</a>	Added new policy based upon Microsoft SDLC	<ul style="list-style-type: none"><li>05 Nov 2021 <a href="#">Ian Bartram</a></li></ul>
16 Dec 2021	<a href="#">Corinne</a>	Reviewed, no changes needed	<ul style="list-style-type: none"><li>16 Dec 2022 <a href="#">Corinne</a></li></ul>
26 Jan 2023	Corinne	Reviewd, no changes needed	<ul style="list-style-type: none"><li>26 Jan 2024 <a href="#">Corinne</a></li></ul>

# Security and Penetration Testing - Policy

**Review period:** Annual

## Introduction

Security and Penetration testing is carried out on software products, installed in their typical environment, to ensure that there are no risks of unauthorized access that might present threats to data security, data integrity and data privacy. Such threats might include, but is not limited to:-

- unauthorized access as a user
- unauthorized access as a result of hacking code
- injection of malicious code
- Loss of data or product availability

For a full list of possible risk types see [Wellnomics Product Security Risk Assessment Matrix](#)

Current best practice guide for performing security and penetration is defined in the following:

- [Penetration Testing of Server - Guide](#)
- [Security Testing of Client - Guide](#)

## Policy for Security Testing of Client Apps

The criteria for selecting whether to run a test on the client applications and which areas of the product to test are as follows:

1. Has there been any significant changes to the product in security threat areas (refer [Threat Model for Wellnomics Client App](#)) such as:
  - a. Interfaces like the internet connection and user account authentication
  - b. Cryptographic tools such as TLS such as the interfaces
  - c. Nature of data being stored or being communicated through interfaces.
2. A retest at least every 12 months to verify everything still passes.

## Policy for Penetration Testing of Server

### Internal Penetration Testing

Due to the overhead of carrying out complete penetration testing on every release (every 8 weeks) the requirement to complete a penetration test on a new release will be based on a risk assessment process completed during the Release QA process. It will be the responsibility of the QA Team Lead to determine whether a penetration test is required. In completing such a risk assessment, the QA Team Lead will consider the following:-

- Time since the last penetration test was completed. The maximum time between penetration tests shall **not exceed 12 months**.
- The changes introduced in the completed sprint and release
- Any changes in operating environments facilitated by the new release e.g. Windows Server versions or SQL Server versions
- Any potential vulnerabilities in either the software or the intended operating environment that would suggest a new penetration test

### External Penetration Testing

Wellnomics will contract a full external manual penetration test **at least every 12 months** from a professional qualified penetration testing consultancy.

## Fixing vulnerabilities

Any vulnerabilities identified during testing will be evaluated using the [Wellnomics Product Security Risk Assessment Matrix](#) to determine severity and resolution priority. If a failure meets the specified threshold a fix will be required to be implemented before the product can be released and a retest will be asked for.

## Testing process & fixing failures or vulnerabilities found

Testing will follow the [Security Testing of Client - Guide](#) or [Penetration Testing of Server - Guide](#) with tests designed to provide full coverage in assessing compliance with [Wellnomics Product Security Guidelines and Best Practice - Client](#) or [Wellnomics Product Security Guidelines and Best Practice - SaaS](#).

Tests must all be designed to provide clear Pass / Fail results with clear evidence that must be saved (e.g. file or screenshot) to provide proof of each result. Testing results should be recorded using the [Client App Security Testing Record - Template](#) or [Penetration Testing Record - Template](#) and saved in [Completed Records for Product Security and Penetration Testing](#)

Any test fails or new vulnerabilities found will be evaluated using the [Wellnomics Product Security Risk Assessment Matrix](#) to determine severity and resolution priority. If a failure meets the specified threshold a fix will be required to be implemented before the product can be released.

If a fix is implemented to address a test failure the testing must be repeated in full on the next version to verify that all the tests pass. A new testing record will be created and saved in [Completed Records for Product Security and Penetration Testing](#)

## Policy Compliance

### Compliance Measurement

Testing records will be created and saved for each test in [Completed Records for Product Security and Penetration Testing](#). Each test will require clear evidence of pass or fail to be attached (e.g. screenshot).

### Exceptions

Any exception to the policy must be approved by the Wellnomics management team, in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies, Processes and Forms

- [Wellnomics Product Security Guidelines and Best Practice - SaaS](#)
- [Wellnomics Product Security Guidelines and Best Practice - Client](#)
- [Penetration Testing of Server - Guide](#)
- [Security Testing of Client - Guide](#)
- [Penetration Testing Record - Template](#)
- [Client App Security Testing Record - Template](#)
- [Completed Records for Product Security and Penetration Testing](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
July 2016	Wayne Owens, Principal Consultant	Converted to new format	20 Jul 2017 <a href="#">Wayne Owens (Unlicensed)</a>
07 Jul 2017	Wayne Owens	Checked for up to date - all OK no changes needed	09 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay	Reviewed, no changes made	<ul style="list-style-type: none"> <li>05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
13 Dec 2018	Wayne Owens	Updated document to reflect move to continuous release V3.4 onwards	<ul style="list-style-type: none"> <li>18 Dec 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
20 May 2020	Wayne Owens	Reviewed, no changes required	<ul style="list-style-type: none"> <li>20 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
24 Aug 2020	Angeli Arino	Converted to a new page	
05 Nov 2020	<a href="#">Kevin</a>	Updated to include client security testing sections and links	<ul style="list-style-type: none"> <li>24 Oct 2021 <a href="#">Aarti</a></li> </ul>
13 Oct 2021	<a href="#">Aarti</a>	Updated to reflect current practices	20 Oct 2022 <a href="#">Aarti</a>



# DEPLOYMENT & HOSTING - Policies

See [DEPLOYMENT & HOSTING - Policies](#) under space [WELLNOMICS INFORMATION SECURITY POLICIES](#) for the master copies of official guidelines and policies relevant to Support & IT. Pages in this section should avoid duplicating the master policies and where possible the master copies should be maintained and just linked to from pages in this space.

- [Customer Services Interactions - Policy](#)
- [Management of Hosting - Policy](#)
- [Receipt, Storage and Deletion of Customer Data - Policy](#)
- [Access Security - Hosting - Policy](#)
- [Threat Modeling - Hosting - Policy](#)
- [Disaster Recovery and Business Continuity - Hosting - Policy](#)

# Customer Services Interactions - Policy

**Review period:** Annual

## Introduction and Overview

As part of its commitment to provide customers with a high level of support in all stages of the engagement process (pre-sales, pilots, trials, post sales, implementations and ongoing support), Wellnomics has developed the approaches included in this document to which all relevant staff must adhere.

## General Principles

The following general principles will apply to all customer interactions:-

- All customer and their representatives be dealt with respect
- All customer interactions shall be conducted in a timely manner and in all responses to customers should be made within 1 working day (the ability to do this may be influenced by time zones and non-corresponding weekends etc. In most circumstances we endeavour to exceed this target and generally do.
- All communications with customer shall be clear and concise and where possible should demonstrate Wellnomics' commitment to "go the extra mile".

All customer interactions should be used as an opportunity to improve and enhance the customer relationship and to develop a close interpersonal relationships with key customer representatives.

## Proactive and Reactive Customer Interactions

Proactive interactions are those initiated by Wellnomics, normally in the context of account management, however there will be some circumstances where support issues may require a proactive approach e.g. advising affected customers of a bug etc. This document is concerned with reactive customer interactions where Wellnomics is responding to a customer following an approach initiated by a customer. Examples where this may occur includes, but is not limited, to:-

1. Support calls for assistance with technical issues
2. Support calls for assistance with usage issues
3. Support calls relating to issues other than technical or usage requests e.g. requests for background information, ergonomics collateral to information etc.
4. Support calls reporting issues with the availability or performance of Hosted Wellnomics SaaS systems
5. Calls related to account matters e.g. invoicing, requests for additional user licenses, requests to extend system modules etc.

Where customer support requests (as outlined in 1-5 above) are received via email to [support@wellnomics.com](mailto:support@wellnomics.com), they are automatically created as a "ticket" within the Freshdesk system. The Freshdesk system is the software database used to record, track and resolve support calls and incidents.

Whilst all "incidents" are to be recorded as support tickets. Not all support tickets will be incidents. For the purposes of reactive support requests, Incidents are defined as *"those circumstances where a customer system is either not available or seriously compromised in terms of performance or the accuracy of data recording or reporting"*. If any recorded support tickets relate to issues that come under the definition of "incidents" then the Incident Management Policy and Procedures will apply - please see

[Incident Management Process - Policy](#) . Please also see additional definitions of "incidents" contained therein.

Definitions relevant to the support processes are also contained within the Wellnomics Software Agreement and SLA signed by all customers and Wellnomics on the conclusion of a sale. The relevant entries are:-

**"Critical Error"** means an error, defect, or omission, which causes the Wellnomics Software to be completely unusable by all Users.

**“Significant Error”** means an error, defect or omission that causes the Wellnomics Software to be unusable in large part by Users.

**“Discrepancy”** means an error or defect in the distribution media or material difference between the operation of the Wellnomics Software and the description of the operation of the Wellnomics Software as contained in the documentation provided for the Wellnomics Software by Wellnomics.

By definition therefore, all critical and significant errors will be “incidents” for the purposes of handling as a support ticket.

In addition to the above, note that the Wellnomics Software Agreement also contains the following Wellnomics responsibility:-

To “provide an error and defect request/reporting service by which the Customer can be assured that Wellnomics will promptly investigate and correct in a future release of the Wellnomics Software any errors, defects, or omissions made known to Wellnomics. Wellnomics may implement such error and defect reporting service on its website”

Note that at this time (please see document date/revision date) the logging of support calls through the website has not been introduced. The Freshdesk system and the automatic logging of emails to [support@wellnomics.com](mailto:support@wellnomics.com) remains the prime method of recording and progressing customer related support calls.

Telephone conversation that may result in the creation of support tickets in Freshdesk - from time to time there may be occasions when a telephone conversation with a customer may give rise to the need to create a support ticket for the recording and actioning of a particular issue. If this happens it is the responsibility of the Wellnomics support personnel to create and email to [support@wellnomics.com](mailto:support@wellnomics.com) to record the details of the issue.

## The Day to Day Management of Support Tickets

Support tickets from [support@wellnomics.com](mailto:support@wellnomics.com) may be created for a number of reasons as outlined above. In normal circumstances, the ticket in Freshdesk is created approximately 5 minutes after the email is received in [support@wellnomics.com](mailto:support@wellnomics.com). It will be the task of the support team member allocated with responsibility to manage Freshdesk tickets to check the new tickets in Freshdesk at least twice per day (9am and 2pm) and to allocate the ownership and responsibility (2 role functions within Freshdesk) of the ticket to a specific person in the support team.

## The Handling of Support Tickets

*A ticket once created within the Support software (currently Freshdesk) will be automatically allocated a number e.g. Ticket#1004367 — Bugs in Wellnomics--reporting computer use*

Note that the text after the ticket number is created from the subject line in the email that gave rise to the creation of the support ticket. The ticket number e.g. Ticket#1004367 should be included in the subject line of all ensuing communications to ensure that subsequent emails are linked to the original ticket. This also required so that all emails are also copied to [support@wellnomics.com](mailto:support@wellnomics.com).

Once a support team member has been given ownership and responsibility for a specific support ticket an email is automatically sent by the Freshdesk system to that person advising them of the ticket allocation

All support calls should be responded to within 1 working day of receipt excepting weekends when any received after 4pm on Friday will need to be responded to first thing on Monday morning. Where possible a support ticket should be responded to as comprehensively as possible such that it is resolved as quickly as possible. Where it is not possible to quickly resolve the issue it should be reviewed on a regular basis and the customer advised of progress.

On occasions, it is possible that some issues are as a result of a bug that may not be fixed until a future software release. Where this is the case a work-around should be offered (if one exists) and the customer advised. The support person responsible for the ticket may elect to keep the ticket “open” until such time that the resolution (by way of release) has been made available to the customer. Where issues are resolved, they should be recorded as such by “closing” the ticket within the Freshdesk system.

## Support Tickets – team approach

From time to time a support ticket may require the efforts of more than one individual, either within the Support Team or the wider Wellnomics team. Where this is the case the ownership and responsibility may be shifted to a new member of the team.

Difficult cases or those requiring potentially significant resources either within Support or the wider company should be discussed within the weekly Support Team meeting, or directly with the Customer Success Manager if more urgent. Notes can be appended to the Freshdesk record of any relevant conversation relating to specific cases.

## Destruction of Data Held on Equipment to be De-commissioned

See policy - [Equipment Disposal Policy](#)

## Reporting and Recording of Incidents Relating to Customer Data

Any reportable incidents relating to stored customer data must be recorded and reported . Reportable incidents include but are not limited to:-

- Loss of media on which customer data is stored e.g. portable drives, laptops etc.
- Unauthorized/unapproved access to customer data.
- Loss of customer data (accidental deletion etc.)

The completed incident report form must be submitted to the Chief Executive at the earliest opportunity. See procedure:-

[Incident Management Process - Policy](#) . This will require the completion of the :- [Incident Report and Investigation Form](#)

## Review & Revision History

Date of change	Responsible	Summary of change	Next revision date
Created 8th January 2015	Wayne Owens	Document created	10 January 2016
15 January 2016	Wayne Owens	Updated document to link to newly created/revised policies and procedures	January 2017
2nd February 2017	Wayne Owens	Updated and refreshed links to related documents	
12 Feb 2018	Chris Mackay	Checked and review, no changes required	
27 Feb 2019	Wayne Owens	Reviewed - removed duplicated text with links to specific policies	<ul style="list-style-type: none"> <li>• 28 Feb 2020 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
04 Mar 2020	Wayne Owens	Reviewed, no changes required	<ul style="list-style-type: none"> <li>• 05 Mar 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
31 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"> <li>• 31 Aug 2021 <a href="#">Corinne</a></li> </ul>
08/04/2022	Corinne Wright	reviewed and no changes required	<ul style="list-style-type: none"> <li>• 08 Apr 2023 <a href="#">Corinne</a></li> </ul>
27/02/23	Wayne Owens	Revised as part of rationalization of multiple policies referencing incident management	27 Feb 2024 <a href="#">Corinne</a>

# Management of Hosting - Policy

**Review Period:** Annual

## Overview

Wellnomics Ltd hosts the Wellnomics SaaS for a number of clients. Systems are hosted on servers provided by Microsoft Azure with whom Wellnomics has a Service Level Agreement for servers currently located in the US, United Kingdom and Australia (Sydney).

## Purpose

This policy sets out the requirements for Wellnomics staff to be able to access hosted customer systems in a safe and secure manner and in accordance with all other relevant data protection and security policies that might contain either general or specific requirements relating to accessing hosted customer systems.

## Scope

This document applies to Wellnomics SaaS systems hosted by Wellnomics on behalf of customers.

This document applies to all employees, contractors, consultants, temporary and other workers at Wellnomics Ltd and its subsidiaries must have awareness of this policy. Notwithstanding this, only those personnel that have been approved by the Wellnomics Management Team are permitted to access customer systems. These staff are specified in the [WELLNOMICS INFORMATION SECURITY POLICY](#) and under the [User Management Policy](#)

## Policy

### General

Physical and Access Security is governed by the [Access Security - Hosting - Policy](#)

Access to and handling of customer data is covered by [Receipt, Storage and Deletion of Customer Data - Policy](#)

All customers will agree to the standard Wellnomics terms and conditions as they apply to hosted systems. Section 4 of Appendix A (Wellnomics Hosted Server) states:-

#### **Appendix A Section 4 DATA SECURITY**

*4.1 Wellnomics acknowledges that the Data is confidential and shall use its best efforts to protect the Data from unauthorized use or disclosure. Without limiting the generality of the foregoing, Wellnomics shall restrict access to the Data to trusted staff who require access for a legitimate purpose and who recognize the importance of maintaining strict confidentiality.*

4.2 Wellnomics employs standard industry protocols for protecting secure and confidential information, such as the Data, from unauthorized access. Wellnomics shall use all reasonable efforts to ensure a secure environment for the transmission and storage of the Data. Wellnomics will take normal precautions to protect the Wellnomics Server from security breaches, including without limitation, security breaches resulting from computer hackers, denial of service attacks, unlawful entry, unauthorized access, theft, disgruntled employees and other fraudulent acts. However, Wellnomics cannot accept liability for any such security breaches that may occur despite all reasonable efforts to prevent. Without limiting the generality of the foregoing, it is the Customer's responsibility to deny access to the Wellnomics Server to any person that severs his or her relationship with the Customer and this should be done in a timely fashion.

## Support

From time to time authorized Wellnomics staff may need to access customer data to facilitate the investigation and resolution of support tickets and other inquiries. This may require the viewing and analysis of data at an individual level. The responsibilities of Wellnomics staff regarding confidentiality and protection of personal information is set out in [WELLNOMICS INFORMATION SECURITY POLICY](#) and all staff are required to comply with these requirements

## System upgrades

Where customer system access is required to system upgrades, the express permission of the client will be necessary if they have amended the standard hosting contract to include such a requirement. By default, contracts do not require such permissions to be sought.

Notwithstanding the above, because system upgrades result in downtime, customers will normally be notified in advance so that a mutually convenient date and time can be agreed for the upgrade.

## Backups

Wellnomics staff manages backups of customer data to backup all files on the application volume of each server (i.e. database and application). Backup is performed daily at 11pm in the relevant server time zone). Backups have a 2 week On-site retention, and two week cloud (region locked) retention. Backups are Weekly Full + Daily Incremental.

Each time the OS is updated or configuration changes made a new snapshot of the OS volume will be taken. This snapshot will be kept indefinitely and used to allow a fast restore of the server in the event of a complete server loss.

If a disaster event occurs, then if the disaster only affects the database or application then a restore is performed from the cloud backup. If the entire server is affected then first the OS snapshot is restored, then the application volume is restored.

## Roles Matrix and Permissions

See [User Management Policy](#)

## Server patches & hardening

### Operating system (Windows Server)

All hosted servers need to be kept up to date with the latest Microsoft Security Patches as per policy . Servers are set to automatically download updates, but they need to be manually installed. Wellnomics support staff are automatically notified of any pending updates/patches and these are normally installed weekly at a time outside of business hours, e.g. over the weekend, to minimize disruption to customers.

After installation or OS upgrade a server OS hardening process is applied as per [Hardening Checklist - Windows Server OS - Template](#) and a record of the completed checklist for each server is retained (see [Windows Server OS/IIS/SQL Hardening Checklists - Completed Records](#) )

### IIS Server

IIS patches or updates are notified to Wellnomics Support staff and will be checked with development team for any possible compatibility issues before being approved for installation.

After initial installation or upgrade of IIS a hardening process is applied as per [Hardening Checklist - IIS Server - Template](#) and a record of the completed checklist for each server is retained (see [Windows Server OS/IIS/SQL Hardening Checklists - Completed Records](#) )

### SQL Server

IIS patches or updates are notified to Wellnomics Support staff and will be checked with the development team for any possible compatibility issues before being approved for installation.

After initial installation or upgrade of IIS a hardening process is applied as per [Hardening Checklist - SQL Server - Template](#) and a record of the completed checklist for each server is retained (see [Windows Server OS/IIS/SQL Hardening Checklists - Completed Records](#) )

## Wellnomics Applications

If security vulnerabilities are identified in the main Wellnomics application either by an issue being reported, or after penetration testing, then a new update or patch will be created and deployed to the server once tested. This is done in co-operation with the customer.

# Notifications and Communication

See also [Incident Management Process - Policy](#) .

Where the normal activities of managing the hosted server environments and / or the Wellnomics systems hosted on such servers reveals either suspicious behavior or circumstances that could result in a data security incident, such behavior and circumstances will be subject to the [Incident Management Process - Policy](#) and this process must be followed, including where deemed necessary, notifying the customer of such behavior or circumstances. It will be for the Wellnomics Chief Executive to determine whether it is necessary for the customer to be notified in any particular incident.

# Policy Compliance

## Compliance Measurement

The Wellnomics Management Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to this policy must be approved by the Wellnomics Management Team

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Related Standards, Policies and Processes

- [Passwords and Encryption - Employees & Contractors - Policy](#)
- [Service Level Agreement and Security Statement](#)
- [User Management - Employees & Contractors - Policy](#)
- <https://wellnomicsdev.atlassian.net/wiki/pages/resumedraft.action?draftId=642449469>
- [Hardening Checklist - Windows Server OS - Template](#)
- [Hardening Checklist - IIS Server - Template](#)
- [Hardening Checklist - SQL Server - Template](#)

# Definitions and Terms

None

# Revision History

Date of change	Responsible	Summary of change	Next revision date
30 Mar 2016	Wayne Owens, Principal Consultant	Updated and converted to new format.	29 Mar 2017 <a href="#">Wayne Owens (Unlicensed)</a>
03 Jul 2017	Wayne Owens, Principal Consultant	Updated aspects relating to the use of licensed software for dedicated hosted server maintenance workstation	04 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
17 May 2018	Kevin Taylor, CEO	Updated section on Backups for cloud servers.	04 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay	Reviewed, no changes made	
1 March 2019	Kevin Taylor	Updated requirements on server patches and hardening and Rackspace backups policies	<ul style="list-style-type: none"> <li>01 Mar 2020 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
22 May 2020	Wayne Owens	Reviewed and updated to change references from Rackspace to Microsoft Azure	<ul style="list-style-type: none"> <li>21 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
24 Aug 2020	Angeli Arino	Converted to a new page	
20 Dec 2020	<a href="#">Kevin</a>	Split out relevant sections into separate Access Security Policy	<ul style="list-style-type: none"> <li>24 Dec 2021 <a href="#">Ian Bartram</a></li> </ul>
20 Dec 2021	<a href="#">Ian Bartram</a>	Reviewed - no material changes required	<ul style="list-style-type: none"> <li>20 Dec 2022 <a href="#">Ian Bartram</a></li> </ul>
23 Mar 2023	<a href="#">Ian Bartram</a>	Reviewed - no material changes required	<ul style="list-style-type: none"> <li>18 Mar 2024 <a href="#">Ian Bartram</a></li> </ul>



# Receipt, Storage and Deletion of Customer Data - Policy

**Review period:** Annual

## Overview

From time to time, Wellnomics may be provided with customer data for the purposes of customer support and troubleshooting, but also for research purposes. These guidelines cover the handling of such data. This is part of Wellnomics Technical and Organizational Measures (TOM) against unauthorized processing of personal data.

## Purpose

The purpose of this policy is to define the guidelines for the secure handling of customer data.

## Scope

This policy applies to all customer data however that may be supplied or communicated. This customer data may be available in a number of forms which includes, but is not limited to:-

- Screenshots, user lists etc. – often supplied as part of a support request in the form of email contents or attachment
- Data downloaded from secure ftp sites set up by Wellnomics Ltd, and stored on the Wellnomics network.
- Database back-ups, copies etc., supplied for trouble shooting and/or analytical analysis.

All Wellnomics employees and affiliates must comply with this policy.

## Policy

Customer data should always be communicated using the most secure means possible. Where customers either supply data or are requested to provide data for troubleshooting or analytical purposes, such data should be transferred using the specific customer account created within [ftp.wellnomicsonline.com](ftp://wellnomicsonline.com). This is a secure site utilizing secure ftp protocols (SFTP). The customer will need to be provided with the sign in criteria for this secure site before they are able to deposit or receive data.

Where possible, the storage of customer data on portable or removable media e.g. laptops, portable drives, pen drives etc. devices should be avoided. In circumstances where this is not possible all efforts should be made to ensure that such data is:

- Anonymised, and/or
- File password protected
- All other devices on which data is stored must be password protected with username and secure (strong) password. This includes all laptops, tablets and smart devices (including phones etc.). In this context, a strong password must comply with the [Password Construction Guidelines](#)
- All data must be encrypted prior to sending and de-crypted on receipt. The method of encryption/decryption must be agreed in advance with the customer and may depend upon the encryption methods to which the customer has access.

In the event that customer data is delivered on portable media, it must be copied to the secure Wellnomics server on the Wellnomics network (currently the server "Holly" is reserved for this purpose) and the source data on the portable device must immediately be deleted through reformatting of the source media. Only members of Wellnomics staff that have a justifiable reason to access customer data will be approved to do so. Any staff member wishing to access non-anonymized customer data can only do so with the approval of the Chief Executive or the Principal Consultant. Application for access must be made using the prescribed form (see [Application for Access to Non Anonymised Customer Data](#)). Completed forms are to be retained in the file kept in the locked data cupboard to provide an audit trail of access to stored data.

Customer data should not be printed to hard media (paper). For this reason the dedicated workstation reserved for managing the hosted servers is not connected to a local printer and has no access to the Wellnomics network or networked printers.

If customer data is received in a non-anonymized form it must be anonymized as soon as is practicable i.e. once the need for non-anonymized data is no longer necessary.

## Data Anonymization, Retention and Destruction

As set out above, where possible, customer data should be anonymized before receipt. Wellnomics can provide customers with anonymization scripts that can be run on customer data prior to sending (via sftp as outlined above). Where anonymization renders the purpose of sending the data futile then non-anonymized data can be accepted.

Data must only be retained for as long as it is required for the purpose for which it was received/obtained. Once this purpose has been satisfied the data must be deleted. Any data that has been stored for 3 months must be approved on a quarterly basis for continued storage. Approval must be sought from either the Chief Executive or the Principal Consultant.

## Destruction of Data Held on Equipment to be Commissioned

Any Wellnomics equipment that does, or may contain, any data or information that relates to the business of Wellnomics or any of its customers must be de-commissioned in accordance with the [Equipment Disposal Policy](#)

## Termination of Contract

On termination contract the responsibility for the termination process, from a customer data perspective, is the Senior Technical Consultant.

On termination of contract, all customer data is to be deleted as soon as is practicable and in any event no longer than 90 days after termination. Destruction of customer data must incorporate checks on the following potential data sources:-

- removable or transportable media
- hosted servers
- Hosted server backups (see below)
- Customer specific secure FTP sites (SFTP)
- All support records hosted in the Wellnomics "Freshdesk" Support Ticketing System

Note regarding hosted systems backups - daily backups are taken of the entire hosted server and not for separate customer systems. As there is a requirement from most customer to maintain backups for a minimum period (normally 90 days) then it is not possible to delete customer data held as encrypted backups for a period of 90 days from termination of contract and deletion of production system.

## Process for termination of contract

- Notification from Sales Team that contract has been terminated with agreed Termination Date (ATD). This notification will be by way of company wide email which will act as the trigger for the following technical processes.
- On the agreed termination date the Senior Technical Officer to:-
  - access the relevant hosting server and delete customer database and related services and website
  - Check for any stored media that may contain hosted customer data and delete through full reformat of data
  - Access Freshdesk System and purge system of all support records
  - Access client specific secure FTP site and delete all customer related data
  - Complete and sign a [Equipment De-Commissioning Form](#) as appropriate for a customer contract termination and store physical copy on client file.

## Policy Compliance

## Compliance Measurement

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Wellnomics management team, in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

- [Acceptable Use - Employees & Contractors - Policy](#)
- [Equipment De-Commissioning - Policy](#)
- [Passwords & Encryption - Employees & Contractors - Guidelines](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
16 May 2017	Wayne Owens, Principal Consultant	updated to new format	15 May 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay	Reviewed, no changes made	<ul style="list-style-type: none"> <li>• 05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
20 May 2020	<a href="#">Chris MacKay (Deactivated)</a>	Reviewed, no changes required	20 May 2021
24 Aug 2020	Angeli Arino	Converted to a new page	
20 Dec 2020	<a href="#">Kevin</a>	Created using content taken from separate documents in other sections.	<ul style="list-style-type: none"> <li>• 24 Dec 2021 <a href="#">Ian Bartram</a></li> </ul>
20 Dec 2021	<a href="#">Ian Bartram</a>	No material changes required	19 Dec 2022 <a href="#">Ian Bartram</a>
23 Mar 2023	<a href="#">Ian Bartram</a>	No material changes required	<ul style="list-style-type: none"> <li>• 18 Mar 2024 <a href="#">Ian Bartram</a></li> </ul>

# Access Security - Hosting - Policy

**Review Period:** Annual

## Overview

Wellnomics as a company has a variety of servers and systems that are secured using physical and logical security measures. This document describes the various methods used under each category. All staff are made aware of these measures and their responsibilities under these measures and training is provided to staff both on enrolment and on a regular basis (annually) thereafter.

In addition to the Wellnomics premises where staff are housed along with the equipment/tools of software development (PCs, laptops, server, routers etc.), Wellnomics also hosts systems on behalf of clients using Microsoft Azure servers located globally (currently in the US, UK and Australia). Whilst logical security under the control of Wellnomics staff applies to both internal and externally hosted systems, physical security is only directly controlled by Wellnomics at its own premises. Physical security of the hosted, Azure servers is under the control of Microsoft and covered by the service level agreement (SLA) that exists between Microsoft and Wellnomics Ltd.

## Purpose

The purpose of this policy is to set out the requirements and form of the access security measures in place at Wellnomics Ltd as it applies to both its internal systems and environment and the hosted environments sources through Microsoft Ltd.

## Policy

### Logical Security

#### Access to Hosted Servers

- Access to hosted servers is via a highly secure Remote Monitoring and Management Software.
- All hosted servers (provided by Microsoft Azure) are protected by usernames and passwords. Passwords must comply with the [Password and Encryption Policy](#) and the [Password Construction Guidelines](#).
- Only those staff approved by the Wellnomics Management Team in the the [WELLNOMICS INFORMATION SECURITY POLICY](#) (Section 4.3) are permitted to access customer hosted systems.
- All access to the RMM software is highly restricted via Roll Based Access Control and application based multi-factor authentication.
- The hosted environment on the server contains only that software required to operate and maintain the hosted server environment and to carry out routine maintenance and upgrades
- All software used on the server must be:-
  - a valid and up to date version with all security patches and other relevant updates applied
  - properly licensed i.e. a full and up to date license must be possessed by Wellnomics Ltd for any software to be utilized in accessing and supporting hosted systems
- **System logging** - all hosted servers will have system logging turned on full. This provides an audit trail of all changes made to hosted systems including logged in user and date/time and type of change - logging cycle to be 90 days when files will overwrite oldest entries
- **Auto logout.** The RMM service used to access hosted servers is set to auto-lock when a technician disconnects.
- **Patch management** - all "patches" to be installed to operating system and related and required software to ensure system stability and the security of stored and transmitted data. See item below on testing prior to deployment.
- Upgrades to hosted systems software: all upgrades to hosted server Wellnomics systems must be tested in a similar, but non-production environment, prior to being deployed on production systems and environments
- The dedicated hosted servers has no access to the Wellnomics network generally and as such is blocked from being able to connect with any physical connection.

- All hosted server configurations, passwords and access credentials and all other information necessary to recreate the hosted server environment in the event of a total system loss are securely stored in Azure and password manager. These are updated as required as passwords etc are changed in accordance with other hosted server and corporate IT policies.

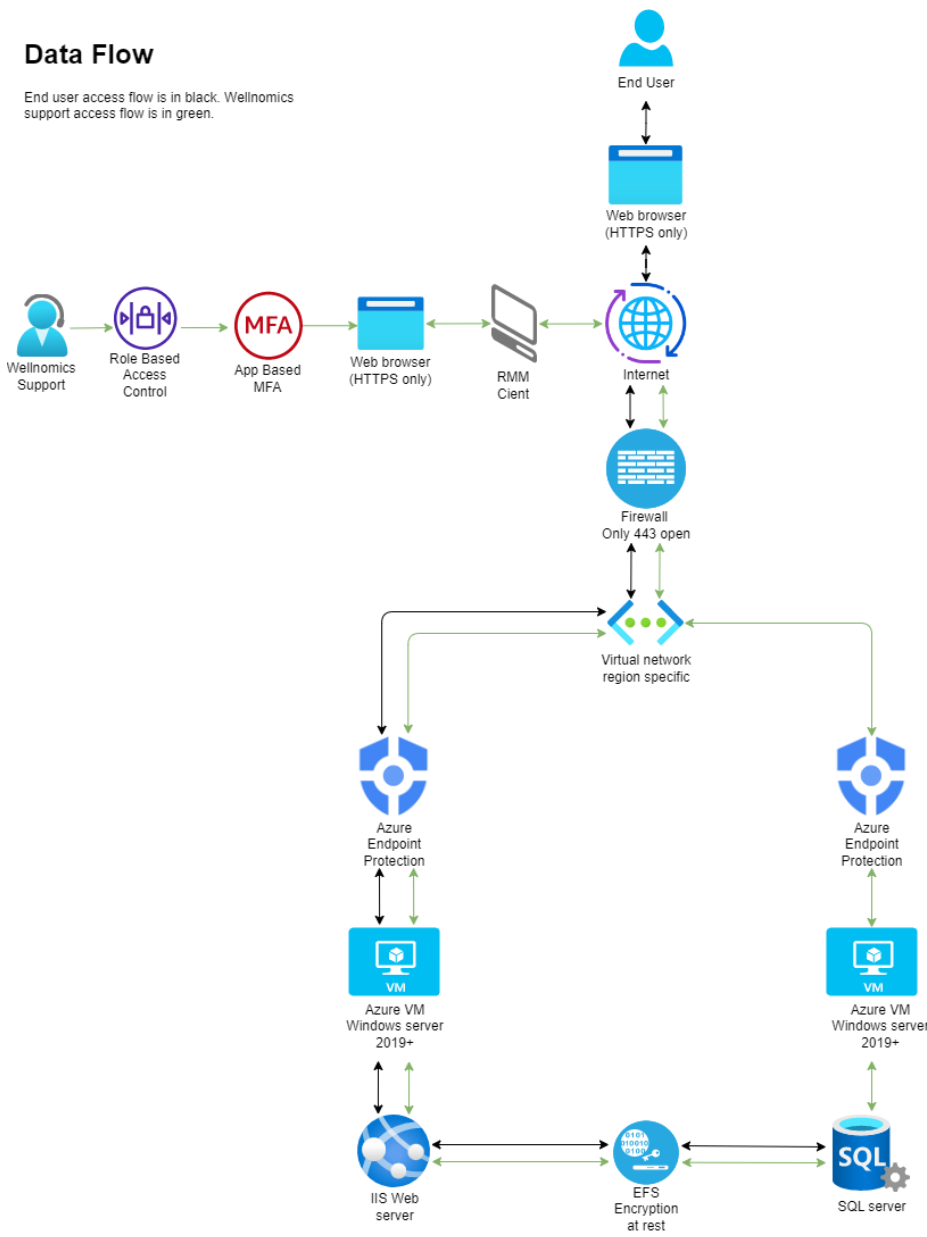
## Access to Hosted Systems

Hosted servers each contain a number of Wellnomics hosted systems. These include client (production) systems along with trial, evaluation and demonstration systems. In all cases, connection to the web interfaces that allow access through usernames and password are via secure https connections. For this reason, all ports on the firewalls that protect the hosted servers are closed *with the exception of port 80* (http), *port 443* (https). Note that port 80 is only open for one purpose - to allow redirection of http requests to a secure https connection. For example, port 80 is used to allow us to redirect any customer typing "http://www.wellnomicsonline.com" into their browser to "https://www.wellnomicsonline.com".

For more detail on hosted server and systems access see [WELLNOMICS INFORMATION SECURITY POLICY](#) Sections 4.2 - **Logical Access - Role Specific Responsibilities for Internal Wellnomics IT Infrastructure and Systems** and also the document [User Management Policy](#) Section 6. Section 6 of the [User Management Policy](#) is subject to monthly review as recorded in the [Authorizations Review Record](#). See also the [Mobile Devices Policy](#)

### Data Flow

End user access flow is in black. Wellnomics support access flow is in green.



## Physical Security - Hosted servers (Microsoft controlled premises - Azure)

Microsoft hosted servers are subject to the terms and conditions set out in the Service Level Agreement that Microsoft has with Wellnomics. Following is a summary of the physical security measures that Microsoft has in place for hosted servers:-

## Physical security of data center

The Microsoft data centers hosting the Wellnomics solutions are fully certified and independently audited. They are secured by card key access and continual surveillance. Specific security initiatives include:

- Staffed 24x7x365 with separate security lobby. Electronic security features with card key access
- Data centre access limited to Microsoft approved personnel
- Security camera monitoring at all data centre locations. CCTV archived video. Alarm systems
- Unmarked facilities with confidential physical addresses (restricted to authorized Microsoft Azure personnel).
- NARC – Network monitoring software
- Eaton Foreseer Facility Management System

## Fire protection

The data center has a state-of-the-art, fire detection and fire suppression system, and uses fully redundant, enterprise-class fire protection equipment, specifically:-

- Early Smoke Detection (VESDA) and Carbon Smoke Detection systems
- Pre-action Dual-interlock Sprinkler Systems

## Power and air conditioning protection

Preventative and protective systems include:-

- HVAC Systems with N+2 Redundancy, CRAH:N+20% Redundancy.
- Generators – N+2 redundancy
- Conditioned power provides all servers with uninterrupted power supply (UPS).

## Physical Security - Wellnomics access to Hosted servers

Wellnomics has in place the following physical security measures around the way its staff access and manage the hosted servers:-

- The Wellnomics building is occupied during normal office hours and all visitors must sign in and be accompanied at all times whilst in the building
- The reception area is staffed at all time during the working day ("normal office hours")
- Outside normal office hours the building is alarmed with a system that can detect intruders and the alarm is monitored 24/7

## Hosted Server Access and RMM

- Hosted servers are accessed via a highly secure RMM (Remote Management & Monitoring) service
- All activities within the RMM service are logged and stored in both a secure cloud and a local back-up.
- The RMM connection and data are protected via a proprietary protocol, AES-256 encryption algorithm, and cloud instances are secured with an encrypted SSL certificate.
- Staff access is controlled with Role-Based Access control so only approved staff can access the RMM service
- Staff access is further controlled with App based multi-factor authentication
- Access to the RMM is further restricted to specific IP addresses
- All RMM connection sessions are limited to a session timer. If that timer is met, Staff must re-authenticate to create a new session.
- The RMM service prevents brute force attacks by logging all failed authentication attempts, including the IP, and blocks the attacking IP after a specified number of failed attempts.

## Compliance and Measurement

All staff must sign a [Information Security Policy Acknowledgment and Agreement Form \(Staff & Contractors\)](#) acknowledging their responsibilities under the various policies and procedures that relate to data protection and privacy and privacy. In signing such an agreement staff :-

- have received training in aspects of Wellnomics policies and procedures as they relate to data privacy and confidentiality
- have understood their responsibilities under the various policies and procedures as they relate to data privacy and confidentiality
- undertake to ensure complacence with the Wellnomics policies and procedures as they relate to data privacy and confidentiality
- agree to comply with any checks or audits carried out under the relevant policies and procedures as they relate to data privacy and confidentiality

The Wellnomics team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Wellnomics Management Team team in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

- [User Management - Employees & Contractors - Policy](#)
- [Authorizations Review Record](#)
- [Information Security Policy Acknowledgment and Agreement - Employees & Contractors - Template](#)
- [Security & Privacy Training - Employees & Contractors - Records](#)
- [Management of Hosting - Policy](#)
- [Access Security - Internal security, Employees & Contractors - Policy](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
16 May 2017	Wayne Owens, Principal Consultant	Created - updated to new format	15 May 2018 <a href="#">Wayne Owens (Unlicensed)</a>
22 Nov 2017	Kevin Taylor, CEO	Added port 80 to list of open ports on server and explanation of restricted use of this port	20 Nov 2018 <a href="#">Chris MacKay (Deactivated)</a>
21 Nov 2018	Chris MacKay	Reviewed, no changes made	<ul style="list-style-type: none"> <li>• 21 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
13 Mar 2019	Wayne Owens	Reviewed, no changes made	<ul style="list-style-type: none"> <li>• <a href="#">Chris MacKay (Deactivated)</a></li> </ul>

19 May 2020	Wayne Owens	Reviewed and updated	21 May 2021 <ul style="list-style-type: none"> <li>Chris MacKay (Deactivated)</li> </ul>
17 Aug 2020	Angeli Arino	Reviewed, no changes made	
20 Dec 2020	Kevin	Split out from Access Security Policy - Internal	<ul style="list-style-type: none"> <li>20 Dec 2021 Ian Bartram</li> </ul>
20 Dec 2021	Ian Bartram	Reviewed - no changes required	<ul style="list-style-type: none"> <li>26 Jan 2023 Ian Bartram</li> </ul>
26 Jan 2023	Ian Bartram	Updated access standards to include RMM and remote access. Added flowchart of end user and support data flows.	<ul style="list-style-type: none"> <li>15 Feb 2024 Ian Bartram</li> </ul>



# Threat Modeling - Hosting - Policy

**Review period:** Annual

Threat Modeling is defined on the OWASP site here [https://owasp.org/www-community/Application\\_Threat\\_Modeling](https://owasp.org/www-community/Application_Threat_Modeling).

Wellnomics performs threat modeling on hosted servers using architecture diagrams that identify data flows and interfaces.

The [Microsoft Threat Modelling tool](#) may be used to build a threat model. This tool helps to identify areas of risk for further analysis.

## Requirements for updating threat models

A threat model must be maintained and reviewed annually, or updated whenever a relevant change is made to the data flows, interfaces or security methods on hosted servers. For example, moving to a new server provide or architecture, changing the methods used to remotely access the servers, or changing the software tools used or user authentication methods.

A documented and up-to-date diagram and/or table must be maintained in Hosting documentation showing:

- Interfaces
- Data flow diagram
- Data classifications (types of data) involved in each part
- Data at rest (storage)
- Data in transit

The threat models must be reviewed every 12 months to ensure its still current, and updated where needed.

## Policy Compliance

### Compliance Measurement

A copy of the threat model and analysis will be saved as part of our completed evidence. Jira will be used to track changes that are identified as needing to be made and used to verify these changes/updates have been implemented in future releases. An annual review conducted by the current Privacy Office will verify that the processes have been followed and up-to-date evidence of such has been provided and saved in the correct locations.

### Exceptions

Any exception to the policy must be approved by the Wellnomics management team, in advance.

## Related Standards, Policies, Processes and Forms

- [Threat Modeling - Hosting - Documentation](#) (will supersede "Access security to server and data - server security model" in [Product Security and Best Practice - SaaS - Guidelines](#))
- [Threat Modelling - App - Documentation](#)
- [Threat Modelling - SaaS - Documentation](#)
- See also "Access security to server and data - server security model" and "Database access security & data flow" in [Product Security and Best Practice - SaaS - Guidelines](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
----------------	-------------	-------------------	--------------------

20 Dec 2020	<a href="#">Kevin</a>	Created policy	<ul style="list-style-type: none"> <li>• 20 Dec 2021 <a href="#">Ian Bartram</a></li> </ul>
13 Dec 2021	Ian Bartram	Updated with links to new docs in policy	<ul style="list-style-type: none"> <li>• 12 Dec 2022 <a href="#">Ian Bartram</a></li> </ul>
13 Dec 2022	Ian Bartram	Updated with links to new docs in policy	<ul style="list-style-type: none"> <li>• 12 Dec 2023 <a href="#">Ian Bartram</a></li> </ul>

# Disaster Recovery and Business Continuity - Hosting - Policy

## Information Technology statement of intent

These documents delineate our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms. These documents summarize our recommended procedures. In the event of an actual emergency situation, modifications to These documents may be made to ensure physical safety of our people, our systems, and our data. Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

## Policy Statement

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan. The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be reviewed and tested every 6 months.

## Objective

The principal objective of the disaster recovery program is to develop, test, and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- Disaster recovery capabilities as applicable to key customers, vendors and others

## Recovery Objectives

**Recovery Point Objective (RPO)** is **24 hours** (i.e. the maximum period of data that could be lost since last backup).

**Recovery Time Objective (RTO)** is **48 hours** (i.e. the maximum period of time within which the system is recovered after a disaster).

## Related documentation

[Disaster Recovery and Business Continuity - Hosting - Guide](#)

## Glossary

- DRT - Disaster Recovery Team
- Business critical - Systems, hardware, and software required for minimal business operation
- Business Continuity - plans deal with difficult situations, so the organization can continue to function with as little disruption as possible.
- Timeline - Expected time period of resolution from the time the DRT are aware of the Incident

Date of Change	Responsible	Summary of Change	Next Revision date
06 Jun 2022	Ian Bartram	New document established	<ul style="list-style-type: none"> <li>• 05 Dec 2022 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	Ian Bartram	Separated some information into guides.	<ul style="list-style-type: none"> <li>• 29 Feb 2024 <a href="#">Ian Bartram</a></li> </ul>

# INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Policies

- Risk Assessment - Internal - Policy
- Incident Management Process - Policy
- Disaster Recovery and Business Continuity - Internal - Policy
- User Management - Employees & Contractors - Policy
- Passwords and Encryption - Employees & Contractors - Policy
- Access Security - Internal security, Employees & Contractors - Policy
- Clean Desk - Employees & Contractors - Policy
- Equipment De-Commissioning - Policy
- Firewall - Internal Security - Policy
- Mobile Devices - Employees & Contractors - Policy
- Change Management - Internal Processes - Policy
- Wireless Communication - Employees & Contractors - Policy
- Wireless Communication Standard
- Anti-Bribery & Corruption - Employees & Contractors - Policy
- Ethics - Employees & Contractors - Policy
- Email - Employees & Contractors - Policy
- Acceptable Use - Employees & Contractors - Policy
- Remote Access - Employees & Contractors - Policy
- Home Working - Employees & Contractors - Policy
- IT Requests - Employees & Contractors

# Risk Assessment - Internal - Policy

**Review period:** Annual

## Overview

In order to objectively evaluate the risk to the Wellnomics business that may result from failures in Wellnomics systems relating to:-

- technical infrastructure, including but not limited to:-
  - reliability of technical assets
  - control of access
- protection of data (from damage, accidental deletion, unauthorized access etc.) including but not limited to:
  - risks associated with unauthorized access or intrusion causing data damage e.g. viruses, malware, ransomware etc.
  - failure of backup systems (either capture or retrieval)

Wellnomics Ltd will carry out a periodic and objective risk assessment

## Purpose

To minimize business disruption and to protect the security and privacy of Wellnomics data and software and customer data stored either internally or on Wellnomics managed hosted servers

## Scope

Covers all Wellnomics systems and personnel and all activities relating to the management of customer systems and data held on hosted servers. Note that all customer data is classified as "sensitive personal data" and all risk assessments will be conducted and completed with this in mind

## Risk Assessment Policy

- The Wellnomics management team, through the Principal Consultant, undertakes to carry out a periodic risk assessment
- The risk assessment will be carried out at least annually, and more frequently in the event of any substantial changes to operations, staff or equipment.
- The form of the risk assessment will be as that defined in Section 5 below
- Completed risk assessments will contain a list of follow up actions (if any) along with recommendations for changes to relevant operations or procedures necessary to mitigate any identified risk.
- Completed risk assessments will be stored in the following location : [Risk Assessments - Completed](#)
- 5 Risk Assessment Form

## The Form

The form specified in 5.3 below will be used for periodic risk assessments as required under 4.1 above. This form may be amended from time to time. Any amended forms will be reflected in 5.2 below and will be used as soon as they are committed to this Policy

## Guidance on the Completion of the Risk Assessment Form

The form requires an objective assessment of 2 criteria, namely

1. the probability of an event occurring (Low, Average or High), and secondly,
2. the impact of the event should it arise (Low Average or High).

These criteria should be independently assessed for each of the areas identified in the risk assessment. Once they have been assessed, their relative risks can be looked up using the following table:-

**Classification:**

**PROBABILITY**

<b>High</b>	3	2	4
<b>Average</b>	1	2	3
<b>Low</b>	1	1	2
	<b>Low</b>	<b>Average</b>	<b>High</b>

**IMPACT**

Any event that scores 3 or more for risk (based on the above look up table) need to be identified and comments must be made on follow up actions or considerations. Follow up actions must be viewed, approved and acknowledged as completed by the CEO before any risk assessment can be marked as complete.

## The Risk Assessment Form

See [Risk Assessment Template](#)

## Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Wellnomics' network:

- [IT Acceptable Use Policy](#)
- [Password and Encryption Policy](#)
- [Password Construction Guidelines](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
September 2016	Wayne Owens, Principal Consultant	Converted to new format	15 Sep 2017 <a href="#">Wayne Owens (Unlicensed)</a>
12 Sep 2017	Wayne Owens	Reviewed, no significant changes made	11 Sep 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay, Support Consultant	Reviewed, no changes made	<ul style="list-style-type: none"> <li>• 05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
20 May 2020	<a href="#">Chris MacKay (Deactivated)</a>	Reviewed, no significant changes made	<ul style="list-style-type: none"> <li>• 20 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>

24 Aug 2020	Angeli Arino	Converted to new format	<ul style="list-style-type: none"> <li>24 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
16 Dec 2021	<a href="#">Ian Bartram</a>	Reviewed, no changes needed	<ul style="list-style-type: none"> <li>26 Jan 2023 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	<a href="#">Ian Bartram</a>	Reviewed, no changes needed	<ul style="list-style-type: none"> <li>26 Jan 2024 <a href="#">Ian Bartram</a></li> </ul>



# Incident Management Process - Policy

**Review period:** At least Annual, or as required

## Background

In any organization incidents may occur that have the potential to negatively impact products, services, standards and customer expectations. It is Wellnomics aim to identify such incidents when they occur and to record, document and investigate the causes of such incidents with the aim of identifying any and all contributing factors. The aim of such a process is to determine what changes may be necessary to prevent recurrence of such incidents in the future

## Scope

This Incident Management Process is intended to cover the following Wellnomics activities and processes:-

- Software Development
- Internal IT infrastructure
- The management and maintenance of hosted servers
- The management and maintenance of demonstration systems

NB Also see [Customer Services Interactions - Policy](#) for incidents identified as part of the customer support process. Such incidents, once identified, will become subject to this policy

The information processed and held by the Wellnomics client software and related database is limited to name, work email address and, in the event that the Discomfort assessment is used, health information.

Also See [Data Classification - Policy](#)

## Policy

### Definitions

The definition of what constitutes an incident includes, but is not limited to, the following:

- Data breach - the unauthorized access to, or unauthorized disclosure of personal information/data, or a loss of personal information/data.
- Loss, corruption or unauthorized copying or dissemination of personal data. Personal data includes but is not limited to:-
  - Financial details e.g. credit card numbers, transaction history, credit reports etc.
  - Tax identification information
  - Identity information e.g. passport details, driver license details etc.
  - Contact information e.g. home address, phone number, email addresses etc.
  - Health information
  - Other sensitive information e.g. sexual orientation, political or religious views.

Note that of the above, the information processed and held by the Wellnomics client software and related database is limited to name, work email address and, in the event that the Discomfort assessment is used, some limited health information.

- an event that resulted in system downtime in excess of 30 minutes - internal systems. In this context, systems include internal servers, virtual machines (VMs), networks (whether in part or whole), remote access portals, wireless access points.
- Unauthorized access to internal systems or data holding employee data (see definition of "Data Breach")
- Unauthorized amendment or deletion of internal data or systems holding employee data (see definition of "Data Breach")

- Unauthorized access to externally hosted systems or data (see definition of “Data Breach”)
- Abuse of Wellnomics equipment, systems or data
- Theft of Wellnomics equipment or data, or the use of Wellnomics equipment or data to facilitate theft of equipment or data.
- Non-compliance with published Wellnomics policies and procedures
- Download and use of unauthorized software/application.
- Suspicious behavior or circumstances that has the potential to damage or delete company data or to allow unauthorized access to company data.

## Exclusions

The following events are specifically excluded from this incident report policy:

External causes (the responsibility of 3rd parties and for which Wellnomics has no direct control) resulting in:-

- unavailability of 3rd party systems including telephone and internet

## Process

- Any incident that comes within the scope of this process shall be recorded using the form - [Incident Investigation Form](#). This notification to be completed and brought to the attention of the Chief Executive at the earliest opportunity and with no delay.
- Once notified, the Chief executive will take immediate responsibility for the subsequent investigation and identification of remedial action. This responsibility may be delegated to a specified person who in the opinion of the Chief Executive is best suited to carrying out an investigation (in normal circumstances the Wellnomics Data Security Officer) and identifying remedial action. Notwithstanding any delegation, the ultimate responsibility for ensuring that any qualifying incident is recorded, investigated and concluded through the identification of remedial action (if any) rests with the Chief Executive (see section “INVESTIGATION” below)
- In the event that an incident relates to the loss, deletion or unauthorized access to employee data, the Chief Executive will be required to notify Staff as soon as possible, but within 24 hours of the incident being identified by Wellnomics.
- In the event that an incident relates to the loss, deletion or unauthorized access to customer data the Chief Executive will be required to notify all affected customers as soon as possible, but within 24 hours of the incident being identified by Wellnomics
- If required, the Chief Executive will require the Wellnomics Data Security Officer to: -
  - fully understand the nature of the incident and the data affected and to identify the nature and cause of the incident.
  - the steps taken (or planned to be taken) to isolate the incident and prevent any further unauthorized data access or loss.
  - identify the impact of the incident and the steps to be taken to restore and/or protect normal business activities.
  - Where there is a legal requirement for Wellnomics to notify relevant authorities of a data breach (as defined in relevant privacy legislation) the Chief Executive will do so.
- Notifications - in the event that the incident is criminal in nature or involves other agencies (other than the data privacy agencies referenced above), it will be for the Chief Executive to determine which agencies need to be notified and the extent of the information that shall be shared with the relevant agencies.

## Investigation

The Wellnomics Chief Executive takes the lead role in any incident investigation. In doing so, and subject to the nature and extent of the incident will

- determine the required resources necessary to investigate the incident and bring it to the speediest conclusion.
- prioritize the incident, in terms of the resources necessary to bring it to the speediest conclusion.
- determine whether there is a necessity to isolate or shut down affected servers and/or systems
- determine whether affected customers need to be notified and the required details of the notification
- the steps taken (or planned to be taken) to isolate the incident and prevent any further unauthorized data access or loss
- identify the impact of the incident and the steps to be taken to restore and/or protect normal business activities

- to agree with the customer any communications or public notifications of the incident. In this context "public" communication relates to any sharing of data or information relating to an incident to parties other than Wellnomics and the customers nominated contacts (see below for notifications to "relevant authorities under privacy legislation).
- Share with affected customers relevant information relating to:-
  - the facts and circumstances of the Data Breach;
  - the likelihood that the Data Breach will result in serious harm to individuals affected by the Data Breach; and
  - whether Customer has any notification obligations (or other obligations) under Law as a result of the Data Breach (see next point)
- Where there is a legal requirement for Wellnomics to notify relevant authorities of a data breach (as defined in relevant privacy legislation) Wellnomics will seek the approval of affected customers prior to such a notification being made. It will be Wellnomics' expectation that the affected customer will, in writing, approve the communication with the relevant authorities, and such approval shall not be unreasonable withheld. Notwithstanding this, it is Wellnomics' understanding that the duty to inform any relevant regulatory authorities rests with:-
  - Under GDPR for UK and EU based customers, this is the the "Data Controller" which will be the Wellnomics customer),
  - Under the Office of the Australian Information Commissioner (OAIC) this is the "organization (customer) or agent (Wellnomics). In such circumstances Wellnomics will devolve the reporting duty to the customer.
  - For the US, there is no single (federal) data breach notification law. At the time of this policy revision all 50 states have varying data breach notification laws not all of which include notification requirements. For US based customers Wellnomics will liaise with affected customers to determine and execute any local notification requirements.
  - For all other jurisdictions, Wellnomics will liaise with affected customers to determine and execute any local notification requirements.
- Share with the customer the results of any investigation including causes, remedies and ongoing monitoring and/or control processes added to prevent future recurrence
- Notifications - in the even that the incident is criminal in nature or involves other agencies (other than the data privacy agencies referenced above), it will be for the Chief Executive to determine which agencies need to be notified and the extent of the information that shall be shared with the relevant agencies. Permission (in writing) will be sought from customers where customer data or details are part of the notification information.

## Policy Compliance

### Compliance Measurement

The Wellnomics Management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### Exceptions

Any exception to the policy must be approved by the Wellnomics Management team in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

[Incident Investigation Form](#)

[Customer Services Interactions - Policy](#)

[Incident Investigation Form - Internal - Template](#)

[Data Classification - Policy](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision due
Created 18 Jan 2017	Wayne Owens, Principal Consultant	New policy document created	<a href="#">Wayne Owens (Unlicensed)</a> 18 Dec 2017
18 May 2017	Kevin Taylor CEO	Reviewed, only, minor grammar changes only	21 May 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay, Support Consultant	Reviewed, no changes	<ul style="list-style-type: none"> <li>05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
27 Nov 2019	Wayne Owens	Reviewed, no changes	<ul style="list-style-type: none"> <li>30 Nov 2020 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
21 Nov 2019	Chris Mackay	Reviewed, no changes	<ul style="list-style-type: none"> <li>12 Nov 2020 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
31 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"> <li>31 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
25 Aug 2021	Wayne Owens	Updated to cover data breaches specifically and also notifications in the event of data breaches	<ul style="list-style-type: none"> <li>25 Aug 2022 <a href="#">Corinne</a></li> </ul>
26 Jan 2023	Corinne Wright	Updated links to relevant pages and grammar spelling updates.	
27 Feb 2023	Wayne Owens	Amended to consolidate multiple polices relating to "incidents" into a single document	<ul style="list-style-type: none"> <li>25 Jan 2024 <a href="#">Corinne</a></li> </ul>

# Disaster Recovery and Business Continuity - Internal - Policy

## Information Technology statement of intent

These documents delineate our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms. These documents summarize our recommended procedures. In the event of an actual emergency situation, modifications to These documents may be made to ensure physical safety of our people, our systems, and our data. Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

## Policy Statement

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan. The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be updated and tested every 6 months

## Objective

The principal objective of the disaster recovery program is to develop, test, and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- Disaster recovery capabilities as applicable to key customers, vendors and others

## Glossary

- DRT - Disaster Recovery Team
- Business critical - Systems, hardware, and software required for minimal business operation
- Business Continuity - plans deal with difficult situations, so the organization can continue to function with as little disruption as possible.
- Timeline - Expected time period of resolution from the time the DRT are aware of the Incident

Date of Change	Responsible	Summary of Change	Next Revision date
----------------	-------------	-------------------	--------------------

06 Jun 2022	Ian Bartram	New document established	<ul style="list-style-type: none"><li>• 05 Dec 2022 <a href="#">Ian Bartram</a></li></ul>
26 Jan 2023	Ian Bartram	Separated some information into guides.	<ul style="list-style-type: none"><li>• 29 Feb 2024 <a href="#">Ian Bartram</a></li></ul>

# User Management - Employees & Contractors - Policy

**Review period:** Annual

NB Some of the information for this document was extracted from the main policy document ([WELLNOMICS INFORMATION SECURITY POLICY1](#)) and created in this document effective from April 2017.

## Overview

This policy covers the granting and reviewing of user rights in terms of access to Wellnomics internal systems and access to systems that Wellnomics host (on Microsoft Azure servers) on behalf of customers. Under this policy the agreed access rights are reviewed on a monthly basis and roles and rights amended in the event of any material changes to access rights requirements

## Purpose

The purpose of this policy is to ensure that Wellnomics staff only have access to those systems and that data that they require access to, to enable them to discharge their responsibilities effectively. The effect of this is that each system and each employee is evaluated on an individual basis and not on a generic basis and employees can only access systems they need to and that systems are only accessible to those users that have a need to access them.

## Scope

This policy applies to all Wellnomics personnel (including all permanent employees and any third parties who may from time to time be contracted to provide a specific services ). It also applies to all internal systems and data and also to externally hosted customer data (hosted on Microsoft Azure servers globally), collectively referred to as "*designated systems*"

## Policy

### General Requirements

- Users will be registered as users within this document and will only be provided access to designated systems on an "as needs" basis.
- Even if granted access to a designated system, access will be limited to the role(s) required to enable the users to fulfill whatever duties they may have on a system, nothing more (the basis of least privilege).
- Each designated system has an identified "system administrator". It will be the duty of each system administrator to review all system updates for a system to determine if there are any implications for roles and access to amend a users access if it becomes prudent to do so.
- For each designated system, User accounts will be review on monthly basis and any changes made in the Authorization Matrix (below).
- Where user access is based on a username and password, the users password must be changed at a frequency in accordance with the [Password and Encryption Policy](#). Where a system allows for enforced password changes, the system administrator will ensure that this is enabled where possible.
- The registering of users and the granting of the various permissions, as they apply to roles and individuals, will be the at the discretion of the Wellnomics CEO and recorded in this document which will be reviewed and updated on a monthly basis and a record of such reviews and any required amendments or revisions will be recorded in recorded in the [Authorizations Review Record](#)
- User privileges and access may be revised, suspended or revoked in the following circumstances:-
  - user leaves the employment of Wellnomics **Action:** all access privileges to be permanently revoked)
  - user is under suspension or being investigated for gross misconduct. **Action:** all access privileges suspended pending outcome

- change of user role requiring reduced access privileges. Action: amend/restrict access privileges as appropriate
- When an employee leaves the [Employee Leaving Checklist - Template](#) must be completed to verify that all rights and roles are correctly revoked and any access rights or responsibilities are correctly reassigned.

## Policy Compliance

### Compliance Measurement

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### Exceptions

Any exception to the policy must be approved by the Wellnomics management team in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## The Authorization Matrix for User Access Rights to Internal and Hosted Systems

Roles Matrix and Permissions 1 - Wellnomics hosted systems and hosted environments. Internal roles to be checked on a monthly basis and updated as required below. The record of reviews to be kept in [Authorizations Review Record](#)

Group			Wellnomics Client App		Wellnomics SaaS				Hosted Servers			
Location	Role	Person (as at 03/06/2021)	Wellnomics App in hosted system *	User management	Group Risk Scores *	Individual Risk Scores *	Individual Risk Scores *	individual Statistics *	Installation	Testing	Commissioning	Ongoing Server Management
Internal NZ	Senior Support Consultant	<a href="#">Corinne</a>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Internal NZ	Support and QA Engineer	<a href="#">Ian Bartram</a>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Internal NZ	Principal Consultant	Wayne Owens	Y	Y	Y	Y	Y	Y		Y		Y
Internal NZ	CEO	Kevin Taylor	Y	Y	Y	Y	Y	Y				
Internal NL	IT Consultant	Martin van Emmerik	Y							Y - NL servers only		
Internal NL	Country Manager	Karin Verhoeven	Y							Y - NL servers only		
Internal AUS	Country Manager	Stephen Gardner	Y	Y								
Customer	End User		Y	Y		Y	Y	Y				
Customer	Manager/Supervisor					? **	? **	? **				
Customer	Wellnomics Local Administrator					? **	? **	? **				



Customer	Wellnomics Administrator					? **	? **	? **				
Customer	Wellnomics IT Administrator					? **	? **	? **				
			** For client to decide									
			* Wellnomics staff access to this data only with the permission of the client									

## Roles Matrix and Permissions 1 - Wellnomics internal systems

Designated System	System Administrator(s)	System Users (no admin access)
Xero - financial system	Gail Whitnall	Gail Whitnall, Kevin Taylor,
Confluence	Matthew Holland	All staff are end users
JIRA	Matthew Holland	All staff are end users
Freshdesk	<a href="#">Ian Bartram</a> <a href="#">Corinne</a>	<a href="#">Wayne Owens</a> <a href="#">Ian Bartram</a> <a href="#">Corinne</a>
HubSpot	<a href="#">Corinne</a> <a href="#">Ian Bartram</a>	Gail Whitnall, Wayne Owens
MS Dynamics CRM	Kevin Taylor, Wayne Owens,	Kevin Taylor, Wayne Owens, Karin Verhoeven, Gail Whitnall, Stephen Gardner
MS Outlook	<a href="#">Ian Bartram</a>	All staff are end users
Hosted Servers - Management	<a href="#">Matt</a> <a href="#">Ian Bartram</a>	None

## Related Standards, Policies and Processes

- [Password Construction Guidelines](#)
- [Password and Encryption Policy](#)
- [Authorizations Review Record](#)
- [Employee Leaving Checklist - Template](#)

## Definitions and Terms

None

## Revision History

Date of change	Responsible	Summary of change	Date of next revision
Created 10 Apr 2017	Wayne Owens, Principal Consultant	Created this document. Removed some parts from  <a href="#">WELLNOMICS INFORMATION SECURITY POLICY</a>	13 Apr 2018 <a href="#">Wayne Owens (Unlicensed)</a>
28 Aug 2017	Wayne Owens	Removed references to Anna T Taylor who left Wellnomics employment effective from 25/8/17	24 Aug 2018
30 Nov 2017	Wayne Owens	Removed references to Tony Galbraith who left in November 2017 and replaced by Chris Mackay	26 Nov 2018 <a href="#">Chris MacKay (Deactivated)</a>

05 Nov 2018	Chris MacKay, Support Consultant	Reviewed, no changes made	<ul style="list-style-type: none"> <li>05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
05 May 2020	Wayne Owens	Reviewed and updated due to changed staff permissions	<ul style="list-style-type: none"> <li>07 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
17 Aug 2020	Angeli Arino	Reviewed and update due to changed staff permissions	<ul style="list-style-type: none"> <li>17 Aug 2021 <a href="#">Angeli Arino (Deactivated)</a></li> </ul>
03 Jun 2021	Wayne Owens	Updated to reflect staff changes	<ul style="list-style-type: none"> <li>03 Jun 2022 <a href="#">Corinne</a></li> </ul>
17 May 2022	Corinne	Review and updated due to changed staff permissions	<ul style="list-style-type: none"> <li>05 Jun 2023 <a href="#">Corinne</a></li> </ul>
31 May 2023	Corinne	Reviewed and no changes required	<ul style="list-style-type: none"> <li>05 Jun 2024 <a href="#">Corinne</a></li> </ul>

# Passwords and Encryption - Employees & Contractors - Policy

**Review period:** Annual

## Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Wellnomics resources. All users, including contractors and vendors with access to Wellnomics systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

## Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

## Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Wellnomics facility, has access to the Wellnomics network, or stores any non-public Wellnomics information. This includes mobile devices such as phones, tablets and similar that are provided for use by Wellnomics Ltd or otherwise used for Wellnomics approved

## Policy

### Password Creation

- All user-level and system-level passwords must conform to the [Password Security - Employees & Contractors - Guidelines](#)
- Users must not use the same password for Wellnomics accounts as for other non-Wellnomics access (for example, personal ISP account, option trading, benefits, and so on).
- Where possible, users must not use the same password for various Wellnomics access needs.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges.
- All service accounts and passwords must be stored in the company password manager in the appropriate collection.

### Password Change

- All passwords associated with the management of hosted servers must be changed on at least a quarterly basis (90 days)
- Password cracking or guessing may be performed on a periodic or random basis by the Wellnomics management Team or its delegates. If a password is guessed or cracked during one of these scans, user will be required to change it to be in compliance with the [Password Security - Employees & Contractors - Guidelines](#)
- Password history is enforced - 3 previously used passwords are stored and any new password must not match any of the 3 previously used.

### Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential Wellnomics information, and stored in the Company Password Manager.

- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not share Wellnomics passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Do not use the "Remember Password" feature of applications (for example, web browsers) *this is disabled via policy for Chrome, Edge, Firefox, and Brave.*
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

## Password Storage

- All Passwords are to be stored securely in the company Password Manager.
- Password Access is to be controlled in a compartmentalized manner; the least access possible should be shared
- All password access, changes, and events are tracked in the company password manger Event logs

## Application Development

Application developers must ensure that all Application Software being developed contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

## Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The\*?#>\*@TrafficOnThe101Was\*&!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

## Policy Compliance

### Compliance Measurement

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### Exceptions

Any exception to the policy must be approved by the Wellnomics management team in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

- [Password Security - Employees & Contractors - Guidelines](#)

## Definitions and Terms

None

## Revision History

Date of change	Responsible	Summary of change	Date of next revision
6th December 2015	Wayne Owens, Principal Consultant	Updated and converted to new format.	December 2016
12 Jun 2017	Wayne Owens, Principal Consultant	Checked and revised, updated	12 Jun 2018 <a href="#">Chris MacKay (Deactivated)</a>
10 May 2018	Chris MacKay, Support Consultant	Revised Password Guidelines	<ul style="list-style-type: none"> <li>• Update Password Policy 10 May 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
20 May 2020	<a href="#">Chris MacKay (Deactivated)</a>	Reviewed, no changes required	<ul style="list-style-type: none"> <li>• 20 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
24 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"> <li>• 24 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
01 Dec 2020	Ian Bartram	Reviewed, updated to include Password Manager	<ul style="list-style-type: none"> <li>• 01 Dec 2022 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	Ian Bartram	Reviewed, updated to include password manager + passphrase changes	<ul style="list-style-type: none"> <li>• 31 Jan 2024 <a href="#">Ian Bartram</a></li> </ul>

# Access Security - Internal security, Employees & Contractors - Policy

**Last updated:** 19 May 2020

**Review Period:** Annual

## Overview

Wellnomics as a company has a variety of servers and systems that are secured using physical and logical security measures. This document describes the various methods used under each category. All staff are made aware of these measures and their responsibilities under these measures and training is provided to staff both on enrollment and on a regular basis (annually) thereafter.

In addition to the Wellnomics premises where staff are housed along with the equipment/tools of software development (PCs, laptops, server, routers etc.)

Note there is a separate access security policy covering hosting - see [Access Security - Hosting - Policy](#)

## Purpose

The purpose of this policy is to set out the requirements and form of the access security measures in place at Wellnomics Ltd as it applies to both its internal systems and environment and the hosted environments sources through Microsoft Ltd.

## Policy

### Logical security

**Workstations** - all workstations on the Wellnomics network are protected by usernames and passwords. Passwords must comply with the [Password and Encryption Policy](#) and the [Password Construction Guidelines](#). In addition, all workstations automatically log out (and require log in again before next use) after 10 minutes of no activity.

**Internal Servers** - all servers on the Wellnomics network are protected by usernames and passwords. Passwords must comply with the [Password and Encryption Policy](#) and the [Password Construction Guidelines](#). Only those that require access to specific servers are provided with user accounts.

### Physical security - Wellnomics controlled premises

Wellnomics based in Christchurch, New Zealand, the Netherlands and Australia has a number of physical security measures in place to protect its environment, including but not limited to:-

- Locked and secured external doors
- Secured and alarmed building with out of hours monitoring service
- Controlled visitor access. All visitors must sign in on entry and be accompanied at all times whilst on the premises. Visitors to sign out on leaving
- Physically secured server and router components, allowing access by authorized staff only.
- Smoke and fire detectors / alarm systems

## Policy Compliance

## Compliance and Measurement

All staff must sign a [Information Security Policy Acknowledgment and Agreement Form \(Staff & Contractors\)](#) acknowledging their responsibilities under the various policies and procedures that relate to data protection and privacy and privacy. In signing such an agreement staff :-

- have received training in aspects of Wellnomics policies and procedures as they relate to data privacy and confidentiality
- have understood their responsibilities under the various policies and procedures as they relate to data privacy and confidentiality
- undertake to ensure complacence with the Wellnomics policies and procedures as they relate to data privacy and confidentiality
- agree to comply with any checks or audits carried out under the relevant policies and procedures as they relate to data privacy and confidentiality

The Wellnomics team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Wellnomics Management Team team in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

- [User Management - Employees & Contractors - Policy](#)
- [Authorizations Review Record](#)
- [Information Security Policy Acknowledgment and Agreement Form \(Staff & Contractors\)](#)
- [Staff Training Materials on Security & Privacy](#)
- [Staff Training Record - Data and Systems Security and Privacy](#)
- [Management of Hosting - Policy](#)
- [Access Security - Hosting - Policy](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
16 May 2017	Wayne Owens, Principal Consultant	Created - updated to new format	15 May 2018 <a href="#">Wayne Owens (Unlicensed)</a>
22 Nov 2017	Kevin Taylor, CEO	Added port 80 to list of open ports on server and explanation of restricted use of this port	20 Nov 2018 <a href="#">Chris MacKay (Deactivated)</a>
21 Nov 2018	Chris MacKay	Reviewed, no changes made	<ul style="list-style-type: none"><li>• 21 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li></ul>

13 Mar 2019	Wayne Owens	Reviewed, no changes made	16 Mar 2020 <ul style="list-style-type: none"> <li>• <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
19 May 2020	Wayne Owens	Reviewed and updated	21 May 2021 <ul style="list-style-type: none"> <li>• <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
17 Aug 2020	Angeli Arino	Reviewed, no changes made	
20 Dec 2020	<a href="#">Kevin</a>	Split out hosting policy	<ul style="list-style-type: none"> <li>• 17 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
01 Dec 2021	<a href="#">Ian Bartram</a>	Reviewed, no changes made	<ul style="list-style-type: none"> <li>• 26 Jan 2023 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	<a href="#">Ian Bartram</a>	Reviewed, no changes made	<ul style="list-style-type: none"> <li>• 26 Jan 2024 <a href="#">Ian Bartram</a></li> </ul>



# Clean Desk - Employees & Contractors - Policy

**Review period:** Annual

## Overview

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user's workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase an employee's awareness about protecting sensitive information.

## Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant (for the future), but it is also part of standard basic privacy controls.

## Scope

This policy applies to all Wellnomics employees and affiliates.

## Policy

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the work day.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

## Policy Compliance

## Compliance Measurement

The Wellnomics team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Wellnomics management team in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

None.

## Definitions and Terms

None.

## Revision History

Date of change	Responsible	Summary of change	Next revision date
6th December 2015	Wayne Owens, Principal Consultant	Updated and converted to new format	6th December 2016
13 Dec 2016	Wayne Owens, Principal Consultant	checked - no updates required	05 Dec 2017
12 Dec 2017	Wayne Owens, Principal Consultant	checked - no updates required	05 Dec 2018 <a href="#">Chris MacKay (Deactivated)</a>
21 Nov 2018	Chris MacKay	Checked, no updates needed	<ul style="list-style-type: none"> <li>21 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
19 May 2020	Chris Mackay	Checked, no updates required	<ul style="list-style-type: none"> <li>19 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
18 Aug 2020	Angeli Arino	Reviewed, changes made as required	<ul style="list-style-type: none"> <li>18 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
01 Dec 2021	Ian Bartram	Reviewed, changes made as required	<ul style="list-style-type: none"> <li>26 Jan 2023 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	Ian Bartram	Reviewed, changes made as required	<ul style="list-style-type: none"> <li>08 Feb 2024 <a href="#">Ian Bartram</a></li> </ul>

# Equipment De-Commissioning - Policy

**Review period:** Annual

## Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Wellnomics data, some of which is considered sensitive. In order to protect our and our customer's data, all storage mediums must be properly erased before being disposed of. Simply deleting or re-formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

## Purpose

The purpose of this policy is to define the guidelines for the disposal of technology equipment and components owned by Wellnomics or for which Wellnomics is otherwise responsible.

## Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within Wellnomics including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, CD's, DVD's floppy disks, portable storage devices (i.e., USB drives), backup drives.

All Wellnomics employees and affiliates must comply with this policy.

## Policy

### Technology Equipment Disposal

- When Technology assets have reached the end of their useful life they should be sent to the IT office for proper disposal. The [Equipment De-commissioning Form](#) must be completed prior to submission to IT.
- IT will securely erase all storage mediums in accordance with current industry best practices.
- All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk of the machine with zero-filled blocks, meeting Department of Defence standards.
- All electronic drives must be de-gaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
- Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.
- IT will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.
- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

## Policy Compliance

### Compliance Measurement

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Wellnomics management team, in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies, Processes and Forms

<b>Related</b>
<a href="#">Equipment De-Commissioning Forms</a>
<a href="#">Completed Equipment Decommissioning Forms</a>

## Revision History

Date of change	Responsible	Summary of change	Next revision date
July 2016	Wayne Owens, Principal Consultant	Converted to new format	20 Jul 2017 <a href="#">Wayne Owens (Unlicensed)</a>
07 Jul 2017	Wayne Owens	Checked for up to date - all OK no changes needed	09 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay	Reviewed, no changes made	<ul style="list-style-type: none"> <li>05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
04 May 2020	Chris Mackay	Reviewed, no changes required	<ul style="list-style-type: none"> <li>03 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
18 Aug 2020	Angeli Arino	Reviewed, no changes required	<ul style="list-style-type: none"> <li>18 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
01 Dec 2021	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"> <li>26 Jan 2023 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"> <li>15 Feb 2024 <a href="#">Ian Bartram</a></li> </ul>



# Firewall - Internal Security - Policy

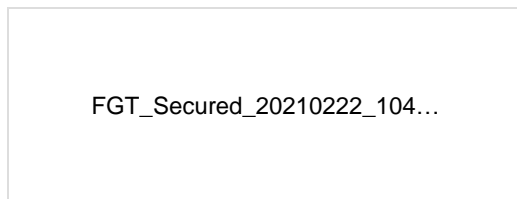
**Review period:** Annual

Wellnomics uses a Fortinet Fortigate 50E Firewall NGFW (Next Generation Firewall)

This is configured to allow only white-listed (approved) sites to be accessed from the internal Wellnomics network. It also prevents unauthorized access to the Wellnomics network from external sites and locations.

All relevant software updates are applied automatically

Firewall Settings - Settings as as last update are included in the Config file below:-

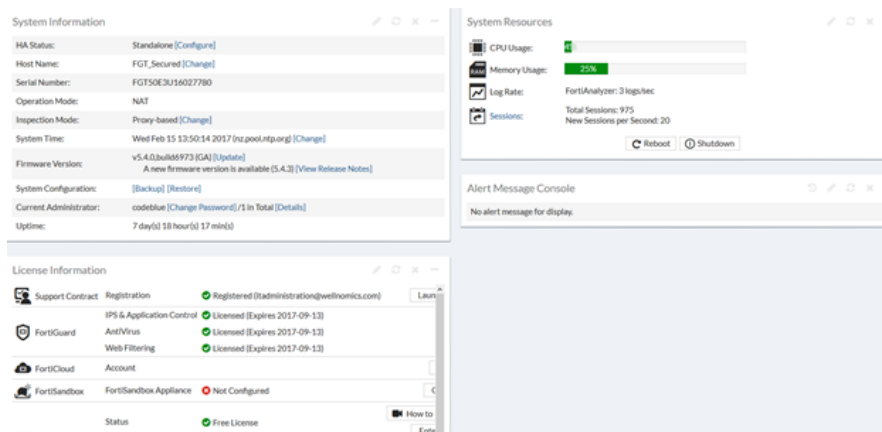


## Update records

Records are added when we find possible issues.

Firewall firmware is updated regularly as we find it safe to do so.

Firewall is kept licensed to help with security profiles.



## Permitted sites, white lists etc.

All trusted sites are available.

No specific websites blocked.

## Revision History

Date of change	Responsible	Summary of change	Next revision date
6th December 2015	Wayne Owens, Principal Consultant	Document created	6th December 2016
08 May 2017	Wayne Owens, Principal Consultant	Document updated	07 May 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay. Support Consultant	Added updated list of Firewall Settings	<ul style="list-style-type: none"> <li>05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
06 May 2020	Chris MacKay. Support Consultant	Updated to reflect new settings	<ul style="list-style-type: none"> <li>06 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
20 Aug 2020	Angeli Arino,	Reviewed, no change required	<ul style="list-style-type: none"> <li>23 Mar 2023 <a href="#">Ian Bartram</a></li> </ul>
23 Mar 2023	Ian Bartram	Reviewed, no change required	<ul style="list-style-type: none"> <li>22 Mar 2024 <a href="#">Ian Bartram</a></li> </ul>

# Mobile Devices - Employees & Contractors - Policy

**Review period:** Annual

## Overview

With advances in computer technology, mobile computing and storage devices have become useful tools to meet the business needs at Wellnomics. These devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily portable and can be used anywhere. As mobile computing becomes more widely used, it is necessary to address security to protect information resources at Wellnomics.

## Purpose

The purpose of this policy is to establish an authorized method for controlling mobile computing and storage devices that contain or access information resources at Wellnomics.

## Scope

Employees, consultants, vendors, contractors, and others who use mobile computing and storage devices on the network at Wellnomics.

## Policy

### *General Policy*

- It is the policy of Wellnomics that mobile computing and storage devices containing or accessing the information resources at Wellnomics must be approved prior to connecting to the information systems at Wellnomics. This pertains to all devices connecting to the network at Wellnomics, regardless of ownership.
- Mobile computing and storage devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), plug-ins, Universal Serial Bus (USB) port devices, CDs, DVDs, flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or company owned, that may connect to or access the information systems at Wellnomics. IT will maintain a list of approved mobile computing and storage devices ([see Asset Register](#)). By definition, any equipment leased, purchased or otherwise provided directly by Wellnomics will be approved for use.
- Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network at Wellnomics. These risks must be mitigated to acceptable levels. Note that it should be the default position that NO information or data that is deemed to be confidential shall be stored on portable devices or on mediums other than those that reside inside the Wellnomics network.
- Portable computing devices and portable electronic storage media must not contain confidential, personal, or sensitive information. Unless written approval has been obtained from the CEO (must be exceptional circumstances), databases or portions thereof, which reside on the network at Wellnomics or on external Wellnomics servers, shall not be downloaded to mobile computing or storage devices. If data is downloaded it must be stored in an encrypted form and the device e.g. laptop, or media e.g. portable drive must be protected with a secure password.
- Mobile phones - mobile phones must be protected via a passcode. On Apple iPhone devices the creation and use of a passcode automatically encrypts all data on the phone. For Android devices, encryption is a configurable application and must be so configured if a Wellnomics supplied phone. When configuring an Android device removable media (the phones memory card) must also be covered by the encryption process.

## Procedures



To report lost or stolen mobile computing and storage devices it will be necessary to complete the *Wellnomics Data Incident Notification, Investigation and Report Form*.

## Roles & Responsibilities

Users of mobile computing and storage devices must actively protect such devices from loss of equipment and disclosure of private information belonging to or maintained by Wellnomics. Before connecting a mobile computing or storage device to the network at Wellnomics, users must ensure it is on the list of approved devices issued by IT ([See Asset Register](#)) which lists all approved devices).

The Wellnomics management team is responsible for the mobile device policy at Wellnomics.

## Removable media

Because of the nature of the way in which Wellnomics operates, there should be no circumstances where data considered "confidential" should leave the Wellnomics premises on any physical devices e.g. thumb drives, removable media etc.

## Encryption

Any devices that hold data that can be considered as "confidential" and thereby covered by the [Privacy Policy](#) must be locked from casual access (with passwords, passkeys etc.) and if the device is to leave the Wellnomics premises, the data on the devices must be encrypted.

The only exception to the above restriction on removable media is a work mobile phone which may hold emails the contents of which are regarded as confidential. For this reason, mobile phones must:-

- be protected by a passcode
- be configured so that the stored data is encrypted.

For users of iPhones, the creation and use of a passcode automatically triggers the encryption of any data on the phone. Users of Android phones will need to configure their phones for encryption as shown in <https://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/>

## Policy Compliance

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, network monitoring, internal and external audits.

## Exceptions

Any exception to the policy must be approved by the Wellnomics management team.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Wellnomics' network:

[IT Acceptable Use Policy](#)

# Revision History

Date of change	Responsible	Summary of change	Next revision date
June 2016	Wayne Owens, Principal Consultant	Updated and converted to new format.	June 2017
03 May 2017	Wayne Owens	Updated to cover encryption of phones	07 May 2018 <a href="#">Wayne Owens (Unlicensed)</a>
15 Jun 2017	Wayne Owens	Reviewed - no changes required	18 Jun 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay	Reviewed, no changes made	05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a>
4 Mar 2019	Kevin Taylor	Made section on removable media clearer	05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a>
20 May 2020	Wayne Owens	Reviewed, no changes required	<ul style="list-style-type: none"> <li>20 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
24 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"> <li>24 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
15 Dec 2021	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"> <li>15 Dec 2022 <a href="#">@Corinne</a></li> </ul>
17 May 2022	Corinne Wright	Reviewed, no changes required	<ul style="list-style-type: none"> <li>17 May 2023 <a href="#">@Corinne</a></li> </ul>
21 Jun 2023	Corinne Wright	Reviewed, no changes required	<ul style="list-style-type: none"> <li>20 Jun 2024 <a href="#">@Corinne</a></li> </ul>

# Change Management - Internal Processes - Policy

**Review period:** Annual

## Background, Definitions and Roles

Wellnomics, as an effective software development company, can only maintain its efficiency and success if all staff understand the process and systems that contribute to its success. Where possible these key systems are documented and communicated to all new staff as part of the staff induction process. Changes to existing systems may be required as a result of a number of factors e.g.

- a required change in the process or system
- changing technology (hardware and software)
- changing staff and/or staff skills
- an identified improvement to an existing process or system
- any change that has implications for time, cost or deliverable dates

Therefore, whilst there may be a number of reasons to change an existing system or process such a change must not be implemented without following the processes set out in this document.

## Definitions

- **Change:** The addition, modification or removal of approved or supported hardware, network, software (excluding the Wellnomics software products), application, environment, system, desktop build or associated documentation. A request for change is submitted in the form of a **Change Request**
- **Change Advisory Board:** A group of people who can give expert advice to change management on the implementation of changes. This Board is likely to be made up of representatives from all areas within IT and representatives from business units.
- **Change control:** The procedure to ensure that all changes are controlled, including the submission, analysis, decision making, approval, implementation and post implementation of the change.
- **Change history:** Auditable information that records, for example, what was done, when it was done, by whom and why.
- **Change management** - is the process of controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption. Request for Change (RFC) Form or screen used to record details of a request for a change to any Change Implementer (CI) within an infrastructure or to procedures and items associated with the infrastructure.

## Roles

- **The Change Manager and Deputies**

The role of the Change Manager in the change process is to authorise/approve minor, low risk changes. The Change Manager will also convene the CAB to discuss the higher risk changes, where appropriate, and make the decision either to implement or reject the change. The Change Manager also ensures that all activities to implement the change are undertaken in an appropriate manner and are documented and reviewed when completed.

For Wellnomics Ltd:

Change Manager is Kevin Taylor, CEO

Deputy Change Manager is Wayne Owens, Principal Consultant

- **Change Initiators** - Anyone within Wellnomics can initiate a change with a general requirement that only relevant and appropriate changes are raised.
- **The Change Advisory Board** - The Change Advisory Board is a group called together by the Change Manager to act in an advisory capacity to the Change Manager to all changes that are categorized as significant or major. They also authorize changes in these categories. The CAB is made up of individuals within or outside Wellnomics Ltd who are relevant in the making the decisions on whether a change should be authorized. They are called together as required in order to ensure that changes are progress in a prompt and efficient manner.
- **The CAB/EC** - The Emergency Change Advisory Board (ECAB) is a group called together by the Change Manager to act as decision makers on ALL changes that are categorized as emergency. This group usually meet virtually as the nature of emergency change means that it has been be agreed and authorized immediately. The ECAB is made up of high level individuals who are relevant in the making the decisions on whether a change should take place immediately as an emergency or if it should be delayed and given an alternative category.
- **The Change Implementer** - a person charged by the CAB to implement any agreed change
- **The Change Tester** - a person charged by the CAB to test the implemented change (this person cannot also be the Change Implementer)

## Scope

This process does not cover the Wellnomics software development process where specific systems are used to manage change (e.g. Atlassian JIRA). It covers all other process and systems at Wellnomics.

## Process

The process flow for a change request is as follows:-

**Step 1** - Change Initiator generates Change Request using the [Change Request Form](#) and forwards to Change Manager.

**Step 2** - The Change Manager enters the Change Request in the [Change Management Log](#) . The status of the Change Request is updated as necessary as the process proceeds

**Step 3** - The Change Request is evaluated by the Change Manager who must discuss the proposed change with at least one other nominated person (normally the Deputy Change Manager). It may be sufficient for the change to approved, amended or declined solely on the basis of the evaluation by the Change Manager and the Deputy Change Manager, or other nominated person.

**Step 4** - if, in the opinion of the Change Manager, the proposed change requires wider evaluation and discussion, the Change Manager may convene a Change Advisory Board meeting which must include either the Change Manager or the Deputy Change Manager and may include any other person that the Change Manager deems appropriate having consideration for the nature and scope of the change request.

**Step 5** - Whether the evaluation of the Change Request is concluded at Step 3 or 4 above, The Change Manager (or Deputy) will document the decision in relation to the change, and if the change is accepted, in full or in part, will also document:-

- the action required to implement the change
- the person responsible for implementing the change (the Change Implementer)
- the person responsible for testing that the change has been implemented in accordance with the requirements/actions
- Sign off the change as completed

## Documentation

All change request must be submitted using the [Change Request Form](#)

All received Change requests must be entered onto the [Change Management Log](#)

## Policy Compliance

### Compliance Measurement

The Wellnomics Management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### Exceptions

Any exception to the policy must be approved by the Wellnomics Management team in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

None.

## Definitions and Terms

See section 1 above

## Revision and Update History

Date of change	Responsible	Summary of change	Next revision due
11 Jul 2017 (created)	Wayne Owens, Principal Consultant	Created new process	16 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay, Support Consultant	Validated Process	<ul style="list-style-type: none"><li>05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li></ul>
20 May 2020	<a href="#">Chris MacKay (Deactivated)</a>	Reviewed, no changes required	<ul style="list-style-type: none"><li>20 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li></ul>
24 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"><li>24 Aug 2021 <a href="#">Ian Bartram</a></li></ul>
15 Dec 2021	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"><li>26 Jan 2023 <a href="#">Ian Bartram</a></li></ul>
26 Jan 2023	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"><li>26 Jan 2024 <a href="#">Ian Bartram</a></li></ul>



# Wireless Communication - Employees & Contractors - Policy

**Review period:** Annual

## Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

## Purpose

The purpose of this policy is to secure and protect the information assets owned by Wellnomics Ltd. Wellnomics Ltd provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Wellnomics grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to Wellnomics' network. Only **those** wireless infrastructure devices that meet the standards **specified in** this policy or are approved for connectivity to a the Wellnomics network.

## Scope

All employees, contractors, consultants, temporary and other workers at Wellnomics, including all personnel affiliated with third parties must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to the Wellnomics network. This applies to all endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

## Policy

### General Requirements

All wireless infrastructure devices that reside at a Wellnomics site and connect to a Wellnomics network, or provide access to information classified as Wellnomics Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by Wellnomics.
- Use Wellnomics approved authentication protocols and infrastructure.
- Use Wellnomics approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.

### Guest Network

- Wellnomics provides a wireless access point (**WellnomicsGuest**) for guests that require internet access. This access point (being on its own independent domain) is isolated from the Wellnomics corporate network (**WellnomicsWIFI**). In no circumstances should Wellnomics Guests be allowed to access the corporate wireless access point which. is subject to the requirements of 4.1 above.

### Home Wireless Device Requirements

- Wireless infrastructure devices that provide direct access to the Wellnomics corporate network, must conform to the Home Wireless Device Requirements as detailed in the [Wireless Communication Standard](#)
- Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the Wellnomics corporate network. Access to the Wellnomics corporate network through this device must use standard remote access authentication.

## Policy Compliance

### Compliance Measurement

The Wellnomics Management Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### Exceptions

Any exception to the policy must be approved by the Wellnomics Management Team in advance in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

- [Wireless Communication Standard](#)
- [Password and Encryption Policy](#)
- [Password Construction Guidelines](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
June 2016	Wayne Owens, Principal Consultant	Updated and converted to new format.	June 2017
12 Jun 2017	Wayne Owens, Principal Consultant	Checked - no updates required	06 Jun 2018
05 Nov 2018	Chris MacKay, Support Consultant	Reviewed, no changes made	<ul style="list-style-type: none"> <li>• 05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
20 May 2020	Wayne Owens, Principal Consultant	Checked - no updates required	<ul style="list-style-type: none"> <li>• 20 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
24 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"> <li>• 24 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
01 Dec 2020	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"> <li>• 01 Dec 2022 <a href="#">Ian Bartram</a></li> </ul>



26 Jan 2023	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"><li>• 01 Feb 2024 <a href="#">Ian Bartram</a></li></ul>
-------------	-------------	-------------------------------	---

# Wireless Communication Standard

**Review period:** Annual

## Overview

See Purpose.

## Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to the Wellnomics network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the Wellnomics Management Team are approved for connectivity to the Wellnomics network.

**Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by a Wellnomics Management Team approved individual or support organization.**

## Scope

All employees, contractors, consultants, temporary and other workers at Wellnomics and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of Wellnomics, must comply with this standard. This standard applies to wireless devices that make a connection the network and all wireless infrastructure devices that provide wireless connectivity to the network.

## Standard

### General Requirements

All wireless infrastructure devices that connect to the Wellnomics network or provide access to must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- It is not envisaged that Bluetooth connections will need to be made to the Wellnomics network. In the event that such a connection is required express approval must be sought from the Wellnomics Management Team. Any Bluetooth devices that are permitted to connect to the Wellnomics Network must use Secure Simple Pairing with encryption enabled.

### Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to the Wellnomics network, such as that need to access Wellnomics information outside normal office hours, must:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

# Policy Compliance

## Compliance Measurement

Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Wellnomics Management Team in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

- [Wireless Communication Policy](#)
- [Password and Encryption Policy](#)
- [Password Construction Guidelines](#)
- [Mobile Devices Policy](#)

## Definitions and Terms

None

## Revision History

Date of change	Responsible	Summary of change	Next revision date
June 2016	Wayne Owens, Principal Consultant	Updated and converted to new format.	June 2017
12 Jun 2017	Wayne Owens, Principal Consultant	Updated to cover new wireless access point	12 Jun 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay, Support Consultant	Reviewed, no changes made	<ul style="list-style-type: none"><li>• 05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li></ul>
20 May 2020	Wayne Owens, Principal Consultant	Updated to cover new wireless access point	<ul style="list-style-type: none"><li>• 20 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li></ul>
24 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"><li>• 24 Aug 2021 <a href="#">Ian Bartram</a></li></ul>
01 Dec 2020	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"><li>• 26 Jan 2023 <a href="#">Ian Bartram</a></li></ul>
26 Jan 2023	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"><li>• 01 Feb 2024 <a href="#">Ian Bartram</a></li></ul>



# Anti-Bribery & Corruption - Employees & Contractors - Policy

**Review period:** Annual

## Purpose

The purpose of this policy is to establish controls to ensure compliance with all applicable anti-bribery and corruption regulations, and to ensure that the Company's business is conducted in a socially responsible manner.

## Policy statement

Bribery is the offering, promising, giving, accepting or soliciting of an advantage as an inducement for action which is illegal or a breach of trust. A bribe is an inducement or reward offered, promised or provided in order to gain any commercial, contractual, regulatory or personal advantage.

It is our policy to conduct all of our business in an honest and ethical manner. We take a zero-tolerance approach to bribery and corruption. We are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate and implementing and enforcing effective systems to counter bribery.

We will uphold all laws relevant to countering bribery and corruption in all the jurisdictions in which we operate.

## Scope

### Who is covered by the policy?

In this policy, **third party** means any individual or organisation you come into contact with during the course of your work for us, and includes actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisors, representatives and officials, politicians and political parties.

This policy applies to all individuals working at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with us, or any of our subsidiaries or their employees, wherever located (collectively referred to as **employees** in this policy).

This policy covers:

- Bribes;
- Gifts and hospitality;
- Facilitation payments;
- Political contributions;
- Charitable contributions.

## Bribes

Employees must not engage in any form of bribery, either directly or through any third party (such as an agent or distributor). Specifically, employees must not bribe a foreign public official anywhere in the world.

## Gifts and hospitality

Employees must not offer or give any gift or hospitality:

- which could be regarded as illegal or improper, or which violates the recipient's policies; or
- to any public employee or government officials or representatives, or politicians or political parties; or
- which exceeds USD100 in value for each individual gift or USD500 in value for each hospitality event (not to exceed a total value of USD1000 in any financial year), unless approved in writing by the employee's manager.

Employees may not accept any gift or hospitality from our business partners if:

- it exceeds USD50 in value for each individual gift or USD100 in value for each hospitality event (not to exceed a total of USD200 in any financial year), unless approved in writing by the employee's manager; or
- it is in cash; or
- there is any suggestion that a return favour will be expected or implied.

Where a manager's approval is required above, if the manager is below Director level then approval must be sought from an appropriate Director.

If it is not appropriate to decline the offer of a gift, the gift may be accepted, provided it is then declared to the employee's manager and donated to charity.

We appreciate that the practice of giving business gifts varies between countries and regions and what may be normal and acceptable in one region may not be in another. The test to be applied is whether in all the circumstances the gift or hospitality is reasonable and justifiable. The intention behind the gift should always be considered.

Within these parameters, local management may define specific guidelines and policies to reflect local professional and industry standards. Where this policy requires written approval to be given, the Managing Director shall put in place a process to maintain a register of all such approvals.

## Facilitation payments and kickbacks

Facilitation payments are a form of bribery made for the purpose of expediting or facilitating the performance of a public official for a routine governmental action, and not to obtain or retain business or any improper business advantage. Facilitation payments tend to be demanded by low level officials to obtain a level of service which one would normally be entitled to.

Our strict policy is that facilitation payments must not be paid. We recognise, however, that our employees may be faced with situations where there is a risk to the personal security of an employee or his/her family and where a facilitation payment is unavoidable, in which case the following steps must be taken:

- Keep any amount to the minimum;
- Create a record concerning the payment; and
- Report it to your line manager.

In order to achieve our aim of not making any facilitation payments, each business of the Company will keep a record of all payments made, which must be reported to the Managing Director, in order to evaluate the business risk and to develop a strategy to minimise such payments in the future.

## Political Contributions

We do not make donations, whether in cash or kind, in support of any political parties or candidates, as this can be perceived as an attempt to gain an improper business advantage.

## Charitable contributions

Charitable support and donations are acceptable (and indeed are encouraged), whether of in-kind services, knowledge, time, or direct financial contributions. However, employees must be careful to ensure that charitable contributions are not used as a scheme to conceal bribery. We only make charitable donations that are legal and ethical under local laws and practices]. No donation must be offered or made without the prior approval of [the compliance manager].

All charitable contributions should be publicly disclosed.

## Your responsibilities

You must ensure that you read, understand and comply with this policy.

The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for us or under our control. All employees are required to avoid any activity that might lead to, or suggest, a breach of this policy.

You must notify your manager **OR** the Managing Director or the confidential helpline as soon as possible if you believe or suspect that a conflict with or breach of this policy has occurred, or may occur in the future.

Any employee who breaches this policy will face disciplinary action, which could result in dismissal for gross misconduct. We reserve our right to terminate our contractual relationship with other workers if they breach this policy.

## Record-keeping

We must keep financial records and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

You must declare and keep a written record of all hospitality or gifts accepted or offered, which will be subject to managerial review.

You must ensure all expenses claims relating to hospitality, gifts or expenses incurred to third parties are submitted in accordance with our expenses policy and specifically record the reason for the expenditure.

All accounts, invoices, memoranda and other documents and records relating to dealings with third parties, such as clients, suppliers and business contacts, should be prepared and maintained with strict accuracy and completeness. No accounts must be kept "off-book" to facilitate or conceal improper payments.

## How to raise a concern

You are encouraged to raise concerns about any issue or suspicion of malpractice at the earliest possible stage. If you are unsure whether a particular act constitutes bribery or corruption, or if you have any other queries or concerns, these should be raised with your line manager **OR** the Managing Director or through the confidential helpline.

## What to do if you are a victim of bribery or corruption

It is important that you tell the Managing Director or the confidential helpline as soon as possible if you are offered a bribe by a third party, are asked to make one, suspect that this may happen in the future, or believe that you are a victim of another form of unlawful activity.

## Protection

Employees who refuse to accept or offer a bribe, or those who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions. We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

We are committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or other corruption offence has taken place, or may take place in the future. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform [the compliance manager] immediately. If the matter is not remedied, and you are an employee, you should raise it formally using the company's Grievance Procedure.

# Training and communication

Training on this policy forms part of the induction process for all new employees. All existing employees will receive regular, relevant training on how to implement and adhere to this policy. In addition, all employees will be asked to formally accept conformance to this policy on an annual basis.

Our zero-tolerance approach to bribery and corruption must be communicated to all suppliers, contractors and business partners at the outset of our business relationship with them and as appropriate thereafter.

## Who is responsible for the policy?

The board of directors has overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it.

The Managing Director has primary and day-to-day responsibility for implementing this policy, and for monitoring its use and effectiveness and dealing with any queries on its interpretation. Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this policy and are given adequate and regular training on it.

## Policy Compliance

### Compliance Measurement

The CEO will monitor the effectiveness and review the implementation of this policy, regularly considering its suitability, adequacy and effectiveness. Any improvements identified will be made as soon as possible. Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in countering bribery and corruption.

All employees are responsible for the success of this policy and should ensure they use it to disclose any suspected danger or wrongdoing.

Employees are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to the Managing Director.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Revision History

Date of Change	Responsible	Summary of change	Next revision date
08 Nov 2020	Kevin Taylor	Added from existing company policy	• 08 Nov 2021 <a href="#">Ian Bartram</a>
16 Nov 2021	Corinne Wright	No changes required	• 16 Dec 2022 <a href="#">Corinne</a>
26 Jan 2023	Corinne Wright	Reviewed, no changes required	• 26 Jan 2024 <a href="#">Corinne</a>





# Ethics - Employees & Contractors - Policy

**Review period:** Annual

## Overview

Wellnomics is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When Wellnomics addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

Wellnomics will not tolerate any wrongdoing or impropriety at any time. Wellnomics will take the appropriate measures to act quickly in correcting the issue if the ethical code is broken.

## Purpose

The purpose of this policy is to establish a culture of openness, trust and to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct. Effective ethics is a team effort involving the participation and support of every Wellnomics employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

## Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Wellnomics, including all personnel affiliated with third parties.

## Policy

### Executive Commitment to Ethics

- Senior leaders and executives within Wellnomics must set a prime example. In any business practice, honesty and integrity must be top priority for executives.
- Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.
- Executives must disclose any conflict of interests regard their position within Wellnomics.

### 4.2 Employee Commitment to Ethics

- Wellnomics employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.
- Every employee needs to apply effort and intelligence in maintaining ethics value.
- Employees must disclose any conflict of interests regard their position within Wellnomics.
- Employees will help Wellnomics to increase customer and vendor satisfaction by providing quality products and timely response to inquiries.
- Employees should consider the following questions to themselves when any behavior is questionable:
  - Is the behavior legal?
  - Does the behavior comply with all appropriate Wellnomics policies?
  - Does the behavior reflect Wellnomics values and culture?
  - Could the behavior adversely affect company stakeholders?
  - Would you feel personally concerned if the behavior appeared in a news headline?
  - Could the behavior adversely affect Wellnomics if all employees did it?

## Company Awareness

- Promotion of ethical conduct within interpersonal communications of employees will be rewarded.
- Wellnomics will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

## Maintaining Ethical Practices

- Wellnomics will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.
- Employees at Wellnomics should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.
- Wellnomics has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

## Unethical Behavior

- Wellnomics will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.
- Wellnomics will not tolerate harassment or discrimination.
- Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.
- Wellnomics will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.
- Wellnomics employees will not use corporate assets or business relationships for personal use or gain.

## Policy Compliance

### Compliance Measurement

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback.

### Exceptions

None.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

- [Anti-Bribery & Corruption - Employees & Contractors - Policy](#)

## Definitions and Terms

None.

## Revision History

Date of Change	Responsible	Summary of change	Next revision date
August 2016	Wayne Owens, Principal Consultant	Updated and converted to new format.	16 Aug 2017 <a href="#">Wayne Owens (Unlicensed)</a>
04 Aug 2017	Wayne Owens	None	08 Aug 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay	Reviewed, no changes made	<ul style="list-style-type: none"> <li>05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
01 May 2020	Chris Mackay	Reviewed, no changes required	<ul style="list-style-type: none"> <li>03 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
18 Aug 2020	Angeli Arino	Reviewed, no changes required	<ul style="list-style-type: none"> <li>18 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
01 Dec 2021	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"> <li>26 Jan 2023 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"> <li>26 Jan 2024 <a href="#">Ian Bartram</a></li> </ul>

# Email - Employees & Contractors - Policy

**Review period:** Annual

## Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

## Purpose

The purpose of this email policy is to ensure the proper use of Wellnomics email system and make users aware of what Wellnomics deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within Wellnomics Network.

## Scope

This policy covers appropriate use of any email sent from a Wellnomics email address and applies to all employees, vendors, and agents operating on behalf of Wellnomics Ltd.

## Policy

1. All use of email must be consistent with Wellnomics policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
2. Wellnomics email accounts should be used primarily for Wellnomics business-related purposes; personal communication is permitted on a limited basis, but non Wellnomics related commercial uses are prohibited.
3. All Wellnomics data contained within an email message or an attachment must be secured according to the *Data Protection Standard*.
4. Email should be retained only if it qualifies as a Wellnomics business record. Email is a Wellnomics business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
5. Email that is identified as a Wellnomics business record shall be retained according to Wellnomics *Record Retention Schedule*.
6. The Wellnomics email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Wellnomics employee should report the matter to their supervisor immediately.
7. Users are prohibited from automatically forwarding Wellnomics email to a third party email system (noted in 4.8 below). Individual messages which are forwarded by the user must not contain Wellnomics confidential or above information.
8. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Wellnomics business, to create or memorialize any binding transactions, or to store or retain email on behalf of Wellnomics. Such communications and transactions should be conducted through proper channels using Wellnomics-approved documentation.
9. Using a reasonable amount of Wellnomics resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Wellnomics email account is prohibited.
10. Wellnomics employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
11. Wellnomics may monitor messages without prior notice. Wellnomics is not obliged to monitor email messages.

## Policy Compliance

## Compliance Measurement

The Wellnomics Management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Wellnomics Management team in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

None.

## Definitions and Terms

None.

## Revision History

Date of change	Responsible	Summary of change	Next revision due
12 Dec 2015	Wayne Owens, Principal Consultant	Updated and converted to new format.	December 2016
05 Dec 2016	Wayne Owens, Principal Consultant	checked for changes - none	10 Dec 2017
18 Dec 2018	Wayne Owens, Principal Consultant	checked for changes - none	<ul style="list-style-type: none"><li>18 Dec 2019 <a href="#">Chris MacKay (Deactivated)</a></li></ul>
19 May 2020	Wayne Owens	Reviewed and checked, no changes required	<ul style="list-style-type: none"><li>21 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li></ul>
18 Aug 2020	Angeli Arino	Reviewed, no change required	<ul style="list-style-type: none"><li>01 Dec 2021 <a href="#">Ian Bartram</a></li></ul>
01 Dec 2021	Ian Bartram	Reviewed, no change required	<ul style="list-style-type: none"><li>26 Jan 2023 <a href="#">Ian Bartram</a></li></ul>
26 Jan 2023	Ian Bartram	Reviewed, no change required	<ul style="list-style-type: none"><li>08 Feb 2024 <a href="#">Ian Bartram</a></li></ul>

# Acceptable Use - Employees & Contractors - Policy

**Review frequency:** Annual

## Overview

Wellnomics' intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Wellnomics' established culture of openness, trust and integrity. Wellnomics is committed to protecting Wellnomics' employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Wellnomics. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Wellnomics employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

## Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Wellnomics. These rules are in place to protect the employee, Wellnomics as a company and its customers. Inappropriate use exposes Wellnomics to risks including virus attacks, compromise of network systems and services, and legal issues.

## Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Wellnomics business or interact with internal networks and business systems, whether owned or leased by Wellnomics, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Wellnomics and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Wellnomics policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Wellnomics, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Wellnomics.

## Policy

### General Use and Ownership

- Wellnomics proprietary information stored on electronic and computing devices whether owned or leased by Wellnomics, the employee or a third party, remains the sole property of Wellnomics. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard*.
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Wellnomics proprietary information.
- You may access, use or share Wellnomics proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the

absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

- For security and network maintenance purposes, authorized individuals within Wellnomics may monitor equipment, systems and network traffic at any time.
- Wellnomics reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

## Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must be approved by Wellnomics as suitable for use. By default, all equipment leased, purchase or otherwise supplied by Wellnomics is so approved.
- System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- Postings by employees from a Wellnomics email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Wellnomics, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

## Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Wellnomics authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Wellnomics-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

### Systems, Network and Software

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Wellnomics. See also [Software Register](#) under IT Section in Confluence.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Wellnomics or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting Wellnomics business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Wellnomics computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Wellnomics account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited.



12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the Wellnomics network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Wellnomics employees to parties outside Wellnomics.

## Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Wellnomics' networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Wellnomics or connected via Wellnomics' network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

## Blogging and Social Media

1. Blogging by employees, whether using Wellnomics's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Wellnomics's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Wellnomics's policy, is not detrimental to Wellnomics's best interests, and does not interfere with an employee's regular work duties. Blogging from Wellnomics's systems is also subject to monitoring.
2. Wellnomics's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Wellnomics and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any similar conduct.
4. Employees may also not attribute personal statements, opinions or beliefs to Wellnomics when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Wellnomics. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Wellnomics's trademarks, logos and any other Wellnomics intellectual property may also not be used in connection with any blogging activity

# Policy Compliance

## Compliance Measurement

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Wellnomics management team in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Related Standards, Policies and Processes

- [Password Security - Employees & Contractors - Guidelines](#)
- [Ethics - Employees & Contractors - Policy](#)
- [Anti-Bribery & Corruption - Employees & Contractors - Policy](#)

## Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:

<https://www.sans.org/security-resources/glossary-of-terms/>

- Blogging
- Honeypot
- HoneyNet
- Proprietary Information
- Spam

## Revision History

Date of change	Responsible	Summary of change	Next revision date
	Wayne Owens, Principal Consultant	Updated and converted to new format	6th December 2016
10 Dec 2016	Wayne Owens	Updated minor details, no significant changes required	12 Dec 2017 <a href="#">Wayne Owens (Unlicensed)</a>
05 Dec 2017	Wayne Owens	Updated minor details, no significant changes required	<a href="#">CChris MacKay (Deactivated)</a> 05 Dec 2018
13 Mar 2019	Wayne Owens	Reviewed and checked	<ul style="list-style-type: none"> <li>• <a href="#">Chris MacKay (Deactivated)</a> 16 Mar 2020</li> </ul>
19 May 2020	Wayne Owens	Reviewed and checked	<a href="#">Chris MacKay (Deactivated)</a> 28 May 2021
20 Aug 2020	Angeli Arino	Reviewed, no changes required	<ul style="list-style-type: none"> <li>• 01 Dec 2021 <a href="#">Ian Bartram</a></li> </ul>
01 Dec 2020	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"> <li>• 26 Jan 2023 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"> <li>• 08 Feb 2024 <a href="#">Ian Bartram</a></li> </ul>

# Remote Access - Employees & Contractors - Policy

**Review period:** Annual

## Overview

Remote access to our corporate network is essential to maintain productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Wellnomics, we must minimize these external risks the best of our ability.

## Purpose

The purpose of this policy is to define rules and requirements for connecting to Wellnomics' network from any host. These rules and requirements are designed to minimize the potential exposure to Wellnomics from damages which may result from unauthorized use of Wellnomics resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Wellnomics internal systems, and fines or other financial liabilities incurred as a result of those losses.

## Scope

This policy applies to all Wellnomics employees, contractors, vendors and agents with a Wellnomics-owned or personally-owned computer or workstation used to connect to the Wellnomics network. This policy applies to remote access connections used to do work on behalf of Wellnomics, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Wellnomics networks.

## Policy

It is the responsibility of Wellnomics employees, contractors, vendors and agents with remote access privileges to Wellnomics' corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Wellnomics.

Only approved Wellnomics equipment will be used to remotely access the Wellnomics network. By definition, any equipment leased, purchased or otherwise provided by Wellnomics is so approved.

## Requirements

Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the [Password Construction Guidelines](#).

Authorized Users shall protect their login and password, even from family members. While using a Wellnomics-owned computer to remotely connect to Wellnomics' corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time.

All hosts that are connected to Wellnomics internal networks via remote access technologies must use up-to-date anti-virus software.

## Policy Compliance

## Compliance Measurement

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, network monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the IT Manager.

## Exceptions

Any exception to the policy must be approved by the Wellnomics management team, in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Wellnomics' network:

- [Acceptable Use - Employees & Contractors - Policy](#)
- [Passwords and Encryption - Employees & Contractors - Policy](#)
- [Passwords & Encryption - Employees & Contractors - Guidelines](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
September 2016	Wayne Owens, Principal Consultant	Converted to new format	15 Sep 2017 <a href="#">Wayne Owens (Unlicensed)</a>
04 Jul 2017	Wayne Owens	Minor amendments to link in new related docs	04 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay, Support Consultant	Reviewed, no changes made	<ul style="list-style-type: none"><li>• 05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li></ul>
20 May 2020	<a href="#">Chris MacKay (Deactivated)</a>	Reviewed, no changes required	<ul style="list-style-type: none"><li>• 20 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li></ul>
24 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"><li>• 24 Aug 2021 <a href="#">Ian Bartram</a></li></ul>
01 Dec 2020	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"><li>• 01 Dec 2022 <a href="#">Ian Bartram</a></li></ul>
26 Jan 2023	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"><li>• 01 Feb 2024 <a href="#">Ian Bartram</a></li></ul>



# Home Working - Employees & Contractors - Policy

## Purpose

To document the situations, requirements and procedures of the Work from Home plan which will enable Wellnomics staff to work from home or from a location other than the Wellnomics offices

## Introduction

Due to the nature of many of the tasks performed by its employees, Wellnomics is often able to offer some flexibility around enabling staff to work from home. As per the Conditions of Employment Guideline:

*“From time to time you may request to work from home or Wellnomics may require you to work from home. Wellnomics’s policy is that every endeavour will be made to ensure you can work from the office and only in specific circumstances approval for working at home will be given by your Reporting Manager.”*

However, there are some situations (personal or business) when it is desirable for an employee to be able to work from home – or remotely - if they are able to do so.

People travelling, or working from remote offices within New Zealand or overseas, will also have recourse to follow these instructions.

It is also possible that this procedure would be invoked through the Business Continuity plan if instigated by a Critical Event (e.g. Pandemic).

## Key Points

Working from home under non-emergency Circumstances Some situations may require working from home on a short-term, temporary basis. These occasions may include:

- Being at home with a sick child or other family member
- Recovery from an infectious illness or other condition when you wish to resume work but do not have medical clearance to return to the office
- Where the ability to provide uninterrupted, single-focussed time to a project or task is required
- Where a task needs to be done outside office hours and it is not necessary to be physically in the office

Other circumstances agreed with their manager In some circumstances, it may be agreed that a staff member works from home for some of their working hours on a permanent basis. While it is preferable for staff to work from the Wellnomics offices, there are a few situations which may warrant ongoing working from home. These occasions may include:

- A requirement for ongoing time shuffling due to a long-term personal commitment such as child care
- A requirement for ongoing split shifts due to the necessity within the

# IT Requests - Employees & Contractors

## Overview

This policy is focused on the IT requests and process to be followed by all staff and contractors when submitting IT requests.

## Purpose

The purpose of this policy is to establish guidelines for submitting IT requests by employees and contractors of Wellnomics to ensure that all IT requests from employees and contractors are handled efficiently, consistently, and securely by the Wellnomics IT department. This policy is also designed to minimize disruptions caused by IT issues and provide a timely resolution to all IT requests.

## Scope

This policy applies to all employees and contractors of Wellnomics who require IT support. All IT requests must be submitted through the Wellnomics Helpdesk ticketing system.

## Policy

1. All IT requests from employees and contractors must be submitted through the [Wellnomics Helpdesk](#) ticketing system. Any IT request submitted outside of the Helpdesk system will not be addressed.
2. All requests emailed to [support@wellnomics.com](mailto:support@wellnomics.com) should contain "IT Request" in the subject or description. Otherwise they may not be properly assigned and the resolution will be delayed.
3. The Helpdesk ticketing system will be used for all IT requests, including hardware and software support, network issues, elevated role requests, and password reset requests.
4. The Helpdesk ticketing system allows you to track the progress and resolution of your IT requests.
5. When submitting an IT request, employees and contractors must provide complete and accurate information regarding the issue and the necessary action required to resolve the problem.
6. The IT department will prioritize IT requests based on the level of urgency and the impact on business operations.
7. The IT department will provide regular updates to the employee or contractor who submitted the IT request on the status of their request until it is resolved.
8. The IT department will maintain the confidentiality and security of all IT requests and any sensitive information related to them.
9. The IT department may, at its discretion, refuse support and escalate any misuse of the IT request process, for any employee or contractor who repeatedly violates this policy or who engages in behavior that jeopardizes the security or integrity of the Wellnomics IT infrastructure.

## Requirements

### Software Requests

- All Software requests should include a business need. i.e. why this is needed to complete your work.
- If the software must be purchased this will require additional approval from the employee's direct supervisor (prior to IT request). Please include the written approval confirmation with the request.

### Elevated Role Requests

Any and all requests for elevated permissions must include the following:

- Business reason
- The required role
- The resource(s) affected.

## Password Reset Requests

- Must be submitted by the staff member or their direct supervisor.
- Must include information regarding the situation that led to the request i.e. was the password forgotten or compromised.

## Policy Compliance

The IT department will regularly monitor compliance with this policy to ensure that all IT requests are being submitted through the Helpdesk ticketing system and that employees and contractors are providing accurate and complete information. The IT department will also review the Helpdesk ticketing system to identify any areas where improvements can be made to the IT support process.

All employees and contractors of Wellnomics are responsible for complying with this policy. Failure to comply with this policy may result in disciplinary action.

Any employee or contractor who becomes aware of a violation of this policy should report it immediately to their supervisor or the IT department.

This policy will be reviewed periodically by the IT department to ensure that it remains current and effective. Any revisions to the policy will be communicated to all employees and contractors of Wellnomics..

## Exceptions

Some exceptions to this policy apply.

- If a staff member cannot access their work computer, they should contact their direct supervisor to submit the ticket.
- If the issue is of business-critical importance, i.e. compromised elevated credentials, the staff member should call IT immediately.

## Revision History

Date of change	Responsible	Summary of change	Next revision due
18 Apr 2023	Ian Bartram	Policy created	<ul style="list-style-type: none"><li>• 18 Apr 2024 <a href="#">Ian Bartram</a></li></ul>
20 Apr 2023	Corinne Wright	Review creation with minor adjustments	<ul style="list-style-type: none"><li>• 20 Apr 2024 <a href="#">Ian Bartram</a></li></ul>



# DOCUMENTATION

- [PRODUCT & SOFTWARE DEVELOPMENT - Documentation](#)
- [DEPLOYMENT & HOSTING - Documentation](#)
- [INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Documentation](#)

# PRODUCT & SOFTWARE DEVELOPMENT

## - Documentation

- [Software Development Life Cycle - Documentation](#)
- [Logging & Diagnostics - SaaS - Documentation](#)
- [Logging - App - Documentation](#)
- [Third Party Components - WorkPace Classic App - Documentation](#)
- [Third Party Components - App - Documentation](#)
- [Third Party Components - SaaS - Documentation](#)
- [Data Privacy Compliance - Documentation](#)
- [Privacy Policy - Default - SaaS - Documentation](#)
- [Product Security and Best Practice - SaaS - Guidelines](#)
- [Product Security and Best Practice - App - Guidelines](#)
- [Access Security - SaaS - Documentation](#)
- [Threat Modelling - App - Documentation](#)
- [Threat Modelling - SaaS - Documentation](#)
- [Software Development Tools - Documentation](#)
- [Static Analysis Security Testing \(SAST\) - Guideline](#)
- [Dynamic Analysis Security Testing \(DAST\) - Guidelines](#)
- [App Security Testing - Guidelines](#)
- [SaaS Security and Penetration Testing - Guidelines](#)

# Software Development Life Cycle - Documentation

Review period: Annual

## Introduction and Background

This process covers all aspects of Wellnomics software development and covers the software products detailed below:-

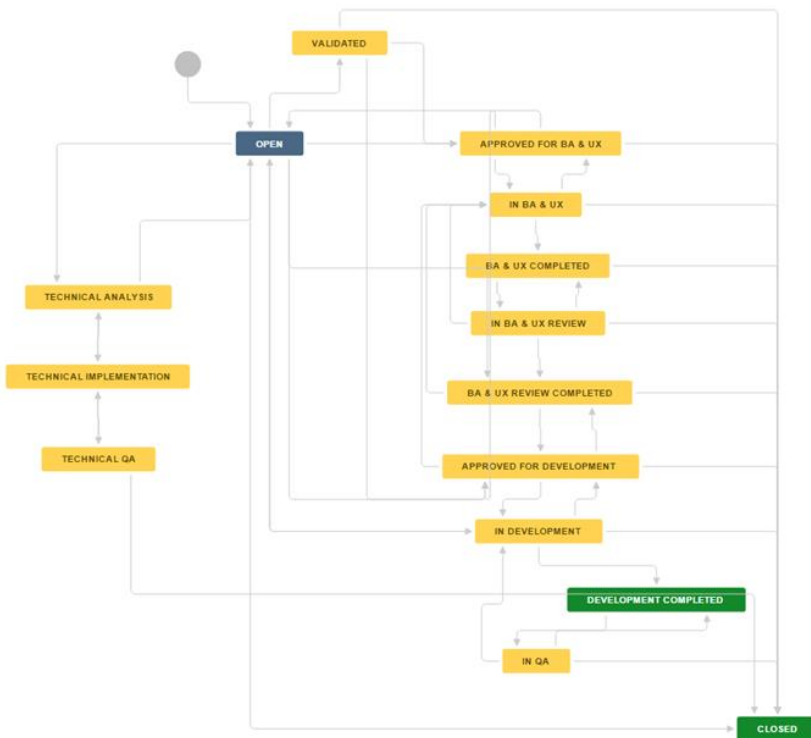
- Wellnomics SaaS
- Wellnomics Client App (for all platforms)

Non development changes are covered by the document - [Change Management Process \(excl. Software Development\)](#)

## Development Change Management Processes

Wellnomics uses an **Agile Software Development Life Cycle (SDLC)** that includes formal processes for initiation, planning, design, development, testing, release and implementation. The company uses best practices in all areas including **Test-Driven Design (TDD)**, separate development and QA teams, **test automation** (including **automated performance testing** and **automated deployment testing**), plus **integration testing** and **continuous release**.

Schematic of change management process for software development :-



The software development change process identifies 2 key states for any proposal for change - the "Ready" state and the "Done" state. See related documents linked below for a full definition of these states.

## Definition of Ready

1. User story defined
2. Follows OUR guidelines
  - Testable
  - Size <= Days
  - Estimable (or Timebox it)
  - Slice vertically
3. Acceptance criteria defined. Must handle
  - Rights and roles (Privacy & Access Controls)
  - Enabled/disabled Assessments & Training
  - Licensing (number of users, license expiry)
  - Data status
4. UI design & text defined
  - Meets guidelines & standards (& glossary)
  - UI text is defined in UI mockup (by default)
5. UX design\flow defined
  - Data validations defined
  - Error messages defined
6. Constraints defined
  - Performance
  - File size
7. Algorithms defined
8. External resources available
  - E.g. images, icons

## Definition of Done

1. Coding standards met
2. Unit tests written & passing on Jenkins
3. Database create & upgrade scripts created
4. Code commented & documented
5. Performance & load requirements met
6. Security requirements met
7. Peer reviewed
8. Builds on Jenkins without errors
9. UI & UX design & guidelines met
10. Constraints & validation rules met
11. Passes W3C validation
12. Automated tests written
13. Acceptance criteria met
14. Tested against Jenkins release build
15. Exploratory testing done

A proposed change cannot start its process through development until it meets the "**Definition of Ready**". Once the development has been completed, a proposed change cannot be released into the product until it meets the "Definition of Done".

**Evidence** : See [Evidence - Use of JIRA Software Development Ticketing and Tracking System](#)

## Details on Software Development

- **Source Control** is done using **Git** (allows easy branching and merging)
- **Continuous Integration** is done using **Jenkins** and all unit tests are rerun upon each commit.

## QA and Testing

We use the following:

- Our software developers use **Test Driven Design** (TDD) with unit tests created for most new features.
- We have a dedicated QA team responsible for doing QA on development items, which are all managed using the **JIRA** issue tracking software
- The QA team is also responsible for maintaining our test automation suite using **Cypress** and **C#**. New automated tests are added covering all bug fixes.
- We have automated nightly integration and release with automated deployment and full test automation suite run nightly, with a test dashboard showing any overnight failures.
- Deployment testing includes testing both a new and an upgraded install from previous release.
- Deployment testing also tests with all of the currently supported versions of Windows, Windows Server, SQL Server and IIS.
- **Test automation suite** includes automated performance testing of critical areas, data testing (calculator tests in C#), and UI error checking across all websites (Cypress). Soon we will also have automated tests for both desktop and mobile that will capture any GUI related issues.
- Unit tests and specially created test datasets are used to validate input and output values to ensure accuracy of data processing within each module of the product.
- The QA engineers also do **exploratory testing** on new features.
- When a release candidate is ready a special release testing process is also run through, which includes a list of manual tests and preparing detailed release notes.
- Release candidate is then passed to Support Team who perform their own implementation and deployment testing of testing including a test deployment and , UI check, detailed testing of new features and known areas of complexity (such as HR import).
- if any issues are found the product has to go back to Dev and the whole process repeated again...
- We also do a full set of manual performance testing on each release candidate using two very large databases containing real world anonymised data from two of our largest customers. This ensures the product meets our performance targets for worst case management reporting (eg on very large group sizes)

## Security and penetration testing

Static code analysis tool **DevExpress CodeRush** is used in all software development to automatically analyse and highlight coding or security issues when code is being written. This ensures no code is committed without it having been analysed for potential security issues.

Every release candidate is fully tested following OWASP (Open Web Application Security Project) guidelines (see [Wellnomics Penetration testing protocol.docx](#)). Security and penetration testing is fully documenting showing how the product has been tested and demonstrating compliance with OWASP guidelines and best practice.

Any High security weaknesses or failures found are fixed before release. Medium weaknesses are fixed before release, or on next release, depending upon complexity of addressing them.

## Releases

All release products and executables are **digitally signed** by an Extended Validation (EV) Digital Certificate (the highest security type of certificate available)

All releases provide backward compatibility with at least the last 5 years, and in some cases up to 10 years, of previous releases of the product, ensuring customers can upgrade smoothly from any prior version released in the last 5-10 years.

All releases are accompanied by:

- **Release Notes** listing all significant new features and enhancements, bugs that have been fixed.

## Policy Compliance

The Wellnomics management team will verify compliance to this policy by through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner. There is also a specific penetration testing report produced for every release (see [Independent Penetration Testing - Results](#) )

# Exceptions

Any exception to the policy must be approved by the Wellnomics management team in advance.

# Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Related Standards, Policies and Processes and Documents

[Definition of Ready](#)

[Definition of Done](#)

# Revision history

Date of change	Responsible	Summary of change	Next revision date
6th December 2015	Wayne Owens, Principal Consultant	Updated and converted to new format	6th December 2016
2nd February 2017	Wayne Owens, Principal Consultant	cross referenced to existing practice - no changes required	January 2018
03 Jul 2017	Kevin Taylor	Checked and updated with minor changes to dev processes	<ul style="list-style-type: none"><li><a href="#">Chris MacKay (Deactivated)</a>03 Jul 2018</li></ul>
03 Jul 2018	Chris MacKay	Updated links and processes to reflect current Workflows	<ul style="list-style-type: none"><li><a href="#">Chris MacKay (Deactivated)</a>03 Jul 2019</li></ul>
20 May 2020	Wayne Owens, Principal Consultant	Added reference to new Wellnomics client software project	<ul style="list-style-type: none"><li>20 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li></ul>
24 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"><li>24 Aug 2021 <a href="#">Angeli Arino (Deactivated)</a></li></ul>
31 Aug 2020	Kevin Taylor	Added comments about CodeRush static code analysis tools	
30 Sep 2020	Angeli Arino	Update mentioned QA Tools in line with what we currently use.	<ul style="list-style-type: none"><li>24 Sep 2021 <a href="#">Ian Bartram</a></li></ul>
10 Oct 2021	Ian Bartram	QA Tools updated	<ul style="list-style-type: none"><li>10 Oct 2022 <a href="#">Aarti</a></li></ul>
08 Sep 2022	<a href="#">Kevin</a>	Reviewed and no changes except formatting	<ul style="list-style-type: none"><li>08 Sep 2023</li></ul>

26 Jan 2023	Corinne Wright	Reviews, removed IT admin guides as part of release process as only hosted sites are upgraded.	26 Jan 2024 <a href="#">Corinne</a>
-------------	----------------	--	-------------------------------------

# Logging & Diagnostics - SaaS - Documentation

## Introduction

The Wellnomics SaaS solution includes logging for the purposes of auditing user actions and tracking and resolving errors.

## Data privacy

No personal user data is recorded in any logs.

## Error logging

- Each module in the SaaS system maintains an error log in a text readable format.
- Any exception or error that occurs in the product or during a process (such as an HR update) will be recorded together with a stack trace with sufficient information to allow full investigation of any issue.

## Trace logging

- If required, trace logging can be enabled for certain modules or processes to provide more detailed tracking of processes to assist with diagnosing issues.

## Audit logging

The system records audit logs within the customer database. These audit logs include:

- All logins and all login failures
- All configuration changes under
  - Admin > Policy configuration
  - Act > Change user settings policy
  - Admin > Manage Organizational Groups
  - Admin > Local Administration
- All suspending and un-suspending of users
- All HR imports and adding, removing or changing of users done as part of an HR import

In order to allow full auditing of system changes and actions each log entry includes the following :-

- Date and time
- User ID of user who made the change
- Name of appropriate feature or function
- Type of action performed e.g. addition, amendment , deletion etc.
- Changed tables/fields in database and changes made
- For login failures the username being used for the login attempt

## Protection against deletion

All audit logs are protected against deletion through the following:



1. No functionality provided to allow editing or deleting of logs by any user
2. Logs are stored under a different database schema from the main schema, where the data logs schema has all edit and delete permissions permanently disabled. This means that even users who are given permission to edit and delete certain data within the main database system can never expand these permissions to delete logging data, as the logging data is under a different schema.

## Customer access to audit logs

Wellnomics support can provide an export of any set of audit logs and period to customers upon request.

## Revision History

Date of change	Responsible	Summary of change	Next revision date
13 May 2017	Wayne Owens, Principal Consultant	Created - updated to new format	15 May 2018 <a href="#">Wayne Owens (Unlicensed)</a>
22 Nov 2017	Kevin Taylor, CEO	Minor updates only	20 Nov 2018 <a href="#">Chris MacKay (Deactivated)</a>
21 Nov 2018	<a href="#">Chris MacKay (Deactivated)</a>	Reviewed, no changes made	12 Nov 2019
6 Mar 2019	Kevin Taylor	Updated content to improve readability	<ul style="list-style-type: none"> <li>06 Mar 2020 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
22 May 2020	Wayne Owens	Updated to reflect change from Microsoft Azure to Microsoft Azure	<ul style="list-style-type: none"> <li>24 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
31 Aug 2020	Angeli Arino	Converted to a new page	
07 Jan 2021	<a href="#">Kevin</a>	Added notes about protection from deletion of logs	
24 Jun 2021	<a href="#">Kevin</a>	Updated to reflect latest features on Azure system	<ul style="list-style-type: none"> <li>24 Jun 2022</li> </ul>
08 Sep 2022	<a href="#">Kevin</a>	Reviewed and no changes needed as of SaaS 4.12	<ul style="list-style-type: none"> <li>08 Sep 2023</li> </ul>

# Logging - App - Documentation

The Wellnomics Client App (installed on desktop or mobile device) includes error and trace logging for the purposes of assisting with troubleshooting configuration issues and identifying and resolving errors.

The logs record things such as:

- System events such as startup and close down
- System configuration and application version information
- History of data communication with the server
- Application errors

The logs are recorded in one or more plain text readable files in (under Windows) the user's local Appdata/Roaming folder on the computer.

No personal user data or user identifying information (such as name or email address) is recorded in any logs.

Logging is available at the following levels:

1. error
2. system
3. info
4. debug
5. debug\_verbose
6. trace

The default log level being *system*. The app supports the ability for a user to temporarily turn on *debug\_verbose*/*trace* level for a single session to assist with troubleshooting.

The Wellnomics Client App also supports an inbuilt feature for user's to email their logs to Wellnomics support - meaning users do not need to search for the log files location.

For more details refer to specific documentation under [App Logging](#)

## Revision history

Date of change	Responsible	Summary of change	Next revision date
24 Jun 2021	<a href="#">Kevin</a>	Created based up WC Logging documentation	<ul style="list-style-type: none"><li>• 24 Jun 2022</li></ul>
08 Sep 2022	<a href="#">Kevin</a>	Reviewed and no changed required. Will need updating once we implement planned automated diagnostics feature	<ul style="list-style-type: none"><li>• 04 Apr 2023 <a href="#">Kevin</a></li></ul>
05 Jul 2023	<a href="#">Wayne Owens</a>	Reviewed and no changed required. Will need updating once we implement planned automated diagnostics feature	<ul style="list-style-type: none"><li>• 04 Jan 2024 <a href="#">Kevin</a></li></ul>

# Third Party Components - WorkPace Classic App - Documentation

<b>Last updated</b>	Nov 2020
<b>Product version</b>	WPC 5.5.7
<b>Platform</b>	Windows

Library	Version	License type	License link	Description	Source code
OpenSSL	1.1.0e-fips 16 Feb 2017	Apache License v2	<a href="https://www.openssl.org/source/license.html">https://www.openssl.org/source/license.html</a>		<a href="https://www.openssl.org/source/license.html">https://www.openssl.org/source/license.html</a>
SQLite	3.8.5	Open source Public domain	<a href="http://sqlite.org/copyright.html">http://sqlite.org/copyright.html</a>	SQLite database engine	<a href="http://sqlite.org/">http://sqlite.org/</a>
CppSQLite3	3.2	Open source Public domain	<a href="https://github.com/neosmart/CppSQLite/blob/master/LICENSE">https://github.com/neosmart/CppSQLite/blob/master/LICENSE</a>	A C++ wrapper around the SQLite3 embedded database library.	<a href="https://github.com/neosmart/CppSQLite/blob/master/LICENSE">https://github.com/neosmart/CppSQLite/blob/master/LICENSE</a>
Json-cpp	1.6.4	MIT License	<a href="https://github.com/open-source-parsers/jsoncpp/blob/master/LICENSE">https://github.com/open-source-parsers/jsoncpp/blob/master/LICENSE</a>	A C++ library for interacting with JSON.	<a href="http://jsoncpp.sourceforge.net/">http://jsoncpp.sourceforge.net/</a>
XMLIO	0.92	LGPL		A C++ XML input/output library	<a href="http://xmlio.sourceforge.net/">http://xmlio.sourceforge.net/</a>
RSA Data Security, Inc. MD5 Message-Digest	3.0	CppSQLite license Open source Public domain	<a href="https://github.com/neosmart/CppSQLite/blob/master/LICENSE">https://github.com/neosmart/CppSQLite/blob/master/LICENSE</a>	interface for the MD5Checksum class	<a href="https://github.com/neosmart/CppSQLite/blob/master/LICENSE">https://github.com/neosmart/CppSQLite/blob/master/LICENSE</a>
zlib	1.2.11	ZLib license Open source Public domain	<a href="https://zlib.net/zlib_license.html">https://zlib.net/zlib_license.html</a>	interface of the 'zlib' general purpose compression library	<a href="https://zlib.net/">https://zlib.net/</a>
gifimage	2.2	Open source		GIF Graphics Object	<a href="http://melander.com/gifimage/">http://melander.com/gifimage/</a>
KS Dev SkinEngine	2.9.1	Commercial. Wellnomics has bought a commercial licence for use in our products.	n/a	Skin engine	<a href="http://www.ksdev.com/">http://www.ksdev.com/</a>

Tinyxml	2.6.2	ZLib license Open source Public domain		TinyXML is a simple, small, minimal, C++ XML parser that can be easily integrating into other programs. Used in wpsync.dll.	<a href="https://github.com">https://github.com</a>
---------	-------	--	--	---	---

# Third Party Components - App - Documentation

<b>Last updated</b>	Mar 2023			
<b>Product version</b>	WC 2.3.0			
<b>Platform</b>	Windows 64bit			
<b>Library</b>	<b>Version</b>	<b>License type</b>	<b>Description</b>	<b>Source code</b>
Qt	6.4.0	<a href="#">GPL 2.0, 3.0, LGPL 3.0</a>	Qt cross-development platform	<a href="https://www.qt.io">https://www.qt.io</a>
OpenSSL	1.1.1t		Open Secure Socket Layer Library	<a href="https://www.openssl.org/">https://www.openssl.org/</a>
Inno Setup	5.5.5	Modified BSD license	Installer	<a href="http://www.jrsoftware.org/isinfo.php">http://www.jrsoftware.org/isinfo.php</a>

See also:

[Third Party Components Review - App 1.3.1 \(Dec 2021\)](#)

# Third Party Components - SaaS - Documentation

Update regularly with new releases

<b>Last updated</b>	Nov 2022			
<b>Product version</b>	WRM 4.14.0			
Library	Version	License type	Copyright	Source
OpenSSL	1.1.0e-fips	Apache License v2 <a href="https://www.openssl.org/source/apache-license-2.0.txt">https://www.openssl.org/source/apache-license-2.0.txt</a>	Copyright © 1999-2018, 16 Feb 2017	<a href="https://">https://</a>
Ajax Control Toolkit	18.1.1	Microsoft Public License <a href="https://raw.githubusercontent.com/DevExpress/AjaxControlToolkit/master/LICENSE.txt">https://raw.githubusercontent.com/DevExpress/AjaxControlToolkit/master/LICENSE.txt</a>	Copyright © 2012-2019, CodePlex Foundation	<a href="https://">https://</a>
Apexcharts	3.21.0	MIT License <a href="https://opensource.org/licenses/mit-license.php">https://opensource.org/licenses/mit-license.php</a>	Copyright © 2018	
Bootstrap	3.4.1	MIT License <a href="http://www.opensource.org/licenses/mit-license.php">http://www.opensource.org/licenses/mit-license.php</a>	Copyright © 2011-2019 Twitter, Inc. Copyright © 2011-2019 The Bootstrap Authors	
D3 visualization library	5.7.0	BSD 3-Clause Revised License <a href="https://github.com/d3/d3/blob/master/LICENSE">https://github.com/d3/d3/blob/master/LICENSE</a>	Copyright © 2010-2017 Mike Bostock	<a href="https://">https://</a>
jQuery Core		MIT License <a href="http://www.opensource.org/licenses/mit-license.php">http://www.opensource.org/licenses/mit-license.php</a>	Copyright © 2009 John Resig	
jQuery MultiSelect plugin		MIT License <a href="http://www.opensource.org/licenses/mit-license.php">http://www.opensource.org/licenses/mit-license.php</a>	Copyright © 2008 A Beautiful Site, LLC.	
jQuery SelectBoxes plugin		MIT License <a href="http://www.opensource.org/licenses/mit-license.php">http://www.opensource.org/licenses/mit-license.php</a>	Copyright © 2006-2009 Sam Collett	<a href="http://w">http://w</a>
jQuery UI	1.11.4	MIT License <a href="http://www.opensource.org/licenses/mit-license.php">http://www.opensource.org/licenses/mit-license.php</a>	Copyright © 2009 AUTHORS.txt	<a href="http://j">http://j</a>
jQuery Cycle Plugin	1.7.1	MIT License <a href="http://www.opensource.org/licenses/mit-license.php">http://www.opensource.org/licenses/mit-license.php</a>	Copyright © 2007-2013	
Microsoft's patterns & practices' Enterprise Library	version 5.0	Apache License, Version 2.0 <a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>	Copyright © Microsoft Corporation 2011	

Node.JS		Node.JS License <a href="https://raw.githubusercontent.com/nodejs/node/master/LICENSE">https://raw.githubusercontent.com/nodejs/node/master/LICENSE</a>	Copyright © Node.js Foundation contributors	<a href="https://">https://</a>
Newtonsoft.Json		MIT License <a href="https://github.com/JamesNK/Newtonsoft.Json/blob/master/LICENSE.md">https://github.com/JamesNK/Newtonsoft.Json/blob/master/LICENSE.md</a>	Copyright © 2007 James Newton-King	<a href="https://">https://</a>
TimeZoneConverter		MIT License <a href="https://github.com/mj1856/TimeZoneConverter/blob/master/LICENSE.txt">https://github.com/mj1856/TimeZoneConverter/blob/master/LICENSE.txt</a>	Copyright © 2017 Matt Johnson	<a href="https://">https://</a>
Toastr		MIT License: <a href="http://www.opensource.org/licenses/mit-license.php">http://www.opensource.org/licenses/mit-license.php</a>	Copyright © 2012-2014 Hans Fjällemark, John Papa & Tim Ferrell.	<a href="https://">https://</a>
Popper.js		MIT License: <a href="https://github.com/FezVrasta/popper.js/blob/master/LICENSE.md">https://github.com/FezVrasta/popper.js/blob/master/LICENSE.md</a>	Copyright © 2016-2019 Federico Zivolo & Contributors	<a href="https://">https://</a>
Tippy.js		MIT License <a href="http://www.opensource.org/licenses/mit-license.php">http://www.opensource.org/licenses/mit-license.php</a>	Copyright © 2019	<a href="https://">https://</a>
TinyMCE	4.3.10	LGPL v2.1 (GNU Lesser General Public License, version 2.1) <a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.txt">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.txt</a>	© 2019 Tiny Technologies Inc.	
SharpZipLib	0.85.5	GNU General Public License, version 2, <a href="http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt">http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt</a>	Copyright © 2001-2007 Mike Krueger, John Reilly	
Vue	2.7.10	MIT License <a href="http://www.opensource.org/licenses/mit-license.php">http://www.opensource.org/licenses/mit-license.php</a>	Copyright © 2014-2019 Evan You	<a href="https://">https://</a>

# Data Privacy Compliance - Documentation

Review period: Annual

## Data Privacy Requirements

Being seen to protect the privacy of employees is increasingly important and many organizations have policies regarding privacy of employee data. In some countries there is special legislation specifically outlining legal requirements for data privacy (see later section *Data Privacy Legislation*). In general, these data privacy requirements can be summarized with the common principles below:

1. Data about employees (referred to as “personal data”) should only be collected if there is a specific purpose for its collection. You can’t just collect data because it “might be useful one day”.
2. The amount of data collected should be limited to just that needed to fulfill the identified purpose.
3. Data should not generally be used for other purposes than that for which it was collected[†].
4. Employees should be informed about the data collection and the purpose for which it is being collected.
5. Employees have the right to request access to the data stored about them.
6. Data should not be kept longer than is necessary.
7. Data should not be transferred to a foreign country unless it can be assured that the data will be only used in accordance with the privacy requirements of the originating country.

Furthermore, when accessing and using this data:

1. Access to the data should only be provided to those who have a legitimate need to use the data (in accordance with the original purpose of its collection).
2. When someone is given access to data, they should only be given access to the minimum data required for them to complete their assigned tasks.
3. Access to sensitive personal data[†], such as health information, should only be provided to people qualified (or trained) to understand and interpret this information correctly.

It should be noted that data privacy requirements only apply to “personal data”, this being data that relates to an individual who can be identified from it. Group statistics where specific individuals cannot be identified, such as averages or distributions, are therefore not covered by data privacy legislation. This said, when using aggregate data it must be ensured that the group size used is large enough that information about individual members of the group cannot be inferred. For example, if high stress levels occur for 66% of the members of the group, and there are only 3 people in the group, then it is going to be easy to identify the employees that have this issue present.

## Health and Safety legislation and employee consent

Employee consent may be required for collecting and using data, particularly sensitive data such as that about health. This could be seen as an issue when it comes to using the Wellnomics solution – with employee consent being required before the data on computer use, or assessments of discomfort, can be collected.

However, most data privacy legislation has specific exemptions for the collection of data for health and safety purposes. Employers have a legal responsibility to ensure the health and safety of their employees at work and most health and safety legislation specifically requires the collection of employee information as part of conducting risk assessments and in identifying early signs of injury (i.e. early reporting of discomfort). Data on exposure (time on computer, number of breaks), pain symptoms, workstation setup and posture, and even psychosocial factors, are all legitimate data for the purposes of conducting accurate risk assessment.

As an employer cannot fulfill his legal responsibilities without collecting this information employee consent is not required. In fact, health and safety legislation normally places a responsibility on employees to cooperate, as employees also have a duty of care to ensure their own health and safety at work. This includes co-operating with any employer initiatives aimed at achieving this (so long as these initiatives are reasonable of course).

This means that (i) the collection of data by the Wellnomics solution cannot contravene data privacy requirements, and (ii) no employee consent is required for the collection.



Of course, although health and safety obligations override data privacy limitations when it comes to the collection of data by the Wellnomics solution, they still apply to the use and access of this data once its collected. This means the data on individuals collected by the Wellnomics solution should only be used for the purposes of health and safety, and access to it should only be by those staff responsible for health and safety.

This does not preclude the use of the data for other purposes in an aggregate or anonymized form. However, it is recommended as good practice to inform staff if the data is to be used for any other purposes, even if this is done in an anonymous form.

## How the Wellnomics solution supports data privacy

The Wellnomics solution supports full compliance with data privacy legislation and policies. It achieves this through the following:

1. the Wellnomics solution records the minimum data[§] on computer use required to calculate exposure risks. The product does not record any detailed data such as what words were typed, which documents were edited, or which websites were viewed. Nor does it record information on work patterns during the day. Instead, only *exposure* data relevant to determining WMSD related risk is recorded. Data such as total hours at the computer, number of breaks, and total keystrokes typed. This ensures the employees privacy with respect to their activity at their computer is preserved as much as possible.
2. the Wellnomics solution is designed to restrict access to raw data such as statistics on computer use, or answers to assessment questionnaires, which could be mis-interpreted or used for other non-health and safety purposes. The product instead focuses on providing interpreted data that is designed for the intended purpose of managing the health and safety risks of employees. This is done by converting computer statistics and questionnaire answers into “risk factors” that indicate the simple presence or absence of a particular known risk for RSI. For example, the risk factor “High computer use” does not report the actual number of hours of computer use, but simply whether the use was above or below a *risk threshold*.
3. Each employee can login to the system and has full access all data recorded about them, including historical data.
4. A Privacy and Access Control feature allows the level of data access to be controlled for different users (or “roles”). This is done in two ways:
  - a. A **Data Privacy Level** controls whether someone can see **Individual** or just **Group** data. For example, a manager may be restricted to seeing just group data such as average risk levels or the top risk factors for their department. Only OH&S personnel may be allowed to view data on individual employees.
  - b. A **Data Access Level** controls what level of data a user can see. For example, access to data on computer statistics may be restricted to just OH&S personnel who are able to interpret this data as part of conducting a detailed evaluation for an employee who is at high risk or has reported an injury.
5. If someone is only given access to Group data, then a minimum group size can be set (e.g. 50 users) to ensure that anonymity is maintained in any group reporting.
6. There are four “roles” defined in the product. Data access and privacy levels can be set separately for each role. Furthermore, each role is automatically restricted to only viewing data on the employees they are responsible for.

Role	Description
End user	An employee with no reporting staff. Can only see their own data.
Manager	Can only see data about their reporting staff (both direct reports, and employees further down the reporting hierarchy).
Local Administrator	Generally company OH&S personnel or ergonomists. Is only given access to users within the group or department they are responsible for.
Global Administrator	The company OH&S manager or a senior manager. The only role that can access data for all employees in the organization.

Data imported from the organization’s HR database is used to define which staff have each role and which employees they are responsible for. Tools are provided to allow the Wellnomics Global Administrator to then adjust access for different users.

## Guidelines for using the Wellnomics solution in accordance with data privacy requirements

## Inform staff

Inform staff about the project making sure to cover:

- What data will be collected.
- How the data will be used.
- Who will have access to the data.

Because the use of the Wellnomics solution will likely be a new concept to staff it will be helpful to include some background on the project. For example, remind staff that as an employer you are responsible for the health and safety of employees at work. This means you have a legal responsibility to take steps to protect staff from the risks of RSI/WMSD. One of the steps required to achieve this is to perform risk assessments for each employee and measure their exposure to the risk factors that can cause RSI. The latest research now shows that time using the computer and the level of breaks are as important as workstation setup in determining risks. This means that monitoring information on exposure is now required as well in order to accurately assess risks.

Perhaps refer employees to some background information on RSI risks – causes and prevention, which explains the multi-factorial nature of RSI.

## Identify roles for managers

Review your OH&S processes and determine what responsibilities your managers are expected to take on regarding the management of health and safety risks of their reporting staff. As access to personal data by their own manager is likely to be the most sensitive area for employees restricting access by managers to only the data needed to fulfil their responsibilities is important.

Depending upon managers responsibilities, some different options are outlined below:

OH&S responsibilities	Recommendation
None	<p>The manager may have no specific OH&amp;S responsibilities, other than to co-operate with OH&amp;S staff when requested. Managers may still be interested to monitor the general risk levels of their staff or department.</p> <p><b>Data Privacy Level = Group</b></p> <p><b>Data Access Level = Overall Risk/Wellbeing</b></p>
Only responsible for ensuring staff complete OH&S training & assessment requirements	<p>The manager may only be responsible for facilitating the OH&amp;S process by ensuring their staff meet the OH&amp;S requirements of completing the training and risk assessments, and their staff have WorkPace installed.</p> <p><b>Manager Data Privacy Level = Group</b></p> <p><b>Manager Data Access Level = Overall Risk/Wellbeing</b></p>
Responsible for monitoring risk levels and taking action to reduce risks, but on a group basis only	<p>The manager may only be responsible for taking action at a group level – e.g. addressing risk factors that are common to their staff or department, and monitoring the overall risk levels amongst their staff to ensure they are being kept below targets.</p> <p>The manager may therefore only need to look at group information to identify if risks are high, and what the common risk factors are. They can then call on OH&amp;S assistance to help address risks on an individual basis amongst their staff if risk levels are high.</p> <p><b>Manager Data Privacy Level = Group</b></p> <p><b>Manager Data Access Level = Risk/Wellbeing Factors</b></p>

<p>Expected to identify high risk staff and ensure appropriate action is taken to reduce risks.</p>	<p>The manager may be expected to take an active role in managing the risks of their staff. Identifying which staff are high risk, and then working with those staff to address those risk factors in co-operation with OH&amp;S support staff.</p> <p><b>Manager Data Privacy Level</b> = Individual</p> <p><b>Manager Data Access Level</b> = Risk/Wellbeing Factors</p>
---	--

It is not recommended that managers be given access to computer use statistics.

## OH&S staff

OH&S staff should be setup as **Local Administrators** in the Wellnomics solution. Each OH&S staff member should then be given access to just the group or groups of staff they are responsible for. OH&S staff will normally be given full access to data on individual employees within their departments.

**Local Administrator Data Privacy Level** = Individual

OH&S staff will need access to at least the Factors level of data.

**Local Administrator Data Access Level** = Factors

This will allow them to view risk reports for employees and see the most detailed level of risk information.

## Access to computer use statistics

the Wellnomics solution is able to provide basic reporting on computer use statistics, such as time using the computer, time using the mouse, number of days using the computer, and number of breaks taken, etc.

Generally speaking access to this data is not needed to manage the health and safety of employees. However, in some circumstances these statistics may be helpful in better understanding the work patterns of a high risk employee or an employee who has reported an injury (have they been working 7 days week? Have they been working overtime with days of over 8 hours at the computer?). These statistics can also be important in the case of a dispute or legal claim – providing objective evidence of the computer use exposure of the individual.

Depending upon your organizations policies you can decide to either provide OH&S staff with access to this data (**Local Administrator Data Access Level** = Statistics) or you can restrict this access only to the Wellnomics Global Administrator, who can then provide reports on this data on a case-by-case basis.

If OH&S staff are provided with access to computer use statistics it is important that they are trained to interpret this data and they do not provide copies of the data to other parties.

## EU-U.S. Privacy Shield Framework

The new [Privacy Shield Framework](#) replaces the old [US-EU Safe Harbor Framework](#) and provides a mechanism for allowing US companies to receive personal data from EU under EU [privacy laws](#) meant to protect European Union citizens.

If your organization already has significant cross-border data transfer between the US and Europe you may already have an existing certification under the above frameworks. For example, if employee human resources data is stored in a common database at a US based head office. The data collected by the Wellnomics solution may be already covered under this certification, or may be able to be covered through a modification or extension to the existing certification.

NOTE: As of 16 July 2020 the new Privacy Shield Framework was struck down by the European Court of Justice on the grounds it did not provide adequate protections to EU citizens on government data collection. This means there may not be a valid legal option for storing EU staff data in the USA currently.

# Using the Wellnomics solution across multiple countries

If an organization will be using the Wellnomics solution across different countries that are not covered by the same data privacy legislation, for example, US and UK, or US and Australia the options are:

1. Locate the the Wellnomics solution data server in the jurisdiction with the strictest data privacy requirements – for example, in Europe.
2. If the server is located in the US, use the EU-US Privacy Shield Framework to self-certify data privacy compliance. NOTE: This option is currently under legal dispute - see above.

## The Data Privacy Legislation

This document is based upon a review conducted by Wellnomics of the:

- [UK Data Protection Act 2018](#)
- [Canadian Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#)
- [Australian Privacy Act 1998](#)
- [New Zealand Privacy Act 2020](#)
- [EU General Data Protection Regulations \(GDPR\) 2018](#)

The **UK Data Protection Act** is based upon the EU GDPR. Although the UK is exiting the European Union it is unlikely to change any aspects of its Data Privacy legislation. This means its expected that complying with the GDRP will to a large degree ensure compliance with the UK Data Protection Act

The **Australian Privacy Act (1988)** is based upon 10 Australian National Privacy Principles[\*\*\*] which are similar to the principles outlined in the GDPR.

The **Canadian PIPEDA** is similar to Australian Privacy Act and can also be set to be a subset of the more strict principles in the EU GDPR.

Overall the principles enshrined within the above acts, and their relation to health and safety legislation, are expected to be representative of data privacy legislation in other countries where such legislation exists although Wellnomics has not undertaken any review of such legislation in other countries.

Generally speaking the EU GDPR are the most strict regulations and meeting these will very likely ensure that the most important legal requirements in other countries will be automatically met.

## Disclaimer

This document represents Wellnomics interpretation of data privacy legalisation and does not constitute a legal opinion. Wellnomics Ltd cannot give any guarantees as to the accuracy of the information contained herein, or the interpretations or opinions expressed. Anyone reading this information or using the Wellnomics solution is advised to take their own legal advice on meeting legislative privacy requirements.

---

[†] Although there are exceptions to this, such as using the data for aggregate purposes, or where the data is first anonymized. Furthermore, other uses can be considered if done in consultation with employees.

[‡] Sensitive data is a special distinction made in data privacy for personal data that may be seen as particularly sensitive, such as data on physical or mental health. There can be stricter requirements around handling of “sensitive” personal data.

[§] Note that the Wellnomics solution can record additional information, such as application usage, which is used by some organizations. But this data recording can be disabled by default and is not required in order to do risks analysis. For full information on what statistics Wellnomics can record see Wellnomics white paper – *What statistics does Wellnomics WorkPace record on computer use?*

[††] [http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_1](http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1)

[‡‡] <http://www.privacy.gov.au/law/act>

[§§] [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/95-46-ce/dir1995-46\\_part1\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf)

[\*\*\*] <http://www.privacy.gov.au/materials/types/infosheets/view/6583>

# Privacy Policy - Default - SaaS - Documentation

**Review period: Annual**

*This Privacy Policy is included in systems by default, but can be amended by customers*

Your privacy is important to us. It is Wellnomics' policy to respect your privacy regarding any information we may collect from you in our software and services.

## 1. Information we collect

### Log data

The Wellnomics software creates and maintains your account on our web server, with a connection to the web being required to create and validate your account, as well as access your profile as recorded and calculated by the software. When you use the software, our web server may automatically log the standard data provided by your web browser. It may include your computer's Internet Protocol (IP) address, your browser type and version, and the time and date of your access.

### Device data

If you install the Wellnomics software on your desktop or mobile device then there is also data collected on computer use (and mobile use) and breaks. This data will include time spent using the computer, mouse and keyboard, number of keystrokes, number of mouse clicks, number of breaks taken, what applications are used most and how much time is spent using each application. This data is used to calculate your wellbeing profile and provide suitable recommendations to you on improving how you use your computer to reduce your risk of injury. For example, the software may provide tips on suitable shortcut keys you can learn for the top applications you use so as to help you become more efficient and use the keyboard instead of the mouse to reduce the stress on your arms and hands. No detailed data on what you type is recorded or stored, only summary data for each day such as the total keystrokes typed for each day, or the total time using the mouse.

Your settings when using the software on your desktop or mobile device are also stored on the web server. This allows your settings to be synchronized across multiple devices and also means the software can provide you with recommendations on adjusting your settings to the best benefit.

### Personal information

As part of creating your account we may ask for personal information, such as your:

- First name and last name
- Email address
- Country
- Preferred language and timezone

This data is used to identify you in the product, to personalize the product to you, to adjust how the product operates, and to communicate with you for the purposes of password recovery and providing you automatically generated advice about improving your wellbeing at the computer.

If you are trialing the product this information may be used to contact you for sales and marketing purposes directly related to the product being trialed. Your personal information will not be provided to 3rd parties or sold, or used for any other purpose.

### Business data

Business data refers to data that accumulates over the normal course of operation on our platform. This may include transaction records, stored files, user profiles, analytics data and other metrics, as well as other types of information, created or generated, as users interact with our services.

## 2. Legal bases for processing

We will process your personal information lawfully, fairly and in a transparent manner. We collect and process information about you only where we have legal bases for doing so.

These legal bases depend on the services you use and how you use them, meaning we collect and use your information only where:

- it's necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract (for example, when we provide a service you request from us);
- it satisfies a legitimate interest (which is not overridden by your data protection interests), such as for research and development, to market and promote our services, and to protect our legal rights and interests;
- you give us consent to do so for a specific purpose (for example, you might consent to us sending you our newsletter); or
- we need to process your data to comply with a legal obligation.

Where you consent to our use of information about you for a specific purpose, you have the right to change your mind at any time (but this will not affect any processing that has already taken place).

We don't keep personal information for longer than is necessary. While we retain this information, we will protect it within commercially acceptable means to prevent loss and theft, as well as unauthorised access, disclosure, copying, use or modification. That said, we advise that no method of electronic transmission or storage is 100% secure and cannot guarantee absolute data security. If necessary, we may retain your personal information for our compliance with a legal obligation or in order to protect your vital interests or the vital interests of another natural person.

## 3. Collection and use of information

We may collect, hold, use and disclose information for the following purposes and personal information will not be further processed in a manner that is incompatible with these purposes:

- to provide you with our platform's core features;
- to enable you to access and use our website and associated applications; and
- to contact and communicate with you.

## 4. International transfers of personal information

The personal information we collect is stored and processed in United States, United Kingdom, Europe and Australia, or where we or our partners, affiliates and third-party providers maintain facilities. By providing us with your personal information, you consent to the disclosure to these overseas third parties. Generally speaking we make our best endeavors to store your information on a regional server in the same region as where you are located.

If there is any need to transfer personal information between servers we will ensure that any transfer of personal information from countries in the European Economic Area (EEA) to countries outside the EEA will be protected by appropriate safeguards, for example by using standard data protection clauses approved by the European Commission, or the use of binding corporate rules or other legally accepted means.

Where we transfer personal information from a non-EEA country to another country, you acknowledge that third parties in other jurisdictions may not be subject to similar data protection laws to the ones in our jurisdiction. There are risks if any such third party engages in any act or practice that would contravene the data privacy laws in our jurisdiction and this might mean that you will not be able to seek redress under our jurisdiction's privacy laws.

## 5. Your rights and controlling your personal information

**Choice and consent:** By providing personal information to us, you consent to us collecting, holding, using and disclosing your personal information in accordance with this privacy policy. If you are under 16 years of age, you must have, and warrant to the

extent permitted by law to us, that you have your parent or legal guardian's permission to access and use the website and they (your parents or guardian) have consented to you providing us with your personal information. You do not have to provide personal information to us, however, if you do not, it may affect your use of this website or the products and/or services offered on or through it.

**Information from third parties:** If we receive personal information about you from a third party, we will protect it as set out in this privacy policy. If you are a third party providing personal information about somebody else, you represent and warrant that you have such person's consent to provide the personal information to us.

**Restrict:** You may choose to restrict the collection or use of your personal information. If you have previously agreed to us using your personal information for direct marketing purposes, you may change your mind at any time by contacting us using the details below. If you ask us to restrict or limit how we process your personal information, we will let you know how the restriction affects your use of our website or products and services.

**Access and data portability:** You may request details of the personal information that we hold about you. You may request a copy of the personal information we hold about you. Where possible, we will provide this information in CSV format or other easily readable machine format. You may request that we erase the personal information we hold about you at any time. You may also request that we transfer this personal information to another third party.

**Correction:** If you believe that any information we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, please contact us using the details below. We will take reasonable steps to correct any information found to be inaccurate, incomplete, misleading or out of date.

**Notification of data breaches:** We will comply laws applicable to us in respect of any data breach.

**Complaints:** If you believe that we have breached a relevant data protection law and wish to make a complaint, please contact us using the details below and provide us with full details of the alleged breach. We will promptly investigate your complaint and respond to you, in writing, setting out the outcome of our investigation and the steps we will take to deal with your complaint. You also have the right to contact a regulatory body or data protection authority in relation to your complaint.

**Unsubscribe:** To unsubscribe from our e-mail database or opt-out of communications (including marketing communications), please contact us using the details below or opt-out using the opt-out facilities provided in the communication.

## 6. Cookies

We use "cookies" to collect information about you and your activity across our site. A cookie is a small piece of data that our website stores on your computer, and accesses each time you visit, so we can understand how you use our site. This helps us serve you content based on preferences you have specified.

We use cookies to help improve your experience of Wellnomics software. We also provide basic information on third-party services we may use, who may also use cookies as part of their service, though they are not covered by our policy.

If you don't wish to accept cookies from us, you should instruct your browser to refuse cookies from the Wellnomics site with the understanding that we may be unable to provide you with some of your desired content and services.

### What is a cookie?

A cookie is a small piece of data that a website stores on your device when you visit, typically containing information about the website itself, a unique identifier that allows the site to recognise your web browser when you return, additional data that serves the purpose of the cookie, and the lifespan of the cookie itself.

Cookies are used to enable certain features (eg. logging in), to store your user settings (eg. timezone, notification preferences).

Cookies set by the website you are visiting are normally referred to as "first-party cookies", and typically only track your activity on that particular site. Cookies set by other sites and companies (ie. third parties) are called "third-party cookies", and can be used to track you on other websites that use the same third-party service.

### Types of cookies and how we use them

#### Essential cookies



Essential cookies are crucial to your experience of a website, enabling core features like user logins, account management, shopping carts and payment processing.

The Wellnomics software uses Essential cookies to enable certain functions in the application.

### Performance cookies

Performance cookies are used in the tracking of how you use a website during your visit, without collecting personal information about you. Typically, this information is anonymous and aggregated with information tracked across all site users, to help companies understand visitor usage patterns, identify and diagnose problems or errors their users may encounter, and make better strategic decisions in improving their audience's overall website experience. These cookies may be set by the website you're visiting (first-party) or by third-party services.

### Functionality cookies

Functionality cookies are used in collecting information about your device and any settings you may configure on the website you're visiting (like language and timezone settings). With this information, websites can provide you with customised, enhanced or optimised content and services. These cookies may be set by the website you're visiting (first-party) or by third-party service.

The Wellnomics software does not use Functionality cookies.

### Targeting/advertising cookies

Targeting/advertising cookies are used in determining what promotional content is more relevant and appropriate to you and your interests. Websites may use them to deliver targeted advertising or to limit the number of times you see an advertisement. This helps companies improve the effectiveness of their campaigns and the quality of content presented to you. These cookies may be set by the website you're visiting (first-party) or by third-party services. Targeting/advertising cookies set by third-parties may be used to track you on other websites that use the same third-party service.

The Wellnomics software does not use Targeting/advertising cookies.

### Third-party cookies on our site

We may employ third-party companies on our websites—for example, analytics providers such as Google analytics. We grant these third parties access to selected information to perform specific tasks on our behalf. They may also set third-party cookies in order to deliver the services they are providing. Third-party cookies can be used to track you on other websites that use the same third-party service. As we have no control over third-party cookies, they are not covered by Wellnomics' cookie policy.

### Our third-party privacy promise

We review the privacy policies of all our third-party providers before enlisting their services to ensure their practices align with ours. We will never knowingly include third-party services that compromise or violate the privacy of our users.

### How you can control or opt out of cookies

If you do not wish to accept cookies from us, you can instruct your browser to refuse cookies from our website. Most browsers are configured to accept cookies by default, but you can update these settings to either refuse cookies altogether, or to notify you when a website is trying to set or update a cookie.

If you browse websites from multiple devices, you may need to update your settings on each individual device.

Although some cookies can be blocked with little impact on your experience of a website, blocking all cookies may mean you are unable to access certain features and content across the sites you visit.

## 7. Limits of our policy

Our website may link to external sites that are not operated by us. Please be aware that we have no control over the content and policies of those sites, and cannot accept responsibility or liability for their respective privacy practices.

## 8. Changes to this policy

At our discretion, we may change our privacy policy to reflect current acceptable practices. We will take reasonable steps to let users know about changes via our website. Your continued use of this site after any changes to this policy will be regarded as acceptance of our practices around privacy and personal information.

If we make a significant change to this privacy policy, for example changing a lawful basis on which we process your personal information, we will ask you to re-consent to the amended privacy policy.

Wellnomics Data Controller  
Wellnomics Ltd, New Zealand  
[support@wellnomics.com](mailto:support@wellnomics.com)

Wellnomics Data Protection Officer  
Privacy Officer  
[privacy@wellnomics.com](mailto:privacy@wellnomics.com)

This policy is effective as of 1 January 2019.

Date of Change	Responsible	Summary of change	Next revision due
01 Jan 2019	@Kevin Taylor	New document added to policies and procedure	08 Jan 2020
16 Jan 2020	@Kevin Taylor	Reviewed - no changes required	15 Jan 2021 @Kevin Taylor
21 Jan 2021	Wayne Owens	no change	20 Jan 2022 <a href="#">Kevin</a>
22 Aug 2022	<a href="#">Kevin</a>	Removed Wellnomics BV as Data Controller	30 Mar 2023

# Product Security and Best Practice - SaaS - Guidelines

**Review period:** Annual

## Contents

- Security Guidelines
- Security Training
- Log on and Authentication methods
- Password security
  - Setting and Resetting Passwords
- Secure connection to server
  - Access security to server and data - server security model
- Security against attacks
  - Brute force attacks
  - Cross-site scripting
- Database access security & data flow
- User accounts
- Penetration Testing
- Policy Compliance
  - Compliance Measurement
- Related Standards, Policies, Processes and Forms
- Revision History

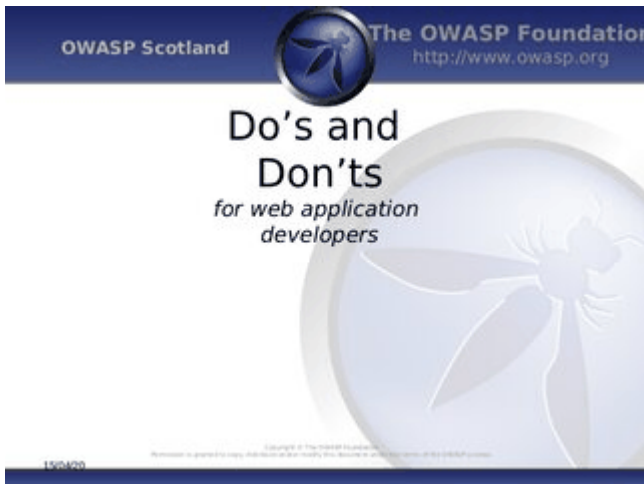
## Security Guidelines

Wellnomics uses the following guides for ensuring the security of its server applications.

- OWASP principles as specified at <https://www.owasp.org>
- [OWASP Secure Coding Practices - Quick Reference Guide](#)
- [Microsoft SDL Cryptographic Recommendations](#)

## Security Training

Developers must all review the following training OWASP PPT *Web\_Application\_Development\_Dos\_and\_Donts* when joining the company



## Log on and Authentication methods

Each UserID is unique and is based upon either the user's email address, or on a unique User ID provided by the organization as part of the HR data feed.

The user accesses the system through their browser. After 20 minutes of inactivity there is an automatic timeout/logout after which the user must log back in again. Note this does not apply to systems using Single Sign On. In this case the session will time out, but the user will not need to log back in.

The software can be configured for authentication using one of the following methods:

- **OAuth / OpenID:** A 'single sign on' authentication method that works across the internet for hosted systems.
- **Forms authentication:** Requires each user to provide a username and password through a login screen.

Use of a login reCAPTCHA is supported to improve security against automated attacks.

## Password security

A minimum password strength can be enforced, with three levels available:

- **Weak:** Password length of 6 characters or more. e.g. "smithw"
- **Medium:** Password length of 6 characters or more. Password must contain at least 1 uppercase character, 1 lowercase character and 1 number. e.g. "Smith3"
- **Strong:** Password length of 8 characters or more. Password must contain at least 1 uppercase character, 1 lowercase character, 1 number and 1 special character. e.g. "Smith!34"

Default password level is always Strong.

Passwords are all stored as **hashed and salted** values in the database using a **SHA256 based algorithm**. This means it is not possible to identify passwords by gaining access to the database. If a user forgets their password they are provided with a password reset link in order to create new password (meeting the current password strength policy). At no time are any passwords sent by e-mail or displayed onscreen. This means the only way a password can be revealed is either by the user revealing it themselves, or via a 'brute force' attack- something that is also protected against (see below).

## Setting and Resetting Passwords

While this is not required when using OAuth/OpenID, if the Portal site is configured to **Forms Authentication** then to set or reset a password requires the following steps:

1. A time limited password set/reset link is emailed to the user. Clicking on this link opens the user's browser with https in which they can create their password.

2. The password is hidden while being typed.
3. The user is required to enter their password twice to verify it.
4. Password strength feedback is provided telling the user if they meet the minimum requirements for passwords (see above Weak, Medium, Strong)

At no time is the user's password emailed to them. No use is made of temporary passwords.

## Secure connection to server

TLS 1.2 is used for ALL communication with the Wellnomics SaaS server. This includes:

- All communication between a user's browser and the Wellnomics SaaS server. This means neither login passwords nor other sensitive data can be captured from TCP/IP packets.
- All communication between the Wellnomics App running on a desktop (Windows, MacOS or Linux) or mobile device (iOS or Android) and the Wellnomics SaaS server.

Before the App can communicate with the SaaS the user must first perform an authentication on that device to verify they have the privileges to connect. This is achieved through the App opening the user's browser and asking them to log into the SaaS with their user account (this may then occur automatically if OAuth is being used). If authentication is successful an authentication token is provided to and saved by the App. This token is locked to a unique ID on the user's computer/device and their SaaS account and is stored securely by the App. This token must then be supplied in any future communication with the server.

## Access security to server and data - server security model

For more information on **Wellnomics Remote Access** to hosted servers refer to [Access Security - Hosting - Policy](#) .

## Security against attacks

### Brute force attacks

The Wellnomics solution has an enforced 1 second delay between repeated failed login attempts (illustrated by the Login button disabling temporarily for 1 second after each click), meaning that it is not practical for automated software to identify a password through a brute force attack. Protection has also been added against brute force password dictionary attacks.

### Cross-site scripting

Protection against cross-site scripting (XSS) Intensive testing has been undertaken to ensure that the software is not vulnerable to Cross Site Scripting (XSS) attack. For an explanation of the techniques mentioned below please refer to the following article [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting).

**Non-Persistent:** All web pages have been developed following best practice security standards specified in Microsoft's Basic Security Practices for Web Applications (see <http://msdn.microsoft.com/enus/library/zdh19h94.aspx>). This ensures no data entry fields are prone XSS attacks.

**Persistent:** All entry fields use the Microsoft's WebControls.TextBox class which validates input and prevents users from entering HTML snippets containing <script> or other malicious tags. SQL Injection All input fields use parameterized SQL statements to avoid any attack paths. Intensive testing has been done to ensure that the Wellnomics system is not vulnerable to SQL Injection attacks. For an explanation of the types of attack the Wellnomics system is protected against see [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection).

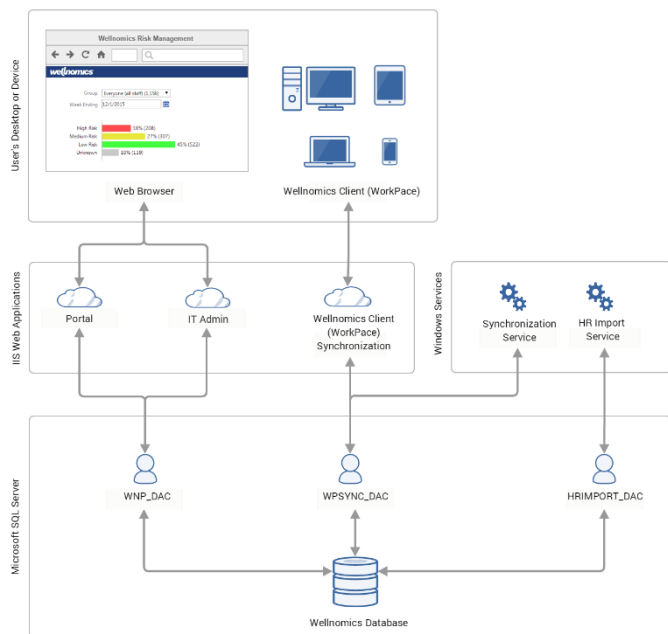
## Database access security & data flow

At the database level a data layer is used for all data access and requires a valid user token to be provided when requesting any data. Then only the data matching that user token (or which that user is allowed to access) is provided. The token is generated based upon the users authentication and login - is not something the user has access to.

Every report or request checks the user's rights and permissions for the requested data and will refuse request if not valid. This means, for example, you can't trick the system by editing the URL to put in the name of a report you shouldn't have access to, or by editing query parameters in a URL.

To ensure data security and data separation for each customer, each customer's data is stored on a logically separate SQL database and a separate application instance is run for each customer accessing this application. It is not possible to access data for another customer from the current customer's application.

Below is a data flow diagram for the system.



## User accounts

There are no default accounts on the system. There is an IT Administrator account created when the system is installed, and this account can be used to select which user is the Wellnomics Administrator, who has the highest privileges.

User accounts are automatically created and disabled/archived based upon a regular HR data feed listing active users. If a new user is added to the HR data feed, then a new user account will be created for this user. If an existing user is removed from the HR data feed, then this use will have their account automatically archived and disabled.

As well as the Wellnomics Administrator, which is the highest privilege account type there are also the following higher privilege account types:

- **Manager:** Defined automatically by having one more staff reporting to them in the HR data feed. The privileges are automatically added or removed based upon the HR data feed.
- **Local Administrator:** Selected manually by the Wellnomics Administrator, who can then choose what rights the Local Administrator has.

## Penetration Testing

Automated penetration testing using a 3rd party penetration testing tool and expert external manual penetration testing is performed regularly. See elsewhere for [Security and Penetration Testing - Policy](#)

## Policy Compliance

### Compliance Measurement

Compliance with this policy will be verified through an annual review which will verify that the product functionality is still operating as per the above guidelines. Compliance will also be verified through the Security and Penetration Testing processes including SAST, DAST functions which are expected to identify security vulnerabilities if the above are not implemented correctly.

## Related Standards, Policies, Processes and Forms

- [Product Threat Modeling - Policy](#)
- [Product Security Risk Assessment - SaaS \(Sep 2020\)](#)
- [Security and Penetration Testing - Policy](#)
- [SaaS Security and Penetration Testing - Guidelines](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
30 Mar 2016	Wayne Owens, Principal Consultant	Updated and converted to new format.	29 Mar 2017 <a href="#">Wayne Owens (Unlicensed)</a>
03 Jul 2017	Wayne Owens, Principal Consultant	Updated aspects relating to the use of licensed software for dedicated hosted server maintenance workstation	04 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
17 May 2018	Kevin Taylor, CEO	Updated section on Backups for cloud servers.	04 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay	Reviewed, no changes made	
1 March 2019	Kevin Taylor	Updated requirements on server patches and hardening and Microsoft Azure backups policies	<ul style="list-style-type: none"> <li>• 01 Mar 2020 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
22 May 2020	Wayne Owens	Reviewed and updated to change references from Microsoft Azure to Microsoft Azure	<ul style="list-style-type: none"> <li>• 21 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
31 Aug 2020	Angeli Arino	Reviewed, no changes made	
28 Sep 2020	Kevin Taylor	Added diagrams for access security and logical data which were in other documentation	<ul style="list-style-type: none"> <li>• 28 Sep 2021 <a href="#">Ian Bartram</a></li> </ul>
05 May 2022	<a href="#">Kevin</a>	Updated to include latest guidelines such as protection against dictionary attacks.	<ul style="list-style-type: none"> <li>• 06 May 2023 <a href="#">Kevin</a></li> </ul>
09 May 2023	<a href="#">Kevin</a>	Reviewed - no changes required	<ul style="list-style-type: none"> <li>• 08 May 2024</li> </ul>

# Product Security and Best Practice - App - Guidelines

Review period: Annual

## Security References

Wellnomics uses the following guides for ensuring the security of its desktop and mobile applications.

- OWASP principles as specified at <https://www.owasp.org>
- [OWASP Secure Coding Practices - Quick Reference Guide](#)
- [Microsoft SDL Cryptographic Recommendations](#)
- [The SSL Conservatory](#)
- [The most dangerous code in the world: validating SSL certificates in non-browser software](#), Paper published by Stanford University, 2012

## Guidelines and Best Practice

### File security

Guideline	Details	Product Requirements to meet Guideline
<ul style="list-style-type: none"><li>• Personal user data and settings should be stored in a single location</li></ul>		<p><b>WorkPace Classic</b></p> <p>User settings and user data stored in two separate files in user's personal appdata roaming folder on device</p> <p><b>Wellnomics Client App</b></p> <p>User settings and user data stored in single files in user's personal appdata roaming folder on device</p>



<ul style="list-style-type: none"> <li>Personal user data and user settings files should be encoded or encrypted in such a way that a 3rd party having a copy of the file by itself would not be able to read valid data from it.</li> </ul>	<ul style="list-style-type: none"> <li>3rd party should not be able to build or obtain a tool that would allow them to decode or decrypt all files later received. This means any encryption should use a different key for each user - there is no common encryption key that is encoded into the source code that would allow a hacker to decompile a copy of the client app to retrieve the key, and thereby gain the ability to decode any future files they gained access to.</li> <li>It may, however, be possible that the personal data file can be read if the 3rd party has complete access to the user's computer and all the files on it. Wellnomics assumes that the user's computer is secure. If the user's computer is compromised and a 3rd party has access to all user files it may be possible to decode/unencrypt and read the personal user data. However, Wellnomics will endeavor to ensure that this will not be a straightforward process even if it did happen - the 3rd party would need to be a sophisticated hacker of some sort and would need to take several steps requiring technical expertise to be able to read the data.</li> </ul>	<p><b>WorkPace Classic</b></p> <p>User settings and user data files are stored in a propriety encoded format that is not easily readable or decodeable by a 3rd party, but the data is not encrypted.</p> <p><b>Wellnomics Client App</b></p> <p>User settings and user data are in a single key encrypted SQLite database file. The key is different for each user and is based upon a unique token generated from the user's credentials, thus making it difficult for anyone to reverse engineer.</p>
<ul style="list-style-type: none"> <li>Configuration files will not store settings data that could affect the product behaviour in any significant manner (aside from branding or text changes), or any modifications to configuration files, such as changing server addresses or communication protocol parameters will be guaranteed to cause an obvious failure in the product operation or communication in such a way that no data or communication is compromised.</li> </ul>		<p>An existing already validated authentication token must be supplied to server at the beginning of any communication. If this does not match the token the user already has for that user then the communication will fail or the user will be asked to reauthenticate with an explanation. The user can then make the choice to reauthenticate against the new server if they wish (i.e. if the change was intentional and expected).</p>

## Communication Security

Guideline	Comments	Product Requirements to meet Guideline
-----------	----------	--

<p><b>All communication should be encrypted</b></p> <ul style="list-style-type: none"> <li>• All communication should be encrypted, except for a initial hello.</li> <li>• Use a best practice market accepted encryption technology with proven security and no currently known exploits.</li> <li>• Never send plain text passwords, even in SSL. All passwords should be hashed and salted.</li> </ul>		<ul style="list-style-type: none"> <li>• TLS 1.2 or above only protocol used for all communication.</li> <li>• <b>Failure handling:</b> Client app communication log shows a error upon sync with server if requirement not met.</li> </ul>
<ul style="list-style-type: none"> <li>• Ensure we have a valid certificate for the encryption technology. If any of these verification tests fail, the product should terminate the connection with the server or other entity.</li> <li>• <b>Domain name:</b> Validate that the certificate is correctly issued to the domain you're communicating with. ✓</li> <li>• <b>Validity dates</b> (both beginning and expiration dates): Ensure current date time is within the beginning and expiration dates. ✓</li> <li>• <b>Revocation status:</b> Ensure certificate has not been revoked before the expiration date. ✓</li> <li>• <b>Trust chain:</b> Certificate should chain to a root certification authority (CA) that is trusted by the platform or explicitly configured by the administrator. ✓</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Usage</b> (for example, "Server Authentication" for servers, "Client Authentication" for clients): We will not check this for Wellnomics products as this could cause issue with customer self-issued certificates when customer-hosted. Not seen as a critical security issue.</li> <li>• <b>Revocation status:</b> Best practice is simply to warn about this, as we cannot guarantee revocation status is fully reliable. <i>See more on this decision below</i></li> </ul>	<p><b>Failure handling</b></p> <ul style="list-style-type: none"> <li>• <b>Domain name:</b> Client app communication log shows a Domain Name validation error upon sync with server.</li> <li>• <b>Validity dates:</b> Client app communication log shows a Validity dates error upon sync with server.</li> <li>• <b>Revocation status:</b> Client app communication log shows a Certificate Revocation error in the log, but continues the sync with server</li> <li>• <b>Trust chain:</b> Client app communication log shows a Trust Chain validation error upon sync with server</li> </ul>
<ul style="list-style-type: none"> <li>• Ensure as short a timeout as is reasonable as this makes it harder for an exploit to be activated to exploit an open communication window.</li> </ul>		<ul style="list-style-type: none"> <li>• <b>Timeout Default = 10 seconds:</b> By default 10 second timeout should be used for all communications, unless a specific use case requires something longer.</li> </ul>
<ul style="list-style-type: none"> <li>• Aim for safely fail rather than fail safe. We should not write our product functionality on the basis we will be able to make the product fail safe. We should assume that any action or process may fail, and ensure that any failure that may be theoretically possible is anticipated and handled in a safe manner i.e. there is error handling for every communication failure (including logging the failure so that we have evidence that can later be analyzed)</li> </ul>		<ul style="list-style-type: none"> <li>• <b>Communication channel error handling:</b> for All communication code should include error handling for when communications fails or an unexpected error occurs. The default behaviour should always be to terminate connection and log an error in application logs.</li> </ul>

# Checking Revocation Status

The decision was made to not support revocation status checking in WPC as the complexities on implementing this for the various methods of checking would require significant development overhead with little added security to the end user. We have reviewed RFC5280 (<https://www.ietf.org/rfc/rfc5280.txt>) and concluded that if this were to be implemented a soft fail implementation would be required, i.e. the client would continue to sync if the check was unable to be completed. This is the case because not all certificates are required to be issued with revocation checking capabilities (this is especially true for internally issued certificates) and this would be building in a single point of failure for the client which is not something we want to do.

Adam Langley from Google provides a good write up on the thinking behind the pitfalls of revocation checking (<https://www.imperialviolet.org/2012/02/05/crlsets.html>)

For WC app we will look to implement warnings only.

## Policy Compliance

### Compliance Measurement

Compliance with this policy will be verified through an annual review which will verify that the product functionality is still operating as per the above guidelines. Compliance will also be verified through the Security and Penetration Testing processes including SAST, DAST functions which are expected to identify security vulnerabilities if the above are not implemented correctly.

## Related Standards, Policies, Processes and Forms

- [Product Threat Modeling - Policy](#)
- [Wellnomics App Security Risk Assessment - Mar 2021](#)
- [Security and Penetration Testing - Policy](#)
- [Security Testing of Client - Guide](#)

## Revision history

Date of change	Responsible	Summary of change	Next revision date
10 Apr 2019	Kevin Taylor	Created as new addition to policy set	13 Apr 2020
20 May 2020	Wayne Owens, Principal Consultant	Reviewed, no changes required	
24 Aug 2020	Angeli Arino	Converted to a new page	
26 Oct 2020	<a href="#">Kevin</a>	Added the "OWASP Secure Coding Practices Quick Reference Guide" from Development pages	
11 Nov 2020	<a href="#">Kevin</a>	Added notes & section on revocation status	<ul style="list-style-type: none"><li>• 10 Nov 2021 <a href="#">Ian Bartram</a></li></ul>
16 Nov 2021	<a href="#">Ian Bartram</a>	Reviewed, minor updates only	<ul style="list-style-type: none"><li>• 15 Nov 2022 <a href="#">Ian Bartram</a></li></ul>
26 Jan 2023	<a href="#">Ian Bartram</a>	Reviewed, no changes required	<ul style="list-style-type: none"><li>• 02 Feb 2024 <a href="#">Ian Bartram</a></li></ul>

# Access Security - SaaS - Documentation

**Review period:** Annual

- Log on and Authentication methods
  - Log in Timeout
- Secure connection to server
- Access security to server and data - server security model
- Password security
  - Setting and Resetting Passwords
- Security against brute force attacks
  - Non-Persistent
  - Persistent
- Database access security & data flow
- User accounts
- Policy Compliance
  - Compliance Measurement
- Related Standards, Policies, Processes and Forms
- Revision History

## Log on and Authentication methods

Each UserID is unique and is based upon either the user's email address, or on a unique User ID provided by the organization as part of the HR data feed.

### Log in Timeout

The user accesses the system through their browser. After 20 minutes of inactivity there is an automatic timeout/logout after which the user must log back in again. Note this does not apply to systems using Single Sign On. In this case the session will time out, but the user will not need to log back in.

The software can be configured for authentication using one of the following methods:

- **OAuth / OpenID:** A 'single sign on' authentication method that works across the internet for hosted systems.
- **Forms authentication:** Requires each user to provide a username and password through a login screen.
- **Windows Authentication (automatic or Single Sign-On):** Only available when internally hosted.

## Secure connection to server

TLS 1.2 is used for ALL communication with the Wellnomics SaaS server. This includes:

- All communication between a user's browser and the Wellnomics SaaS server. This means neither login passwords nor other sensitive data can be captured from TCP/IP packets.
- All communication between the Wellnomics Client App (e.g. WorkPace) running on a desktop (Windows, MacOS or Linux) or mobile device (iOS or Android) and the Wellnomics SaaS server.

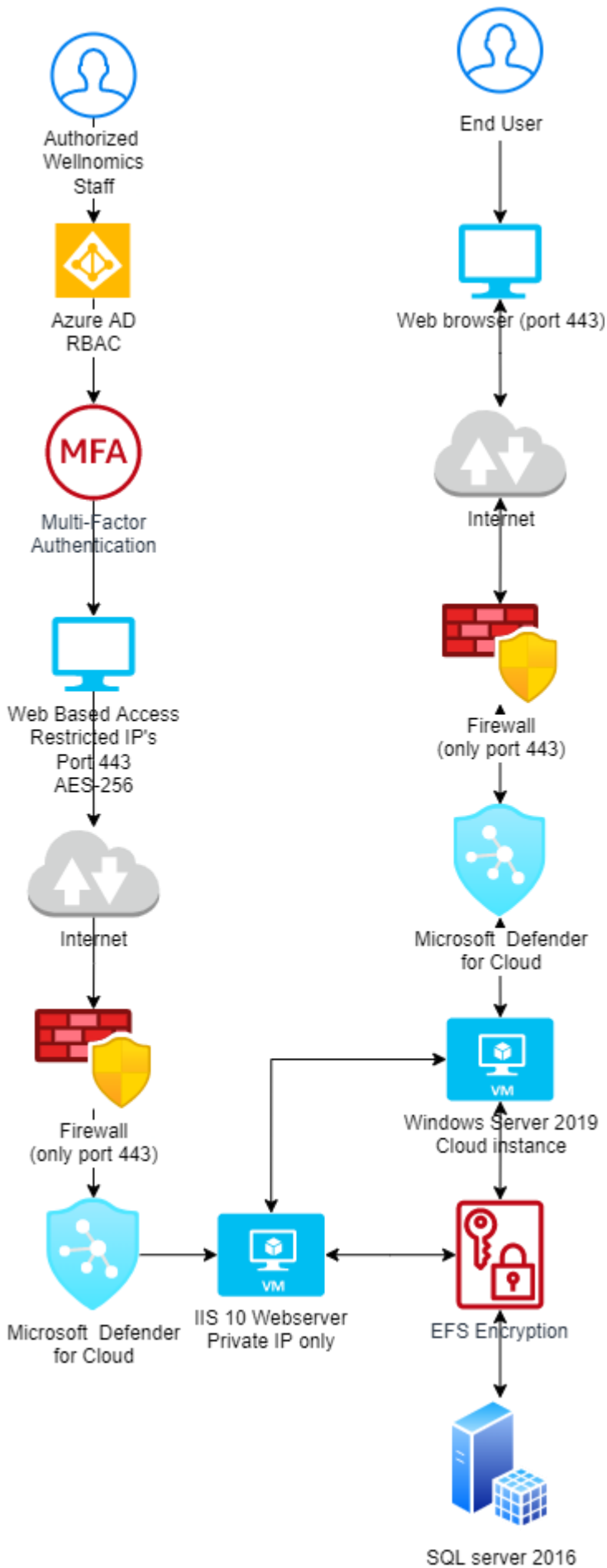
The data sent by the Client is additionally authenticated using domain name, user name and the license key. All data packets not matching a registered user or having an invalid license key are rejected by the server.

At the app level authentication is either by requiring a match between the domain/username provided from the Single Sign On server and the user's desktop login, or a second alternative option is based around the users email address, with the user required to authenticate via their email to create an account, then authenticate against this account on any new device they start using (with an authentication token then being stored on the device (laptop or mobile). This token must then be supplied in any future communication with the server.

Intensive testing has been completed to ensure that the Wellnomics server is not susceptible to any form of attack, including buffer overflows.

## Access security to server and data - server security model

The available access options and data routes are outlined below. Note this diagram will be superseded shortly by separate documentation covering [Threat Modelling - SaaS - Documentation](#) and [Threat Modeling - Hosting - Documentation](#)



Created in <https://www.draw.io/>, you can import the XML file below if any changes need to be made.

Wellnomics\_hosted\_Topolo...

## Password security

If using Forms Authentication a minimum password strength can be enforced, with three levels available:

- **Weak:** Password length of 6 characters or more. e.g. "smithw"
- **Medium:** Password length of 6 characters or more. Password must contain at least 1 uppercase character, 1 lowercase character and 1 number. e.g. "Smith3"
- **Strong:** Password length of 8 characters or more. Password must contain at least 1 uppercase character, 1 lowercase character, 1 number and 1 special character. e.g. "Smith!34"

Passwords are all stored as **hashed and salted** values in the database using a **SHA256 based algorithm**. This means it is not possible to identify passwords by gaining access to the database. If a user forgets their password they are provided with a password reset link in order to create new password (meeting the current password strength policy). At no time are any passwords sent by e-mail or displayed onscreen. This means the only way a password can be revealed is either by the user revealing it themselves, or via a 'brute force' attack- something that is also protected against (see below).

## Setting and Resetting Passwords

While this is not required when using Windows Authentication (SSO), if the Portal site is configured to **Forms Authentication** then to set or reset a password requires the following steps:

1. A time limited password set/reset link is emailed to the user. Clicking on this link opens the user's browser with https in which they can create their password.
2. The password is hidden while being typed.
3. The user is required to enter their password twice to verify it.
4. Password strength feedback is provided telling the user if they meet the minimum requirements for passwords (see above Weak, Medium, Strong)

At no time is the user's password emailed to them. No use is made of temporary passwords.

## Security against brute force attacks

The Wellnomics solution has an enforced 1 second delay between repeated failed login attempts (illustrated by the Login button disabling temporarily for 1 second after each click), meaning that it is not practical for automated software to identify a password through a brute force attack. Protection against cross-site scripting (XSS) Intensive testing has been undertaken to ensure that the software is not vulnerable to Cross Site Scripting (XSS) attack. For an explanation of the techniques mentioned below please refer to the following article [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting).

### Non-Persistent

All web pages have been developed following best practice security standards specified in Microsoft's Basic Security Practices for Web Applications (see <http://msdn.microsoft.com/enus/library/zdh19h94.aspx>). This ensures no data entry fields are prone XSS attacks.

### Persistent

All entry fields use the Microsoft's WebControls.TextBox class which validates input and prevents users from entering HTML snippets containing <script> or other malicious tags. SQL Injection All input fields use parameterized SQL statements to avoid any attack paths. Intensive testing has been done to ensure that the Wellnomics system is not vulnerable to SQL Injection attacks. For an explanation of the types of attack the Wellnomics system is protected against see [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection).

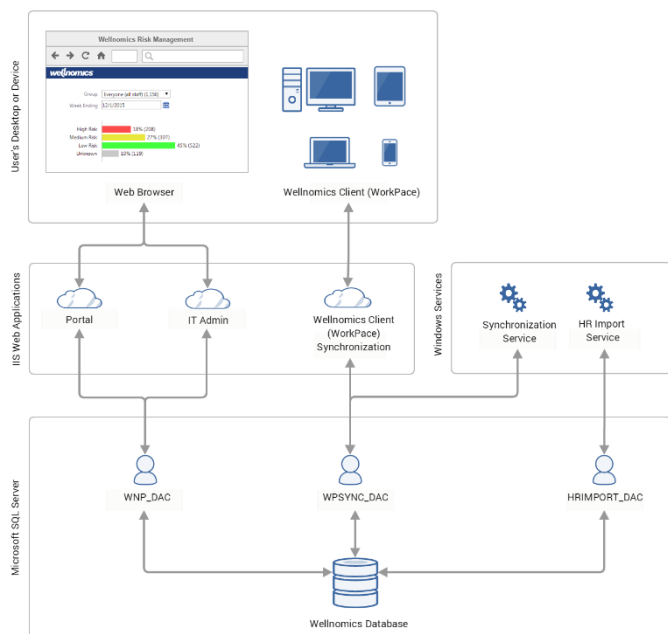
## Database access security & data flow

At the database level a data layer is used for all data access and requires a valid user token to be provided when requesting any data. Then only the data matching that user token (or which that user is allowed to access) is provided. The token is generated based upon the users authentication and login - is not something the user has access to.

Every report or request checks the user's rights and permissions for the requested data and will refuse request if not valid. This means, for example, you can't trick the system by editing the URL to put in the name of a report you shouldn't have access to, or by editing query parameters in a URL.

To ensure data security and data separation for each customer, each customer's data is stored on a logically separate SQL database and a separate application instance is run for each customer accessing this application. It is not possible to access data for another customer from the current customer's application.

Below is a data flow diagram for the system.



## User accounts

There are no default accounts on the system. There is an IT Administrator account created when the system is installed, and this account can be used to select which user is the Wellnomics Administrator, who has the highest privileges.

User accounts are automatically created and disabled/archived based upon a regular HR data feed listing active users. If a new user is added to the HR data feed, then a new user account will be created for this user. If an existing user is removed from the HR data feed, then this use will have their account automatically archived and disabled.

Higher privilege accounts are of two types:

- **Manager:** Defined automatically by having one more staff reporting to them in the HR data feed. The privileges are automatically added or removed based upon the HR data feed.
- **Local Administrator:** Selected manually by the Wellnomics Administrator, who can then choose what rights the Local Administrator has.



# Policy Compliance

## Compliance Measurement

Compliance with this policy will be verified through an annual review which will verify that the product functionality is still operating as per the above guidelines. Compliance will also be verified through the Security and Penetration Testing processes including SAST, DAST functions which are expected to identify security vulnerabilities if the above are not implemented correctly.

## Related Standards, Policies, Processes and Forms

- [Product Threat Modeling - Policy](#)
- [Product Security Risk Assessment - SaaS \(Sep 2020\)](#)
- [Security and Penetration Testing - Policy](#)
- [SaaS Security and Penetration Testing - Guidelines](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
30 Mar 2016	Wayne Owens, Principal Consultant	Updated and converted to new format.	29 Mar 2017 <a href="#">Wayne Owens (Unlicensed)</a>
03 Jul 2017	Wayne Owens, Principal Consultant	Updated aspects relating to the use of licensed software for dedicated hosted server maintenance workstation	04 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
17 May 2018	Kevin Taylor, CEO	Updated section on Backups for cloud servers.	04 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay	Reviewed, no changes made	
1 March 2019	Kevin Taylor	Updated requirements on server patches and hardening and Microsoft Azure backups policies	• 01 Mar 2020 <a href="#">Chris MacKay (Deactivated)</a>
22 May 2020	Wayne Owens	Reviewed and updated to change references from Microsoft Azure to Microsoft Azure	• 21 May 2021 <a href="#">Chris MacKay (Deactivated)</a>
31 Aug 2020	Angeli Arino	Reviewed, no changes made	
28 Sep 2020	Kevin Taylor	Added diagrams for access security and logical data which were in other documentation	• 28 Sep 2021 <a href="#">Ian Bartram</a>
17 May 2022	Ian Bartram	Updated Access diagram	• 17 May 2023 <a href="#">Ian Bartram</a>
05 Jul 2022	Ian Bartram	Reviewed, no changes made	• 17 May 2024 <a href="#">Ian Bartram</a>

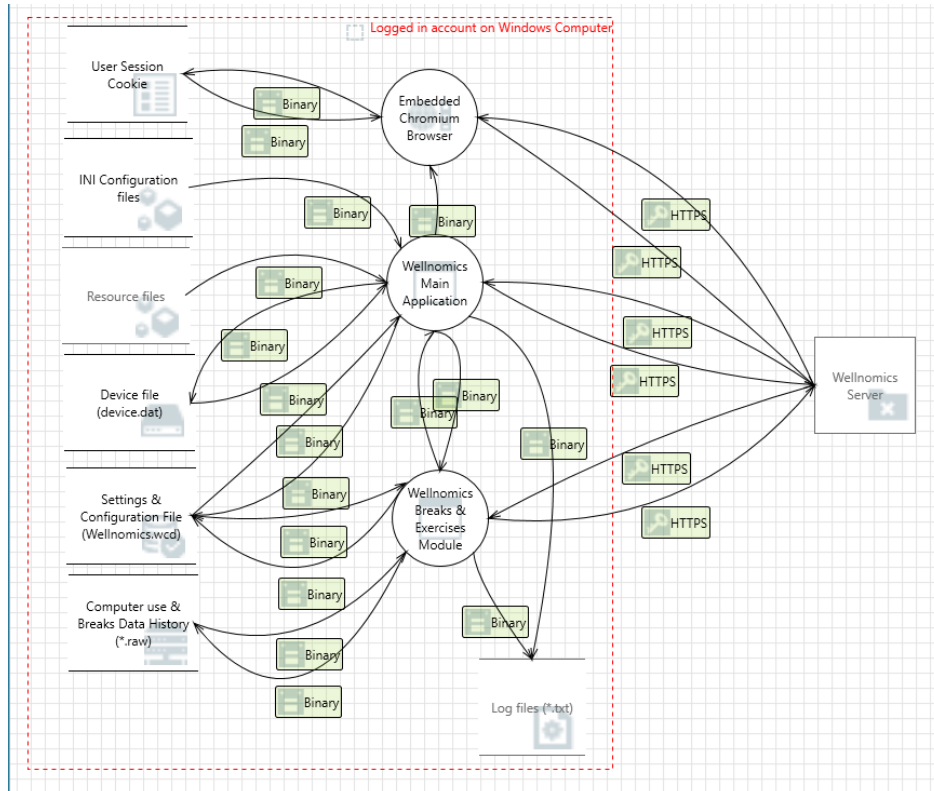
# Threat Modelling - App - Documentation

Review period: Annual

See also [Threat Modelling - SaaS - Documentation](#) and [Threat Modeling - Hosting - Documentation](#)

Created using Microsoft Threat Modelling App (see file below - you will need to download Microsoft Threat Modelling tool)

## Threat Model



Wellnomics App Threat Mo...

## Threat Analysis and Mitigation

The threat review generated by the MS Threat Modelling tool is below.

The table below analyses each of these threats, rates their risks according to [Product Security Risk Assessment Matrix - Policy](#) and explains how each risk is mitigated, where mitigation is necessary.

Table with each row showing:

- Risk from MS Threat model
- Risk Rating (High/Medium/Low)

- *Explanation (why its given this rating)*
- *Mitigation (explanation of how risk is mitigated if its High or Medium risk).*

<b>Id</b>	<b>Category</b>	<b>Title</b>	<b>Risk Description</b>	<b>Interaction</b>	<b>Risk Rating</b>	<b>Risk Explanation</b>	<b>Mitigation</b>
248	Denial Of Service	Data Flow HTTPS Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	HTTPS	Low	<ul style="list-style-type: none"> <li>• Thread ID: 6 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
247	Denial Of Service	Potential Process Crash or Stop for Embedded Chromium Browser	Embedded Chromium Browser crashes, halts, stops or runs slowly; in all cases violating an availability metric.	HTTPS	High	<ul style="list-style-type: none"> <li>• Server related</li> </ul>	N/A
200	Denial Of Service	Data Flow HTTPS Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	HTTPS	Low	<ul style="list-style-type: none"> <li>• Thread ID: 6 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
195	Denial Of Service	Data Flow HTTPS Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	HTTPS	Low	<ul style="list-style-type: none"> <li>• Thread ID: 6 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
194	Denial Of Service	Potential Process Crash or Stop for Wellnomics Main Application	Wellnomics Main Application crashes, halts, stops or runs slowly; in all cases violating an availability metric.	HTTPS	Medium	<ul style="list-style-type: none"> <li>• The execution of the WC in this regard is continuously being maintained and tested</li> </ul>	No action required
192	Denial Of Service	Data Flow HTTPS Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	HTTPS	Low	<ul style="list-style-type: none"> <li>• Thread ID: 6 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
243	Denial Of Service	Potential Excessive Resource Consumption for Embedded Chromium Browser or User Session Cookie	Does Embedded Chromium Browser or User Session Cookie take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Binary	Low	<ul style="list-style-type: none"> <li>• Chromium browser has mitigation for this vulnerability</li> </ul>	No action required
142	Denial Of Service	Potential Excessive Resource Consumption for Wellnomics Breaks & Exercises Module or Settings & Configuration File (Wellnomics.wcd)	Does Wellnomics Breaks & Exercises Module or Settings & Configuration File (Wellnomics.wcd) take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Binary	Low	<ul style="list-style-type: none"> <li>• WCD does not require a large footprint and will not drastically increase in size</li> </ul>	No action required
187	Denial Of Service	Data Flow HTTPS Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	HTTPS	Low	<ul style="list-style-type: none"> <li>• Thread ID: 6 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"

277	Denial Of Service	Potential Excessive Resource Consumption for Wellnomics Main Application or Device file (device.dat)	Does Wellnomics Main Application or Device file (device.dat) take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Binary	Low	<ul style="list-style-type: none"> <li>Device.dat only contains the device id information and will not drastically increase in size.</li> </ul>	No action required
206	Denial Of Service	Potential Excessive Resource Consumption for Wellnomics Main Application or Log files (*.txt)	Does Wellnomics Main Application or Log files (*.txt) take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Binary	Low	<ul style="list-style-type: none"> <li>Log files do increase in size, especially with trace debugging, but should not affect the performance of the WC application.</li> <li>In the past, we have been able to generate a 2GB trace log and the client was still able to run. Of course, trace logging is only known by the developers.</li> </ul>	No action required
203	Denial Of Service	Potential Excessive Resource Consumption for Wellnomics Breaks & Exercises Module or Log files (*.txt)	Does Wellnomics Breaks & Exercises Module or Log files (*.txt) take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Binary	Low	<ul style="list-style-type: none"> <li>Log files do increase in size, especially with trace debugging, but should not affect the performance of the WC application.</li> <li>In the past, we have been able to generate a 2GB trace log and the client was still able to run. Of course, trace logging is only known by the developers.</li> </ul>	No action required
186	Denial Of Service	Potential Process Crash or Stop for Wellnomics Breaks & Exercises Module	Wellnomics Breaks & Exercises Module crashes, halts, stops or runs slowly; in all cases violating an availability metric.	HTTPS	High	<ul style="list-style-type: none"> <li>The execution of the WC in this regard is continuously being maintained and tested</li> </ul>	N/A
124	Denial Of Service	Potential Excessive Resource Consumption for Wellnomics Main Application or Settings & Configuration File (Wellnomics.wcd)	Does Wellnomics Main Application or Settings & Configuration File (Wellnomics.wcd) take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Binary	Low	<ul style="list-style-type: none"> <li>WCD does not require a large footprint and will not drastically increase in size</li> </ul>	No action required
157	Denial Of Service	Potential Excessive Resource Consumption for Wellnomics Breaks & Exercises Module or Computer use & Breaks Data History (*.raw)	Does Wellnomics Breaks & Exercises Module or Computer use & Breaks Data History (*.raw) take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Binary	Low	<ul style="list-style-type: none"> <li>The raw file does not require a large footprint and will not drastically increase in size</li> </ul>	No action required
254	Denial Of Service	Data Flow HTTPS Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	HTTPS	Low	<ul style="list-style-type: none"> <li>Thread ID: 6 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"

249	Elevation Of Privilege	Elevation Using Impersonation	Embedded Chromium Browser may be able to impersonate the context of Wellnomics Server in order to gain additional privilege.	HTTPS	Low	<ul style="list-style-type: none"> <li>Not Applicable - Communication can't be facilitated through this method</li> </ul>	N/A
30	Elevation Of Privilege	Elevation Using Impersonation	Wellnomics Breaks & Exercises Module may be able to impersonate the context of Wellnomics Server in order to gain additional privilege.	HTTPS	Low	<ul style="list-style-type: none"> <li>Not Applicable - Communication can't be facilitated through this method</li> </ul>	N/A
257	Elevation Of Privilege	Cross Site Request Forgery	Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The user browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, ... The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.	HTTPS	Low	<ul style="list-style-type: none"> <li>We dont have cross site scripting in the browser.</li> </ul>	N/A
197	Elevation Of Privilege	Elevation by Changing the Execution Flow in Wellnomics Main Application	An attacker may pass data into Wellnomics Main Application in order to change the flow of program execution within Wellnomics Main Application to the attacker's choosing.	HTTPS	Medium	<ul style="list-style-type: none"> <li>Threat ID: 8 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
196	Elevation Of Privilege	Wellnomics Main Application May be Subject to Elevation of Privilege Using Remote Code Execution	Wellnomics Server may be able to remotely execute code for Wellnomics Main Application.	HTTPS	Low	<ul style="list-style-type: none"> <li>There is no server code that executes code (with any potential threat) to the client</li> </ul>	No action required

255	Elevation Of Privilege	Cross Site Request Forgery	Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, ... The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.	HTTPS	Low	<ul style="list-style-type: none"> <li>We don't have cross site scripting in the browser.</li> </ul>	N/A
189	Elevation Of Privilege	Elevation by Changing the Execution Flow in Wellnomics Breaks & Exercises Module	An attacker may pass data into Wellnomics Breaks & Exercises Module in order to change the flow of program execution within Wellnomics Breaks & Exercises Module to the attacker's choosing.	HTTPS	Low	<ul style="list-style-type: none"> <li>Threat ID: 8 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
188	Elevation Of Privilege	Wellnomics Breaks & Exercises Module May be Subject to Elevation of Privilege Using Remote Code Execution	Wellnomics Server may be able to remotely execute code for Wellnomics Breaks & Exercises Module.	HTTPS	Low	<ul style="list-style-type: none"> <li>There is no server code that executes code (with any potential threat) to the client</li> </ul>	No action required
182	Elevation Of Privilege	Elevation Using Impersonation	Wellnomics Main Application may be able to impersonate the context of Wellnomics Server in order to gain additional privilege.	HTTPS	Low	<ul style="list-style-type: none"> <li>Not Applicable - Communication can't be facilitated through this method</li> </ul>	N/A
250	Elevation Of Privilege	Embedded Chromium Browser May be Subject to Elevation of Privilege Using Remote Code Execution	Wellnomics Server may be able to remotely execute code for Embedded Chromium Browser.	HTTPS	Low	<ul style="list-style-type: none"> <li>The chromium browser is sandboxed which mitigates this attack. There is an ongoing process for active mitigation for this</li> </ul>	N/A
251	Elevation Of Privilege	Elevation by Changing the Execution Flow in Embedded Chromium Browser	An attacker may pass data into Embedded Chromium Browser in order to change the flow of program execution within Embedded Chromium Browser to the attacker's choosing.	HTTPS	Low	<ul style="list-style-type: none"> <li>Threat ID: 8 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"

241	Information Disclosure	Weak Access Control for a Resource	Improper data protection of User Session Cookie can allow an attacker to read information not intended for disclosure. Review authorization settings.	Binary	Low	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>Stored the same way as a Google Chrome browser</li> </ul>	See threat ID + Corresponding "Action Required"
130	Information Disclosure	Weak Access Control for a Resource	Improper data protection of INI Configuration files can allow an attacker to read information not intended for disclosure. Review authorization settings.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
165	Information Disclosure	Authorization Bypass	Can you access Settings & Configuration File (Wellnomics.wcd) and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
279	Information Disclosure	Weak Access Control for a Resource	Improper data protection of Device file (device.dat) can allow an attacker to read information not intended for disclosure. Review authorization settings.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
276	Information Disclosure	Authorization Bypass	Can you access Device file (device.dat) and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>Device.dat file is parsable only to the client. It is stored in binary form</li> </ul>	See threat ID + Corresponding "Action Required"
112	Information Disclosure	Weak Access Control for a Resource	Improper data protection of Settings & Configuration File (Wellnomics.wcd) can allow an attacker to read information not intended for disclosure. Review authorization settings.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
281	Information Disclosure	Weak Access Control for a Resource	Improper data protection of Resource files can allow an attacker to read information not intended for disclosure. Review authorization settings.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
205	Information Disclosure	Authorization Bypass	Can you access Log files (*.txt) and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.	Binary	Low	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>Probably not relevant as these are error logs produced by the client. Mainly relevant to developers</li> </ul>	See threat ID + Corresponding "Action Required"

202	Information Disclosure	Authorization Bypass	Can you access Log files (*.txt) and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>Probably not relevant as these are error logs produced by the client. Mainly relevant to developers</li> </ul>	See threat ID + Corresponding "Action Required"
163	Information Disclosure	Authorization Bypass	Can you access Computer use & Breaks Data History (*.raw) and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
148	Information Disclosure	Weak Access Control for a Resource	Improper data protection of Settings & Configuration File (Wellnomics.wcd) can allow an attacker to read information not intended for disclosure. Review authorization settings.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
162	Information Disclosure	Authorization Bypass	Can you access Settings & Configuration File (Wellnomics.wcd) and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
155	Information Disclosure	Weak Access Control for a Resource	Improper data protection of Computer use & Breaks Data History (*.raw) can allow an attacker to read information not intended for disclosure. Review authorization settings.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
265	Information Disclosure	Authorization Bypass	Can you access User Session Cookie and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.	Binary	Low	<ul style="list-style-type: none"> <li>Threat ID: 6 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>The chrome browser itself requires local admin rights for accessibility</li> </ul>	See threat ID + Corresponding "Action Required"
246	Repudiation	Potential Data Repudiation by Embedded Chromium Browser	Embedded Chromium Browser claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	HTTPS	Low	<ul style="list-style-type: none"> <li>Logging &amp; recording the source, time and summary of the data is what is actually done</li> </ul>	No action required
199	Repudiation	External Entity Wellnomics Server Potentially Denies Receiving Data	Wellnomics Server claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	HTTPS	Low	<ul style="list-style-type: none"> <li>Logging &amp; recording the source, time and summary of the data is what is actually done</li> </ul>	No action required



193	Repudiation	Potential Data Repudiation by Wellnomics Main Application	Wellnomics Main Application claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	HTTPS	Low	<ul style="list-style-type: none"> <li>Logging &amp; recording the source, time and summary of the data is what is actually done</li> </ul>	No action required
191	Repudiation	External Entity Wellnomics Server Potentially Denies Receiving Data	Wellnomics Server claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	HTTPS	Low	<ul style="list-style-type: none"> <li>Logging &amp; recording the source, time and summary of the data is what is actually done</li> </ul>	No action required
216	Repudiation	Potential Weak Protections for Audit Data	Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure access to the log is through a reference monitor, which controls read and write separately. Document what filters, if any, readers can rely on, or writers should expect	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
215	Repudiation	Insufficient Auditing	Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is such capture lightweight enough to be left on all the time? Do you have enough data to deal with repudiation claims? Make sure you log sufficient and appropriate data to handle a repudiation claims. You might want to talk to an audit expert as well as a privacy expert about your choice of data.	Binary	Low	<ul style="list-style-type: none"> <li>Multiple logs are generated and are sufficient enough for the developers to understand.</li> <li>If more information is required, we can enable the user to do trace logging in order to get an idea on where specifically an error/bug has occurred.</li> <li>Logging is continuously being updated and maintained by the developers.</li> </ul>	No action required
214	Repudiation	Data Logs from an Unknown Source	Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.	Binary	Low	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>Logs are information to the developers. It has been produced such that it is uniquely identifiable by the developers.</li> <li>There's not much to gain from receiving fake logs, the developers can spot any unfamiliar details and if we can't reproduce it, it won't be a priority.</li> </ul>	See threat ID + Corresponding "Action Required"
213	Repudiation	Lower Trusted Subject Updates Logs	If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"

211	Repudiation	Potential Weak Protections for Audit Data	Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure access to the log is through a reference monitor, which controls read and write separately. Document what filters, if any, readers can rely on, or writers should expect	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
210	Repudiation	Insufficient Auditing	Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is such capture lightweight enough to be left on all the time? Do you have enough data to deal with repudiation claims? Make sure you log sufficient and appropriate data to handle a repudiation claims. You might want to talk to an audit expert as well as a privacy expert about your choice of data.	Binary	Low	<ul style="list-style-type: none"> <li>Multiple logs are generated and are sufficient enough for the developers to understand. If more information is required, we can enable the user to do trace logging in order to get an idea on where specifically an error/bug has occurred.</li> <li>Logging is continuously being updated and maintained by the developers.</li> </ul>	No action required
209	Repudiation	Data Logs from an Unknown Source	Thread ID: 1 Logs are information to the developers. It has been produced such that it is uniquely identifiable by the developers. There's not much to gain from receiving fake logs, the developers can spot any unfamiliar details and if we can't reproduce it, it won't be a priority.	Binary	Low	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>Logs are information to the developers. It has been produced such that it is uniquely identifiable by the developers.</li> <li>There's not much to gain from receiving fake logs, the developers can spot any unfamiliar details and if we can't reproduce it, it won't be a priority.</li> </ul>	See threat ID + Corresponding "Action Required"
208	Repudiation	Lower Trusted Subject Updates Logs	If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
185	Repudiation	Potential Data Repudiation by Wellnomics Breaks & Exercises Module	Wellnomics Breaks & Exercises Module claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	HTTPS	Low	<ul style="list-style-type: none"> <li>Logging &amp; recording the source, time and summary of the data is what is actually done</li> </ul>	No action required
253	Repudiation	External Entity Wellnomics Server Potentially Denies Receiving Data	Wellnomics Server claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	HTTPS	Low	<ul style="list-style-type: none"> <li>Logging &amp; recording the source, time and summary of the data is what is actually done</li> </ul>	No action required

137	Spoofing	Spoofing of Destination Data Store Settings & Configuration File (Wellnomics.wcd)	Settings & Configuration File (Wellnomics.wcd) may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Settings & Configuration File (Wellnomics.wcd). Consider using a standard authentication mechanism to identify the destination data store.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
198	Spoofing	Spoofing of the Wellnomics Server External Destination Entity	Wellnomics Server may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Wellnomics Server. Consider using a standard authentication mechanism to identify the external entity.	HTTPS	Low	<ul style="list-style-type: none"> <li>Threat ID: 8 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
242	Spoofing	Spoofing of Destination Data Store User Session Cookie	User Session Cookie may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of User Session Cookie. Consider using a standard authentication mechanism to identify the destination data store.	Binary	Low	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>Stored the same way as a Google Chrome browser</li> </ul>	See threat ID + Corresponding "Action Required"
240	Spoofing	Spoofing of Source Data Store User Session Cookie	User Session Cookie may be spoofed by an attacker and this may lead to incorrect data delivered to Embedded Chromium Browser. Consider using a standard authentication mechanism to identify the source data store.	Binary	Low	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>Stored the same way as a Google Chrome browser</li> </ul>	See threat ID + Corresponding "Action Required"
128	Spoofing	Spoofing of Source Data Store INI Configuration files	INI Configuration files may be spoofed by an attacker and this may lead to incorrect data delivered to Wellnomics Main Application. Consider using a standard authentication mechanism to identify the source data store.	Binary	Medium	<ul style="list-style-type: none"> <li>Threat ID: 5 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
146	Spoofing	Spoofing of Source Data Store Settings & Configuration File (Wellnomics.wcd)	Settings & Configuration File (Wellnomics.wcd) may be spoofed by an attacker and this may lead to incorrect data delivered to Wellnomics Breaks & Exercises Module. Consider using a standard authentication mechanism to identify the source data store.	Binary	High	<ul style="list-style-type: none"> <li>Threat ID: 3 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
190	Spoofing	Spoofing of the Wellnomics Server External Destination Entity	Wellnomics Server may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Wellnomics Server. Consider using a standard authentication mechanism to identify the external entity.	HTTPS	Low	<ul style="list-style-type: none"> <li>Threat ID: 6 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
278	Spoofing	Spoofing of Source Data Store Device file (device.dat)	Device file (device.dat) may be spoofed by an attacker and this may lead to incorrect data delivered to Wellnomics Main Application. Consider using a standard authentication mechanism to identify the source data store.	Binary	High	<ul style="list-style-type: none"> <li>Threat ID: 3 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>The client looks for the device.dat file in the appdata folder so the file requires admin privileges. Not only that, the id is in binary + has to match with user key settings.</li> </ul>	See threat ID + Corresponding "Action Required"

275	Spoofing	Spoofing of Destination Data Store Device file (device.dat)	Device file (device.dat) may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Device file (device.dat). Consider using a standard authentication mechanism to identify the destination data store.	Binary	High	<ul style="list-style-type: none"> <li>• Threat ID: 3 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>• The client looks for the device.dat file in the appdata folder so the file requires admin privileges. Not only that, the id is in binary + has to match with user key settings.</li> </ul>	See threat ID + Corresponding "Action Required"
110	Spoofing	Spoofing of Source Data Store Settings & Configuration File (Wellnomics.wcd)	Settings & Configuration File (Wellnomics.wcd) may be spoofed by an attacker and this may lead to incorrect data delivered to Wellnomics Main Application. Consider using a standard authentication mechanism to identify the source data store.	Binary	High	<ul style="list-style-type: none"> <li>• Threat ID: 3 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
280	Spoofing	Spoofing of Source Data Store Resource files	Resource files may be spoofed by an attacker and this may lead to incorrect data delivered to Wellnomics Main Application. Consider using a standard authentication mechanism to identify the source data store.	Binary	High	<ul style="list-style-type: none"> <li>• Threat ID: 3 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
204	Spoofing	Spoofing of Destination Data Store Log files (*.txt)	Log files (*.txt) may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Log files (*.txt). Consider using a standard authentication mechanism to identify the destination data store.	Binary	Low	<ul style="list-style-type: none"> <li>• Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>• Logs aren't read by the Client application, only applicable developers</li> </ul>	See threat ID + Corresponding "Action Required"
119	Spoofing	Spoofing of Destination Data Store Settings & Configuration File (Wellnomics.wcd)	Settings & Configuration File (Wellnomics.wcd) may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Settings & Configuration File (Wellnomics.wcd). Consider using a standard authentication mechanism to identify the destination data store.	Binary	High	<ul style="list-style-type: none"> <li>• Threat ID: 3 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
201	Spoofing	Spoofing of Destination Data Store Log files (*.txt)	Log files (*.txt) may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Log files (*.txt). Consider using a standard authentication mechanism to identify the destination data store.	Binary	Low	<ul style="list-style-type: none"> <li>• Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>• Logs aren't read by the Client application, only applicable developers</li> </ul>	See threat ID + Corresponding "Action Required"
154	Spoofing	Spoofing of Source Data Store Computer use & Breaks Data History (*.raw)	Computer use & Breaks Data History (*.raw) may be spoofed by an attacker and this may lead to incorrect data delivered to Wellnomics Breaks & Exercises Module. Consider using a standard authentication mechanism to identify the source data store.	Binary	High	<ul style="list-style-type: none"> <li>• Threat ID: 3 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
156	Spoofing	Spoofing of Destination Data Store Computer use & Breaks Data History (*.raw)	Computer use & Breaks Data History (*.raw) may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Computer use & Breaks Data History (*.raw). Consider using a standard authentication mechanism to identify the destination data store.	Binary	High	<ul style="list-style-type: none"> <li>• Threat ID: 3 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"

252	Spoofing	Spoofing of the Wellnomics Server External Destination Entity	Wellnomics Server may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Wellnomics Server. Consider using a standard authentication mechanism to identify the external entity.	HTTPS	Low	<ul style="list-style-type: none"> <li>Threat ID: 6 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> </ul>	See threat ID + Corresponding "Action Required"
138	Tampering	Potential SQL Injection Vulnerability for Settings & Configuration File (Wellnomics.wcd)	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.	Binary	Low	<ul style="list-style-type: none"> <li>SQL injections not relevant to client</li> </ul>	N/A
256	Tampering	JavaScript Object Notation Processing	If a dataflow contains JSON, JSON processing and hijacking threats may be exploited.	HTTPS	Low	<ul style="list-style-type: none"> <li>Threat ID: 6 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>There is JSON processing between the client and server but the method of hijacking (or man in the middle attacks) is highly unlikely due to the requests</li> </ul>	See threat ID + Corresponding "Action Required"
178	Tampering	JavaScript Object Notation Processing	If a dataflow contains JSON, JSON processing and hijacking threats may be exploited.	HTTPS	Low	<ul style="list-style-type: none"> <li>Threat ID: 6 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>There is JSON processing between the client and server but the method of hijacking (or man in the middle attacks) is highly unlikely due to the requests</li> </ul>	See threat ID + Corresponding "Action Required"
212	Tampering	Risks from Logging	Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.	Binary	Low	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>See Threat #214</li> </ul>	See threat ID + Corresponding "Action Required"
207	Tampering	Risks from Logging	Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.	Binary	Low	<ul style="list-style-type: none"> <li>Threat ID: 1 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a> See Threat #214</li> </ul>	See threat ID + Corresponding "Action Required"

120	Tampering	Potential SQL Injection Vulnerability for Settings & Configuration File (Wellnomics.wcd)	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.	Binary	Low	<ul style="list-style-type: none"> <li>SQL injections not relevant to client</li> </ul>	N/A
282	Tampering	Authenticated Data Flow Compromised	An attacker can read or modify data transmitted over an authenticated dataflow.	Binary	Low	<ul style="list-style-type: none"> <li>Thread ID: 3 <a href="#">Product Security Risk Assessment - App (Mar 2021)</a></li> <li>Modifying resource files (which is media information like videos or images) won't achieve much in terms of exposing any private information</li> </ul>	See threat ID + Corresponding "Action Required"

## Related Standards, Policies, Processes and Forms

Based on [Product Threat Modeling - Policy](#)

Date of Change	Responsible	Summary of change	Next revision
March 2021	<a href="#">Kevin</a>	Updated for App version 1.1.2.1287	<ul style="list-style-type: none"> <li>10 Mar 2022 <a href="#">Kevin</a></li> </ul>
Sep 2022	<a href="#">Kevin</a>	Reviewed and is still valid for App 2.0	<ul style="list-style-type: none"> <li>03 Jul 2023 <a href="#">Kevin</a></li> </ul>
06 Jul 2023	<a href="#">Kevin</a>	Still valid - no changes required	<ul style="list-style-type: none"> <li>09 Jul 2024 <a href="#">Kevin</a></li> </ul>

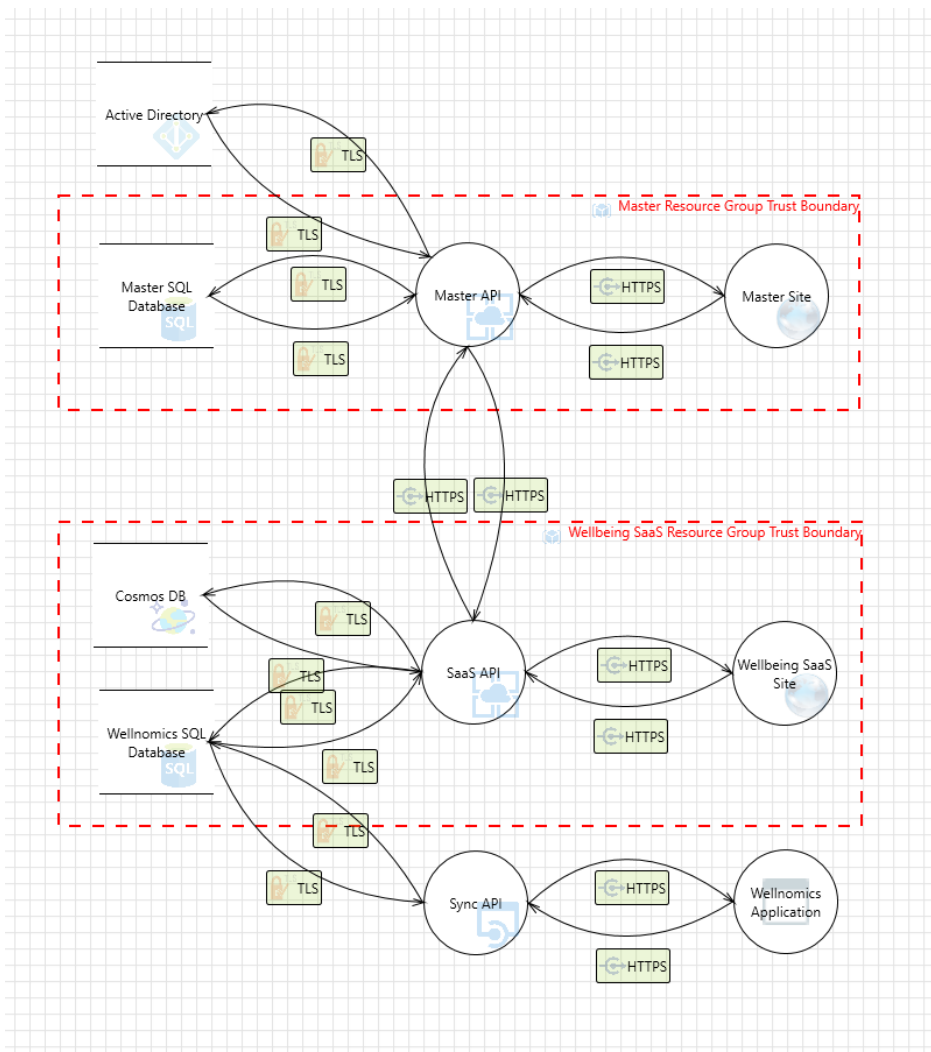
# Threat Modelling - SaaS - Documentation

*WIP: Need to check that each threat generated has been mitigated and if it hasn't, it should populate the Product Security Risk Assessment table* Product Security Risk Assessment - SaaS (Sep 2020)

<b>Last updated</b>	19-07-2023
<b>Based upon product version</b>	

## Threat Model

Created using Microsoft Threat Modelling App



## Threat Analysis and Mitigation

The threat review generated by the MS Threat Modelling tool is below:

Invalid file id - 653676...

The table below analyses each of these threats, rates their risks according to [Product Security Risk Assessment Matrix - Policy](#), and explains how each risk is mitigated, and where mitigation is necessary.

Table with each row showing:

- Risk from MS Threat model
- Risk Rating (High/Medium/Low)
- Explanation (why its given this rating)
- Mitigation (explanation of how risk is mitigated if its High or Medium risk).

Id	Category	Title	Risk Description	Interaction	Risk Rating	Risk Explanation	Mitigation
0	Spoofing	An adversary can spoof the target web application due to insecure TLS certificate configuration	Ensure that TLS certificate parameters are configured with correct values	HTTPS	High		
1	Spoofing	An adversary can steal sensitive data like user credentials	Attackers can exploit weaknesses in system to steal user credentials. Downstream and upstream components are often accessed by using credentials stored in configuration stores. Attackers may steal the upstream or downstream component credentials. Attackers may steal credentials if, Credentials are stored and sent in clear text, Weak input validation coupled with dynamic sql queries, Password retrieval mechanism are poor,	HTTPS	High		<ul style="list-style-type: none"> <li>• Each user password is hashed with salt (never stored as clear text).</li> <li>• Recaptcha is implemented on login.</li> <li>• Reset password token used to verify user on password reset.</li> <li>• HTTPS communication protocols transmit credentials securely over network.</li> <li>• Strong password policies.</li> </ul>
2	Spoofing	An adversary can create a fake website and launch phishing attacks	Phishing is attempted to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a Web Server which is a trustworthy entity in electronic communication	HTTPS	High	Question: Do we have anything in place to prevent the spoofing of the Wellnomics domain? Like an authentication on outgoing emails or something?	<ul style="list-style-type: none"> <li>• HTTPS communication protocols transmit credentials securely over network.</li> </ul>
3	Spoofing	An adversary may spoof SaaS API and gain access to the Wellbeing Site or Master API	If proper authentication is not in place, an adversary can spoof a source process or external entity and gain unauthorized access to the Web Application	HTTPS	High	Question: How does the site/Master API know the SaaS API is legit?  CSFR handling using same-origin credentials should also be implemented. (There is a ticket for this).	



5	Tampering	An adversary can execute remote code on the server through XSLT scripting	An adversary can execute remote code on the server through XSLT scripting	HTTPS	High	XSLT: eXtensible Stylesheet Language Transformations  Do we do this: <ul style="list-style-type: none"><li>Web Application Firewall (WAF) to detect and block malicious XSLT payloads/requests.</li></ul>	<ul style="list-style-type: none"> <li>Strict input validation and sanitisation.</li> <li>Least privilege principle applied to all user accounts.</li> </ul>
6	Tampering	An adversary may inject malicious inputs into an API and affect downstream processes	An adversary may inject malicious inputs into an API and affect downstream processes	HTTPS	High	Question: Do we have rate limiting/throttling mechanisms to limit the number of requests made within a specific time frame?	<ul style="list-style-type: none"> <li>Strict input validation and sanitisation.</li> <li>Dynamic SQL queries parameterised.</li> <li>API requires authentication and authorisation (user credentials and rights on JWT with expiration time).</li> </ul>
7	Tampering	An adversary can gain access to sensitive data by performing SQL injection through Web App	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.	HTTPS	High		<ul style="list-style-type: none"> <li>Strict input validation and sanitisation.</li> <li>Dynamic SQL queries parameterised.</li> </ul>
8	Tampering	An adversary can gain access to sensitive data stored in Web App's config files	An adversary can gain access to the config files. and if sensitive data is stored in it, it would be compromised.	HTTPS	High		<ul style="list-style-type: none"> <li>Sensitive data not stored in config files.</li> </ul>
9	Repudiation	Attacker can deny a malicious act on an API leading to repudiation issues	Attacker can deny a malicious act on an API leading to repudiation issues	HTTPS	High	Question: do we keep logs on API activity for legal repudiation purposes?	<ul style="list-style-type: none"> <li>Attacks prevented with authentication token.</li> <li>RBAC implemented.</li> </ul>
10	Repudiation	Attacker can deny the malicious act and remove the attack foot prints leading to repudiation issues	Proper logging of all security events and user actions builds traceability in a system and denies any possible repudiation issues. In the absence of proper auditing and logging controls, it would become impossible to implement any accountability in a system	HTTPS	High	^?	

11	Information Disclosure	An adversary can reverse weakly encrypted or hashed content	An adversary can reverse weakly encrypted or hashed content	HTTPS	High		<ul style="list-style-type: none"> <li>• Crypto's SHA-256 hashing</li> </ul>
12	Information Disclosure	An adversary may gain access to sensitive data from log files	An adversary may gain access to sensitive data from log files	HTTPS	High	Question: what log files exist here and do they contain sensitive data?	
13	Information Disclosure	An adversary can gain access to sensitive information through error messages	An adversary can gain access to sensitive data such as the following, through verbose error messages - Server names - Connection strings - Usernames - Passwords - SQL procedures - Details of dynamic SQL failures - Stack trace and lines of code - Variables stored in memory - Drive and folder locations - Application install points - Host configuration settings - Other internal application details	HTTPS	High		<ul style="list-style-type: none"> <li>• Error messages are kept fairly generic.</li> <li>• Lack of details provided in the errors.</li> </ul>
14	Denial Of Service	An adversary may block access to the application or API hosted on Wellbeing SaaS Site through a denial of service attack	An adversary may block access to the application or API hosted on Wellbeing SaaS Site through a denial of service attack	HTTPS	High		
15	Denial Of Service	An adversary may block access to the application or API hosted on SaaS API through a denial of service attack	An adversary may block access to the application or API hosted on SaaS API through a denial of service attack	HTTPS	High		
16	Tampering	An adversary can tamper critical database securables and deny the action	An adversary can tamper critical database securables and deny the action	TLS	High		
17	Tampering	An adversary may leverage the lack of monitoring systems and trigger anomalous traffic to database	An adversary may leverage the lack of intrusion detection and prevention of anomalous database activities and trigger anomalous traffic to database	TLS	High		
18	Repudiation	An adversary can deny actions on database due to lack of auditing	Proper logging of all security events and user actions builds traceability in a system and denies any possible repudiation issues. In the absence of proper auditing and logging controls, it would become impossible to implement any accountability in a system.	TLS	High		

19	Information Disclosure	An adversary can gain access to sensitive PII or HBI data in Wellnomics SQL Database	Additional controls like Transparent Data Encryption, Column Level Encryption, EKM etc. provide additional protection mechanism to high value PII or HBI data.	TLS	High		
20	Information Disclosure	An adversary can gain access to sensitive data by performing SQL injection	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.	TLS	High		
21	Elevation Of Privilege	An adversary can gain unauthorized access to database due to lack of network access protection	If there is no restriction at network or host firewall level, to access the database then anyone can attempt to connect to the database from an unauthorized location	TLS	High		
22	Elevation Of Privilege	An adversary can gain unauthorized access to Azure SQL database due to weak account policy	Due to poorly configured account policies, adversary can launch brute force attacks on Wellnomics SQL Database	TLS	High		
23	Elevation Of Privilege	An adversary can gain unauthorized access to Wellnomics SQL Database due to loose authorization rules	Database access should be configured with roles and privilege based on least privilege and need to know principle.	TLS	High		
24	Elevation Of Privilege	An adversary may gain unauthorized access to Wellnomics SQL Database account in a subscription	An adversary may gain unauthorized access to Wellnomics SQL Database account in a subscription	TLS	High		
26	Spoofing	An adversary can gain unauthorized access to Cosmos DB due to weak CORS configuration	An adversary can gain unauthorized access to Cosmos DB due to weak CORS configuration	TLS	High		

27	Spoofing	An adversary may replay stolen long-lived Resource tokens of CosmosDB	An adversary may get access to Resource tokens used to authenticate to DocumentDB. If the lifetime of these tokens is not finite, the adversary may replay the stolen tokens for a long time.	TLS	High		
28	Information Disclosure	An adversary may gain access to sensitive clear-text data in CosmosDB	An adversary may gain access to sensitive clear-text data in DocumentDB storage	TLS	High		
29	Information Disclosure	An adversary can gain access to sensitive PII or HBI data in Cosmos DB	Additional controls like Transparent Data Encryption, Column Level Encryption, EKM etc. provide additional protection mechanism to high value PII or HBI data.	TLS	High		
30	Information Disclosure	An adversary can abuse poorly managed Cosmos DB's access keys	An adversary can abuse poorly managed Cosmos DB's access keys and gain unauthorized access to storage.	TLS	High		
34	Elevation Of Privilege	An adversary can gain unauthorized access to Cosmos DB due to loose authorization rules	Database access should be configured with roles and privilege based on least privilege and need to know principle.	TLS	High		
35	Elevation Of Privilege	An adversary may gain elevated privileges on Cosmos DB NoSQL Database	An adversary may gain elevated privileges on the contents of Cosmos DB if over-privileged master or read-only keys are used to connect	TLS	High		
36	Elevation Of Privilege	An adversary may read unauthorized content stored in Cosmos DB	An adversary may gain elevated privileges on the document stored in Cosmos DB storage.	TLS	High		
37	Elevation Of Privilege	An adversary may directly connect to Cosmos DB from anywhere	An adversary may directly connect to Cosmos DB from anywhere since Cosmos DB does not have any Firewall restrictions that can be enforced.	TLS	High		
38	Elevation Of Privilege	An adversary may gain unauthorized access to Cosmos DB account in a subscription	An adversary may gain unauthorized access to Cosmos DB account in a subscription	TLS	High		
39	Elevation Of Privilege	A compromised access key may permit an adversary to have more access than intended to an Cosmos DB instance	A compromised access key may permit an adversary to have over-privileged access to an Cosmos DB instance	TLS	High		

40	Elevation Of Privilege	An adversary can gain unauthorized access to Azure Cosmos DB instances due to weak network security configuration	An adversary can gain unauthorized access to Azure Cosmos DB instances due to weak network security configuration	TLS	High		
54	Spoofing	An adversary may spoof Wellnomics SQL Database and gain access to Web Application	If proper authentication is not in place, an adversary can spoof a source process or external entity and gain unauthorized access to the Web Application	TLS	High		
55	Spoofing	An adversary may spoof Wellnomics SQL Database and gain access to Web API	If proper authentication is not in place, an adversary can spoof a source process or external entity and gain unauthorized access to the Web Application	TLS	High		
58	Tampering	An adversary can gain access to sensitive data by performing SQL injection through Web API	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.	TLS	High		
60	Information Disclosure	An adversary can gain access to sensitive information from an API through error messages	An adversary can gain access to sensitive data such as the following, through verbose error messages - Server names - Connection strings - Usernames - Passwords - SQL procedures - Details of dynamic SQL failures - Stack trace and lines of code - Variables stored in memory - Drive and folder locations - Application install points - Host configuration settings - Other internal application details	TLS	High		
61	Information Disclosure	An adversary can gain access to sensitive data by sniffing traffic to Web API	An adversary can gain access to sensitive data by sniffing traffic to Web API	TLS	High		
62	Information Disclosure	An adversary can gain access to sensitive data stored in Web API's config files	An adversary can gain access to the config files. and if sensitive data is stored in it, it would be compromised.	TLS	High		

63	Denial Of Service	An adversary may block access to the application or API hosted on Sync API through a denial of service attack	An adversary may block access to the application or API hosted on Sync API through a denial of service attack	TLS	High		
64	Elevation Of Privilege	An adversary may gain unauthorized access to Sync API due to poor access control checks	An adversary may gain unauthorized access to Web API due to poor access control checks	TLS	High		
68	Spoofing	An adversary may spoof Wellnomics Application and gain access to Web Application	If proper authentication is not in place, an adversary can spoof a source process or external entity and gain unauthorized access to the Web Application	HTTPS	High		
69	Spoofing	An adversary may spoof Wellnomics Application and gain access to Web API	If proper authentication is not in place, an adversary can spoof a source process or external entity and gain unauthorized access to the Web Application	HTTPS	High		
82	Information Disclosure	An adversary can gain access to sensitive PII or HBI data in Master SQL Database	Additional controls like Transparent Data Encryption, Column Level Encryption, EKM etc. provide additional protection mechanism to high value PII or HBI data.	TLS	High		
86	Elevation Of Privilege	An adversary can gain unauthorized access to Master SQL Database due to loose authorization rules	Database access should be configured with roles and privilege based on least privilege and need to know principle.	TLS	High		
87	Elevation Of Privilege	An adversary may gain unauthorized access to Master SQL Database account in a subscription	An adversary may gain unauthorized access to Master SQL Database account in a subscription	TLS	High		
88	Denial Of Service	An adversary may block access to the application or API hosted on Master API through a denial of service attack	An adversary may block access to the application or API hosted on Master API through a denial of service attack	TLS	High		
94	Spoofing	An adversary may spoof Master API and gain access to Web Application	If proper authentication is not in place, an adversary can spoof a source process or external entity and gain unauthorized access to the Web Application	HTTPS	High		

95	Spoofing	An adversary may spoof Master API and gain access to Web API	If proper authentication is not in place, an adversary can spoof a source process or external entity and gain unauthorized access to the Web Application	HTTPS	High		
105	Denial Of Service	An adversary may block access to the application or API hosted on Master Site through a denial of service attack	An adversary may block access to the application or API hosted on Master Site through a denial of service attack	HTTPS	High		
108	Spoofing	An adversary can bypass authentication due to non-standard Azure AD authentication schemes	An adversary can bypass authentication due to non-standard Azure AD authentication schemes	TLS	High		
109	Spoofing	An adversary can get access to a user's session by replaying authentication tokens	An adversary can get access to a user's session by replaying authentication tokens	TLS	High		

## Related Standards, Policies, Processes and Forms

Based on [Product Threat Modeling - Policy](#)

# Software Development Tools - Documentation

**Review Period:** Annual

Wellnomics uses the following Approved tools and security testing options for software development.

Purpose	Tool	Version	Recommended	Security Testing options
<b>SERVER</b>				
Development Framework	Microsoft .NET	.Net 4.8	4.8 or newer	
Development Languages	C# Compiler	.Net 4.8	2019 or newer	
	Node.js	16.x		
IDE & Code Editors	Microsoft Visual Studio	17.2.3 (2022)	16.1.16 (2019 or newer)	
	Visual Studio Code	n/a Auto updates		
	Programmers Notepad	2.4.2.X		
Database	Microsoft SQL Server	2019 (15.x)		
Code management	Gitkraken	n/a Auto updates		
	Bitbucket	N/A (Cloud)		
	GIT	2.21.0		
<b>CLIENT</b>				
Development Language	C++			
Development Framework	Qt			
SAST	CppCheck	2.2		
<b>QA</b>				
Test management	Atlassian Jira Test management	n/a Auto updates		
Test automation - Web	Cypress	4.7.0		
	Node JS	16.x		
Test automation - Desktop	Squish	6.6.1		
API Testing	Insomnia	2022.5		
Vulnerability Testing	NetSparker (Invicti Standard)	6.5.0		
<b>OTHER</b>				
Continuous Integration	Jenkins			



File comparison	Beyond Compare	4.1.9		
	Agent Ransack	2017.03.02.44979		
Editor	Programmers Notepad	2.4.2.1440		

For sources for recommended versions refer [Software Development Tools - Policy](#)

## Related Standards, Policies and Processes

- [Software Development Tools - Policy](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
06 Nov 2020	<a href="#">Kevin</a>	Copied from existing internal documents	<ul style="list-style-type: none"> <li>• 24 Aug 2021 <a href="#">Angeli Arino (Deactivated)</a></li> </ul>
06 Nov 2021		To be updated with developers	<ul style="list-style-type: none"> <li>• 24 Jun 2022 <a href="#">Matt</a></li> </ul>
24 Jun 2022	<a href="#">Matt</a>	Reviewed Updated where required	<ul style="list-style-type: none"> <li>• 16 Jul 2023 <a href="#">Matt</a></li> </ul>

# Static Analysis Security Testing (SAST) - Guideline

Current Tools	Platform	Languages	Warnings disabled (if any)
CodeRush	Server	C# .NET	
CPPCheck	Client	C++	
Microsoft <a href="https://docs.microsoft.com/en-us/cpp/code-quality/?view=msvc-160">https://docs.microsoft.com/en-us/cpp/code-quality/?view=msvc-160</a>	Client	C++	

## Overview

This guideline shows the priority for addressing different warning types and vulnerability levels highlighted by our current code analysis tools. This guide covers both client & server tools.

The intention is to provide a simple **High (Must Fix)/Medium (Next Release)/Low (Ignore if not too many)** decision path for engineers to use to decide whether issues need to be resolved.

Risk level	Priority
Low risk	Not a priority
Medium Risk	Nice to address
High risk	Must address

## Best Practice - zero warnings

Best practice is to aim for as close to zero warnings as possible. If there are too many low level warnings something important may be lost in the detail and easier to miss. It is also harder to verify compliance when there are lots of warnings.

Note there may be switches in the tools that can be used to suppress some low level warnings that we decide are not important.

## Fix Guide

To be completed as needed

Warning Types	Rating	Comments
Tool 1		
Tool 2		

## Related documents

- [Static Analysis Security Testing \(SAST\) - Policy](#)
- [Static Analysis Security Testing \(SAST\) - Records](#)
- [Software Development Tools - Documentation](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
05 Nov 2020	<a href="#">Kevin</a>	Created	<ul style="list-style-type: none"> <li>• 05 Nov 2021 <a href="#">Angeli Arino (Deactivated)</a></li> </ul>
01 May 2021	<a href="#">Kevin</a>	Updated with compiler warnings and SonarCloud	<ul style="list-style-type: none"> <li>• 01 May 2022</li> </ul>
06 Jul 2021	<a href="#">Corinne</a>	Updated risk table to mirror the Risk Assessment Matrix	
14 Sep 2021	<a href="#">Kevin</a>	Updated list of current tools used	<ul style="list-style-type: none"> <li>• 14 Sep 2022</li> </ul>
08 Sep 2022	<a href="#">Kevin</a>	Reviewed and no changes needed	<ul style="list-style-type: none"> <li>• 08 Sep 2023</li> </ul>

# Dynamic Analysis Security Testing (DAST) - Guidelines

**Review Period:** Annual

Current DAST Tools	Warnings disabled
Netsparker	<ul style="list-style-type: none"><li>Update Netsparker info when implemented finally <a href="#">Aarti</a></li></ul>

## Overview

This guide shows the priority for addressing different warning types and vulnerability levels highlighted by our current DAST tools. The intention is to provide a simple Must Fix/Can Fix/Ignore decision path for engineers to use to decide whether issues need to be resolved.

As a general guide as many warnings as possible should be resolved and fixed.

Rating	Description
<b>Must Fix</b>	Issue must be fixed. Code cannot be committed with any items at this level present.
<b>Try to Fix</b>	Try to fix if possible and effort/cost not too high.
<b>Can ignore</b>	Can be ignored (as long as there aren't hundreds of them)

## Best Practice - zero warnings

Best practice is to aim for as few warnings as possible. If there are too many low level warnings something important may be lost in the detail and easier to miss. It is also harder to verify compliance when there are lots of warnings.

Note there may be switches in the DAST tool that can be used to suppress some low level warnings that we decide are not important. If this is done this

## Test Environment

Document the server test environment to be used below;

- Document the DAST test environment to be used below; [Aarti](#)

## Fix Guide

Warning Type	Rating	Comments
<ul style="list-style-type: none"><li>Write up warnings fix guide for Netsparker <a href="#">Aarti</a></li></ul>		

## Related documents

- [Dynamic Analysis Security Testing \(DAST\) - Policy](#)
- [Dynamic Analysis Security Testing \(DAST\) - Records](#)
- [Software Development Tools - Documentation](#)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
05 Nov 2020	<a href="#">Kevin</a>	Created	<ul style="list-style-type: none"><li>• 05 Nov 2021 <a href="#">Angeli Arino (Deactivated)</a></li></ul>
06 Dec 2021	<a href="#">Corinne</a>	reviewed and no changes required	<ul style="list-style-type: none"><li>• 25 Nov 2022 <a href="#">Corinne</a></li></ul>
26 Jan 2023	<a href="#">Corinne</a>	reviewed and no changes required	<ul style="list-style-type: none"><li>• 26 Jan 2024 <a href="#">Corinne</a></li></ul>

# App Security Testing - Guidelines

Review period: Annual

Below are the set of tests that must be run when testing the App. Every test must pass for the application to pass.

Test Area	Test Methodology	Pass	Fail	Notes
<b>Communication Security</b>				
<b>Security protocol</b>				
Security protocol is TLS 1.2 or above	Force server to only communicate using TLS 1.1 or below and app communication with server should fail with an error.	App communication log shows a error upon sync with server	App communication log shows a successful sync with server	
<b>Certificate validation</b>				
Domain name	Issue an SSL certificate with a mis-matched domain name.	App communication log shows a Domain Name validation error upon sync with server.	App communication log shows a successful sync with server	
Revocation status	Issue an SSL certificate and then revoke it?	App successfully communicates with server and:  App communication log shows a Certificate Revocation error in the log	App communication log shows no warnings about revoked certificate.	
Trust chain	Issue a self-signed SSL certificate that is not trusted. Test <i>before</i> and <i>after</i> Client contacts the server	App communication log shows a Trust Chain validation error upon sync with server	App communication log shows a successful sync with server	
<b>File security</b>				
Personal and settings data not stored in multiple locations	Take a copy of folders where files are being installed. Do a diff before and after to see what files are being updated/written to.  Review these files more closely.	Only a small number of files are changed or updated. Reviewing these files they either cannot be opened in a plain text editor with meaningful content, or if they can, they clearly upon inspection have no personal user data or user settings.	Otherwise	
Personal data file should be encoded/encrypted	Try opening file in a Visual Studio text editor and Hex editor	File won't open or read as text or has no obviously readable text or data in it when viewed. Should present as unreadable content.	File opens cleanly in Text editor, or in Hex editor reviewing file shows recognizable text o data content.	
	Open user data/setting files in SQL lite reader	File can't be read as is encrypted or not an SQL Lite compatible file	File can be read in SQL Lite	

## Revision History

Date of change	Responsible	Summary of change	Next revision date

04 Nov 2020	<a href="#">Kevin</a>	Documented test processes. Added File Security checks section as well	
11 Nov 2020	<a href="#">Kevin</a>	Modified Pass/Fail criteria for Revocation Status to differentiate between WPC and WC	10 Nov 2021 <a href="#">Angeli Arino (Deactivated)</a>

# SaaS Security and Penetration Testing - Guidelines

**Review period:** Annual

See also [Security and Penetration Testing - Policy](#)

## Selection criteria

The criteria for selecting which areas of the product to test are as follows:

1. Testing puts a higher priority and more extensive on areas that are accessed most commonly and by end users compared with pages accessed less frequently and by administrators only.
2. ALL the pages that end users have access are extensively tested, including all entry fields on every page. For example, My risk profile, Notes, assessments completion and sync data
3. ALL public facing pages that anyone can access to (without having to log in) are extensively tested. For example, login page, forget password page, new account page.
4. For the rest of the tests priority is placed on testing all pages that insert information on the database and we test all text boxes and text areas that input information that will be saved in the database.

Area	Test coverage	Notes
Cross-site Scripting (XSS)	<ul style="list-style-type: none"><li>• URL Script injection</li><li>• Execute HTML</li><li>• Execute JavaScript</li></ul>	
SQL Injection	<ul style="list-style-type: none"><li>• Standard SQL injection</li><li>• Stacked queries</li><li>• Fingerprinting the Database</li><li>• Union Exploitation</li><li>• Error based Exploitation</li><li>• Out of band Exploitation</li><li>• Time delay Exploitation</li><li>• Stored Procedure Injection</li></ul>	
Broken authentication and session management	<ul style="list-style-type: none"><li>• Email address as a User ID</li><li>• Password Strength Controls (IT admin can overwrite)</li><li>• Secure Password Recovery Mechanism</li><li>• Store Passwords in a Secure Fashion</li><li>• Logging and Monitoring</li></ul>	verify that <a href="#">OWASP guidelines</a> are followed as per this list



	<ul style="list-style-type: none"> <li>• Email address as a User ID</li> <li>• Password Strength Controls (IT admin can overwrite)</li> <li>• Secure Password Recovery Mechanism</li> <li>• Store Passwords in a Secure Fashion</li> <li>• Logging and Monitoring</li> </ul>	
File upload flaws	<ul style="list-style-type: none"> <li>• Upload .gif file to be resized</li> <li>• Upload .jsp file into web tree</li> <li>• Upload huge files</li> <li>• Upload file using malicious path or name</li> <li>• Upload file containing personal data</li> <li>• Upload file containing "tags"</li> <li>• Upload .html file containing script</li> <li>• Upload .jpg file containing a Flash object</li> <li>• Upload .exe file</li> <li>• Upload .rar file to be scanned by antivirus</li> <li>• Upload virus infected file</li> </ul>	When evaluating risks note that any vulnerabilities in this area will be similar as for any email server that allows attachments. Every user with an anti-virus will be protected from most of these vulnerabilities. The virus will not be executed on the server if is uploaded.
Caching servers attacks	<ul style="list-style-type: none"> <li>• Test Browser cache</li> </ul>	
Cross Site Request Forgery (CSRF)	<ul style="list-style-type: none"> <li>• Internal API</li> <li>• External API</li> </ul>	
	<ul style="list-style-type: none"> <li>• Dictionary attack</li> <li>• Brute force attack</li> <li>• Rainbow table attack</li> </ul>	
Password cracking	<ul style="list-style-type: none"> <li>• Dictionary attack</li> <li>• Brute force attack</li> <li>• Rainbow table attack</li> </ul>	Password always will have vulnerability when we have the human factor. We implement the best practices and extra security having a unique salt for each password.
Server misconfigurations	<ul style="list-style-type: none"> <li>• Verify the frameworks used on the development environment</li> <li>• Verify if all the software used in development environment are supported for the distribution company</li> </ul>	
Command Injection	<ul style="list-style-type: none"> <li>• Command injection in a HTTP request</li> </ul>	

Forceful browsing	<ul style="list-style-type: none"> <li>Changing URL parameters to have access to private information</li> </ul>	
-------------------	---	--

## Revision History

Date of change	Responsible	Summary of change	Next revision
01 Jan 2021	Kevin Taylor	New document	<ul style="list-style-type: none"> <li>03 Jan 2022 <a href="#">Corinne</a></li> </ul>
23 Apr 2022	Corinne Wright	Reviewed no changes	<ul style="list-style-type: none"> <li>23 Apr 2023 <a href="#">Corinne</a></li> </ul>
23 Jun 2023	Corinne Wright	reviewed no changes	<ul style="list-style-type: none"> <li>24 Jun 2024 <a href="#">Corinne</a></li> </ul>

# DEPLOYMENT & HOSTING - Documentation

- [Microsoft Azure Security and Compliance - Documentation](#)
- [Access Security - Hosting - Documentation](#)
- [Threat Modeling - Hosting - Documentation](#)
- [Service Level Agreement and Security Statement](#)
- [SaaS Service Level Agreement - Uptime Monitoring - Guideline](#)
- [Monitoring - Hosting - Guideline](#)
- [Disaster Recovery and Business Continuity - Hosting - Guide](#)

# Microsoft Azure Security and Compliance - Documentation

**Review period:** Annual

Microsoft Azure provides hosting facilities for Wellnomics under the terms and conditions as contained in the documents below. Microsoft does not have direct logical access to the servers but simply provide the physical architecture and support. Refer below to specific compliance documents available from Microsoft and documents on security

## Full list of latest compliance documents

Go to: <https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc?view=o365-worldwide>

Physical Security	<a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security">https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security</a>
Infrastructure Security	<a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure">https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure</a>
General Documentation	<a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/">https://docs.microsoft.com/en-us/azure/security/fundamentals/</a>
SOC 1, 2, and 3 Reports	<a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc?view=o365-worldwide#soc-1-2-and-3-reports-overview">https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc?view=o365-worldwide#soc-1-2-and-3-reports-overview</a>
Audit Reports and Certificates	<a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc?view=o365-worldwide#audits-reports-and-certificates">https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc?view=o365-worldwide#audits-reports-and-certificates</a>
Service Level Agreement	<a href="https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=17583">https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=17583</a>

## Revision History

Date of change	Responsible	Summary of change	Next revision date
10 Jun 2020	Wayne Owens, Principal Consultant	New document created to reflect change from Rackspace to Azure	<ul style="list-style-type: none"><li>16 Jun 2021 <a href="#">Ian Bartram</a></li></ul>
05 Sep 2022	Ian Bartram	No changes required	<ul style="list-style-type: none"><li>05 Sep 2022 <a href="#">Ian Bartram</a></li></ul>
05 Sep 2022	Ian Bartram	No changes required	<ul style="list-style-type: none"><li>05 Sep 2023 <a href="#">Ian Bartram</a></li></ul>

# Access Security - Hosting - Documentation

## Overview

All Hosted servers are accessed via a Secure Remote Management service. Role-Based Access control and app based MFA is required to ensure no unapproved staff can access hosting servers. The Zero-Trust model is applied to ensure only staff who absolutely require access have it.

## Service features

- The RMM service uses end to end AES 256-bit encryption.
- Timed sessions
- session and server logging + Audits
- IP login restrictions
- Brute-Force timeouts
- Secure AD based SSO
- AD based RBAC
- App based multi-factor Authentication

Current Servers:

Server	Region	Role
AMER-DB-1	East US	SQL Server
AMER-WEB-1	East US	SQL + Webserver
AMER-WEB-4	East US	Webserver
APAC-DB-1	Australia Southeast	SQL Server
APAC-WEB-1	Australia Southeast	Webserver
EU-DB-1	North Europe (Dublin)	SQL Server
EU-WEB-1	North Europe (Dublin)	Webserver

# Threat Modeling - Hosting - Documentation

See also (DRAFT) [Threat Model for Wellnomics SaaS](#) and [Threat Model for Wellnomics Client App](#)

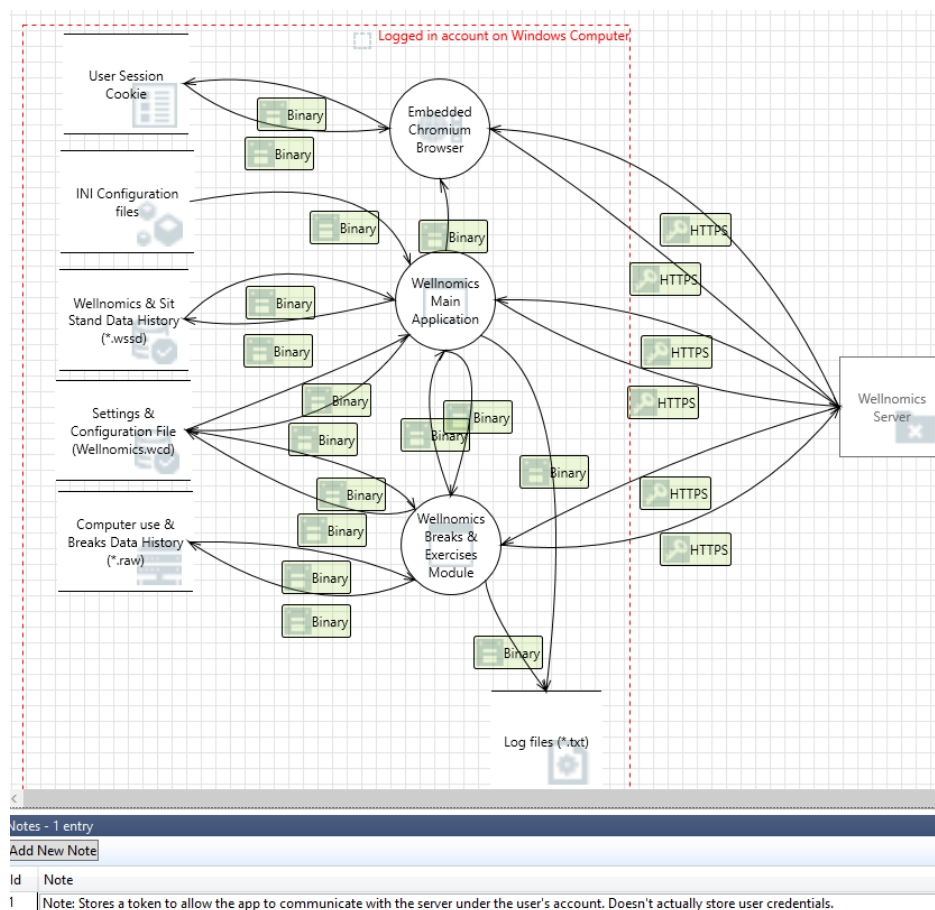
*Draft to be completed!*

Last updated ?

## Threat Model

Created using Microsoft Threat Modelling App (see file below - you will need to download Microsoft Threat Modelling tool)

*Replace the below with hosting threat model*



Wellnomics App Threat Mo...

## Threat Analysis and Mitigation

The threat review generated by the MS Threat Modelling tool is below:

*Add here*

The table below analyses each of these threats, rates their risks according to [Product Security Risk Assessment Matrix - Policy](#) and explains how each risk is mitigated, where mitigation is necessary.

*Table with each row showing:*

- *Risk from MS Threat model*
- *Risk Rating (High/Medium/Low)*
- *Explanation (why its given this rating)*
- *Mitigation (explanation of how risk is mitigated if its High or Medium risk).*

## Related Standards, Policies, Processes and Forms

Based on [Threat Modeling - Hosting - Policy](#)

# Service Level Agreement and Security Statement

**Review period:** Annual

This document summarizes Wellnomics' Level of Service for customers using the Wellnomics solution which is hosted within Microsoft Azure. It should be noted that Wellnomics solution is not a pure SaaS solution but in most implementations includes a key desktop software component (the Wellnomics app) as well. The solution is designed so that any downtime of the SaaS component doesn't affect the availability of the desktop component which will continue operating fine without server availability for long periods (e.g. multiple days).

- Definitions
- Availability of service target
- Downtime
- Server and data security
  - Physical security of data
  - Data and access security
  - Database encryption
  - Server security policy
- Performance and availability
  - Network availability and firewalls
  - Hardware availability
  - Performance monitoring
  - Availability monitoring
- Data redundancy and disaster recovery
  - Protection against data loss
- Software updates
  - Support and issue resolution
  - Incident resolution and escalation process
- Related standards, policies and processes
- Revision history

## Definitions

“**Wellnomics SaaS**” refers to the hosted services provided by Wellnomics for access by users through a browser.

“**Downtime**” means when a Category 1 Issue causes the Wellnomics SaaS to be unavailable for a majority of users.

“**Scheduled Downtime**” means any scheduled Wellnomics SaaS unavailability for maintenance, upgrades, enhancements or changes to the website or Wellnomics SaaS and HR import updates

“**Unscheduled Downtime**” means any unplanned Wellnomics SaaS unavailability that is not covered by Scheduled Downtime.

“**Excluded Downtime**” means any Wellnomics SaaS unavailability or Unscheduled Downtime that is due to factors outside the control of Wellnomics.

“**Service Uptime Percentage**” means the percentage of time the Wellnomics SaaS is available for after accounting for any Scheduled or Excluded Downtime.

## Availability of service target

Wellnomics availability of service target is an annual **Service Uptime Percentage** of 99.5%.



# Downtime

**Scheduled Downtime** includes routine scheduled maintenance or reasonable emergency maintenance and updates and upgrades. Customers will be informed of planned Scheduled Downtime dates and duration prior to these occurring.

HR Import updates also require a period of Downtime as groups and user permissions are re-created based upon latest HR data.

**Unscheduled Downtime** may occur for a variety of reasons that are outside the control of Wellnomics. Examples include:

- Force majeure events or other factors outside of Wellnomics reasonable control, including, without limitation, internet access or related problems that temporarily prevent access to the Wellnomics SaaS (note the Wellnomics SaaS may still be running, but access from certain locations may be unavailable).
- Azure hosting provider outages including hardware failures or data center connection issues and third-party equipment, apps, add-ons, software or technology
- Customer configuration or Wellnomics SaaS usage errors that cause an availability or access issue to the Wellnomics SaaS . For example, accidentally doing an HR data import that incorrectly archives valid users, thereby causing their access to the Wellnomics SaaS to be disabled.
- Customer's equipment, software, network connections or other infrastructure which may affect access to the Wellnomics SaaS
- Incorrect configuration of customer systems that interface with the Wellnomics SaaS but are outside Wellnomics responsibility. For example, incorrect configuration changes or service unavailability of a customer OAuth service that is used to authenticate user access to the Wellnomics SaaS.

# Server and data security

The Wellnomics SaaS runs on a dedicated and fully managed Windows servers hosted within a secure state-of-the-art data centers run by Microsoft on the Azure platform, one of the world's leading hosting companies. A range of physical location options are available, including for example, USA, Australia and Ireland.

The servers running the Wellnomics SaaS run up to date versions Windows Server and Microsoft SQL. Each customer's data is stored in a separate SQL database, ensuring data separation between customers. Physical server security and the security of data are ensured through a number of industry standard safeguards

## Physical security of data

The Microsoft Azure data centers hosting the Wellnomics SaaS are fully certified and independently audited. They are secured by card key access and continual surveillance. For more details on data center security refer to [Microsoft Azure Security and Compliance - Documentation](#) in *Wellnomics Information Security Policies & Procedures*.

## Data and access security

The Wellnomics SaaS has been designed to provide a high level of security against unauthorized access to data. There is a considerable amount of work put into this which is covered in extensive policies and documentation in the *Wellnomics Information Security Policies & Procedures*

## Database encryption

Database encryption-at-rest can be provided on request via use of Microsoft's Encrypted File System (EFS) solution.

## Server security policy

Refer to [Access Security - Hosting - Policy](#) under *Wellnomics Information Security Policies & Procedures*.

# Performance and availability

## Network availability and firewalls

Within the Microsoft Azure environment a number of network protection and firewall systems are enabled including:-

- Redundant Cisco 3-tier LAN Architecture
- Azure Port Monitoring Service

## Hardware availability

Hardware availability is ensured through the choice of Microsoft Azure's world-class data centres with redundant power and HVAC systems, and covered by a worst case scenario 1-hour Hardware Replacement guarantee ensuring that any hardware faults are repaired immediately no matter what time of the day or night they may occur.

There is a 2-hour commencement of onsite data restores in the event of a worst case scenario hardware failure - ensuring that a new server is up and running again with recovered data within 2 hours.

## Performance monitoring

The Wellnomics SaaS has a range of inbuilt database and system integrity and process checks which are shown in a system monitoring dashboard available through the IT Administration Portal .

## Availability monitoring

Wellnomics uses 24/7 continuous monitoring tools to monitor server and Wellnomics SaaS availability and the successful running of key services on each server. Wellnomics Support staff are notified immediately via mobile app and email of any issues requiring attention.

# Data redundancy and disaster recovery

The Wellnomics SaaS uses Locally Redundant Storage (LRS) which replicates the data three times within a single physical location in the primary region. LRS provides at least 99.999999999% (11 nines) durability of objects over a given year. backups are also synced with a secure Azure Recovery service ensuring data can be recovered if there's any local disasters.

Wellnomics manages system backups which are performed **daily**. Multiple backups are retained to ensure reliable restore when required.

**Recovery Point Objective (RPO) is 24 hours** (i.e. the maximum period of data that could be lost since last backup).

**Recovery Time Objective (RTO) is 48 hours** (i.e. the maximum period of time within which the system is recovered after a disaster).

Other aspects of disaster recovery are covered by our data centre supplier - Microsoft. This includes automatic replacement of faulty hardware, data recovery and restarting of servers by the 24x7x365 support staff at Microsoft.

For more on Disaster Recovery refer to [INCIDENT RESPONSE & DISASTER RECOVERY - Policies](#) under *Wellnomics Information Security Policies & Procedures*

## Protection against data loss

Note that the biggest data input for the Wellnomics SaaS is data recorded by the Wellnomics app and the solution is designed to be robust to outages with the Wellnomics app continuing to record and store data for long periods (30 days by default) without server availability. Even if data were to be lost from the server it will be automatically resynced by the Wellnomics app when a connection is restored. This means that even if a restore from backup is required there is unlikely to be any permanent data loss.

# Software updates

Systems are installed using hardened, patched Operating Systems. All updates are tested prior to installation to ensure full compatibility with the Wellnomics software. Hardening is applied to the Operating System, IIS Server and SQL Server. Refer to *Wellnomics Information Security Policies & Procedures* documents [Hardening Checklist - Windows Server OS - Template](#), [Hardening Checklist - SQL Server - Template](#), [Hardening Checklist - IIS Server - Template](#)

## Support and issue resolution

In the event that customers experience any access, performance or usability issues they can be reported by email to [support@wellnomics.com](mailto:support@wellnomics.com) or through Wellnomics website and a support ticket will be automatically generated and prioritized within Wellnomics support system. Wellnomics support staff monitor all support tickets and have a target response time to all support tickets of 1 business day (based on New Zealand business hours).

Wellnomics will endeavor to fix any reported issues as quickly as possible. However, some issues may require considerable technical work to firstly identify the cause, then if needed, develop and test a software fix, then deploy any fix to servers. The table below shows the worst case time limits for addressing issues of different severity.

Wellnomics support hours are 8:30am to 5pm Monday-Friday New Zealand Daylight Time excluding public holidays. Support may be provided outside these hours either (i) by prior arrangement or (ii) if a Category 1 issue needs to be resolved.

Issue severity	Description	Target worst case time limit for correction
<b>Category 1</b>	An issue causing the Wellnomics SaaS to be totally inoperable or unavailable for a majority of users for more than 15 minutes	48 hours (RTO)
<b>Category 2</b>	An issue causing significant loss of functionality, performance or access to the Wellnomics SaaS for a significant proportion of users for more than 15 minutes. No workaround available.	7 days
<b>Category 3</b>	An issue causing significant loss of functionality, performance or access to the Wellnomics SaaS for a significant proportion of users for more than 15 minutes. Workaround available.	21 days
<b>Category 4</b>	Any other issue	Next product update subject to issue priority based upon Wellnomics Issue severity ranking and prioritization matrix

## Incident resolution and escalation process

Escalation procedures are in place and communicated to the customer so that they have access to Wellnomics management. These procedures provide increasing levels of authority.

Support Team => Customer Success Manager => CEO

## Related standards, policies and processes

- [Management of Hosting - Policy](#)
- [Access Security - Hosting - Policy](#)
- [Threat Modeling - Hosting - Policy](#)
- [Microsoft Azure Security and Compliance - Documentation](#)
- [SaaS Service Level Agreement - Uptime Monitoring - Guideline](#)

## Revision history

Date of change	Responsible	Summary of change	Next revision date
30 Mar 2016	Wayne Owens, Principal Consultant	Updated and converted to new format.	29 Mar 2017 <a href="#">Wayne Owens (Unlicensed)</a>
03 Jul 2017	Wayne Owens, Principal Consultant	Updated aspects relating to the use of licensed software for dedicated hosted server maintenance workstation	04 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
17 May 2018	Kevin Taylor, CEO	Updated section on Backups for cloud servers.	04 Jul 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay	Reviewed, no changes made	
1 March 2019	Kevin Taylor	Updated requirements on server patches and hardening and Rackspace backups policies	<ul style="list-style-type: none"> <li>01 Mar 2020 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
05 Jun 2020	Wayne Owens	Reviewed and updated to change references from Rackspace to Microsoft Azure	<ul style="list-style-type: none"> <li>21 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
24 Aug 2020	Angeli Arino	Converted to a new page	
07 Jan 2021	<a href="#">Kevin</a>	Updated to include latest Azure based info and latest server software versions plus added links to related policies	
07 Jan 2021	<a href="#">Chris MacKay (Deactivated)</a>	Updated page to include new OS, SQL and IIS versions. Also updated Disk and Backup section to reflect recent changes in these areas.	
04 Oct 2021	<a href="#">Ian Bartram</a>	Reviewed SLA and updated to reflect improved procedures and new processes with Azure	<ul style="list-style-type: none"> <li>07 Oct 2022 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	<a href="#">Ian Bartram</a>	Updated backup information to include the offsite cloud storage of backups.	<ul style="list-style-type: none"> <li>25 Jan 2024 <a href="#">Ian Bartram</a></li> </ul>

# SaaS Service Level Agreement - Uptime Monitoring - Guideline

The Wellnomics SaaS SLA <https://wellnomicsdev.atlassian.net/wiki/pages/resumedraft.action?draftId=42868567> has a target of 99.5% **Service Uptime Percentage**. The SLA also provides definitions of:

- **Downtime**
- **Scheduled Downtime**
- **Unscheduled Downtime**
- **Excluded Downtime”**

We need to be able to measure the **Service Uptime Percentage** of all our customer sites so we can report on this to our customers and check that we are meeting our targets.

To do this we need to:

- maintain a list of **Monitored Sites**. This should include all Standard SaaS and Bespoke SaaS sites and selected other sites like the Wellnomics Company Website and Demo Site.
- Use pulseway to monitor 'Uptime' for every **Monitored Site**
- Long term we need to measure any time with a **Category 1 Error**. But for now a site being 'up' is defined as being that the login page is rendered and available
- We will produce a monthly report covering every **Monitored Site**
- The report will show **Raw Uptime** % for each month - which is simply the % of time the site login page was available.
- If the **Raw Uptime Percentage** is < 99.5% then Wellnomics Support will review the detailed logs to
  - Filter out any downtime periods <15 mins.
  - List the number of outages >15 mins and classify each outage by its cause
  - Each cause needs to then be classified as either
    - **Excluded Downtime**
    - **Scheduled Downtime**
    - **Bad Downtime**: Downtime that counts against our **Service Uptime Percentage**
  - If this is for a key customer like Intel, provide the report to Customer Success Manager so they can provide it to Intel.
  - If the net **Service Uptime Percentage** is still our SLA target of 99.5 % then escalate to Customer Success Manager for action, as we may owe the customer a Service Credit.

# Monitoring - Hosting - Guideline

Wellnomics has a range of monitoring services in place to monitor performance and availability of the SaaS platform and customer specific implementations. These are described below

## Web server availability

An uptime monitor is used to monitor in real-time the availability of all web servers. Any downtime or unavailability is notified immediately to support staff 24/7. Further RMM services are used to monitor server resources and events.

## Network responsiveness

Monitoring tools provided by Azure are used to monitor the network responsiveness of each server and identify and notify support staff of any load issues and track load levels and patterns over time.

## Discrete number of network connections

There is logging of the number of network connections also which provides performance measures for servers that allow support staff to take action to improve load balancing if needed.

## Success/failure of scheduled processes

Automated or on demand batches services such as the HR data import & update automatically provide email notifications of success and failure to either Wellnomics or customer support staff. Detailed logging within the system allows analysis of reasons for any failure so appropriate corrections can be made if needed.

## System check

For each customer implementation there is a system check panel that verifies the correct status of all system components and modules. If there are any errors these are displayed on the system check page. An automated system check email can also be configured to provide a regular update on the system status.

# System check

## Wellnomics Admin

- ✔ **Database Version**  
Database version (4.4.0) is compatible.
- ✔ **Time Zone**  
The time zone is configured for this system.
- ✔ **Website URLs**  
The website URLs are configured for this system.

## Wellnomics Synchronization

- ✔ **Web Service Connection**  
Connection successful.
- ✔ **Application Version**  
Applications are compatible.
- ✔ **Database Connection**  
Database connection successful.
- ✔ **Database Configuration**  
Wellnomics Synchronization database configuration matches.
- ✔ **Logging Check**  
Log directory is accessible by the Wellnomics Synchronization.

## Wellnomics HR Import Service

- ✔ **Service Connection**  
Communication successful.
- ✔ **Application Version**  
Applications are compatible.
- ✔ **Database Connection**  
Database connection successful.
- ✔ **Database Configuration**  
Wellnomics HR Import Service database configuration matches.
- ✔ **Status Check**  
HR Import has not completed a job since the service was started. The HR Importer last polled for work at 24 Jun 2021 4:39 AM. The HR Validator last polled for work at 24 Jun 2021 4:39 AM.
- ✔ **Logging Check**  
Log directory is accessible by the Wellnomics HR Import Service.

## Wellnomics Portal

- ✔ **Web Service Connection**  
Connection successful.
- ✔ **Application Version**  
Applications are compatible.
- ✔ **Database Connection**  
Database connection successful.
- ✔ **Database Configuration**  
Wellnomics Portal database configuration matches.
- ✔ **Application Pool Pipeline Check**  
Managed pipeline mode is set to 'Integrated' for the Wellnomics Portal in application pool 'wellbeing.wellnomicsonline.com' in IIS.
- ✔ **Logging Check**  
Log directory is accessible by the Wellnomics Portal.

# Disaster Recovery and Business Continuity - Hosting - Guide

physical hardware issues are covered by Microsoft Azure guarantees, our scenarios cover those under our control

## Objective

Outline business critical systems, disaster scenarios, a plan for restoration, and expected timeline.

## Contacts

Name; Title	DRT Role	Contact Option	Contact Info
Ian Bartram; Systems Administrator	Hosted systems restoration	Mobile Email	022-515-3633 <a href="mailto:ian.bartram@pm.me">ian.bartram@pm.me</a> , <a href="mailto:ian.bartram@wellnomics.com">ian.bartram@wellnomics.com</a>
Sam Dravitzki; Software Engineer	Hosted systems restoration backup	Email	
Matt Holland; Sr Developer	Hosted systems restoration backup		
Corinne Wright; Customer Success Manager	Customer communication	Email	

## Business Critical Systems

These systems include the VM and all managed resources, see diagram of all resources here [Azure hosted VM architecture](#)

- AMER-DB-1
- AMER-WEB-1
- AMER-WEB-4
- APAC-DB-1
- APAC-WEB-1
- EU-DB-1
- EU-WEB-1

## Scenarios

1. **Unresponsive Azure Agent;** Occasionally the Agent which manages communication between the VM Azure will enter an unresponsive state. This renders the VM essentially functionless.
2. **System Failure;** Due to system file corruption or a bad windows updates the OS can occasionally fail.
3. **Data Failure;** Corrupted data drive or full loss of the attached storage.

## Scenario - Unresponsive Agent

System/ Task	Threat	Resolution	Timeline to full restore	DRT Contact
--------------	--------	------------	--------------------------	-------------



Hosted VM	Agent unresponsive	<a href="#">Redeploy + Reapply VM</a>	10-15min	Ian, Sam, Matt
-----------	--------------------	---------------------------------------	----------	----------------

## Scenario - System Failure

System/ Task	Threat	Resolution	Timeline	DRT Contact
Hosted VM	System Failure	<a href="#">Deploy a backup</a>	1-2 days	Ian, Sam, Matt

## Scenario - Data Failure

System/ Task	Threat	Resolution	Timeline	DRT Contact
Hosted VM	Attached disk Data corruption	<a href="#">Restore disks</a> or <a href="#">Recovery files</a>	1-2 days	Ian, Sam, Matt

Date of Change	Responsible	Summary of Change	Next Revision date
06 Jun 2022	Ian Bartram	New document established	<ul style="list-style-type: none"> <li>05 Dec 2022 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	Ian Bartram	Separated some information into guides.	<ul style="list-style-type: none"> <li>29 Feb 2024 <a href="#">Ian Bartram</a></li> </ul>

# INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Documentation

- Critical Events - Guidelines
- Monitoring - Internal - Guideline
- Website Terms & Conditions (not Hosting)
- Passwords & Encryption - Employees & Contractors - Guidelines
- Building Security - Documentation
- Disaster Recovery and Business Continuity - Internal - Guide
- Security & Privacy Training - Employees & Contractors - Guideline
- Employee Agreement & Contract - Example
- Employee Position Description - Example
- Disciplinary Procedures - Employees & Contractors - Guidelines
- INTERNAL ONLY

# Critical Events - Guidelines

**Review period:** Annual

## Purpose

To ensure all Staff Members remain as safe as possible in any Pandemic, natural or other Disaster so that the Wellnomics business can continue to operate with minimum disruption. This will be achieved through the implementation of a robust plan prior to the occurrence of any Critical Event.

## List of Appendices

1. Planning for a Critical Event - Personal Information form
  - Process Summary & Checklist – Planned Events
  - Process Summary & Checklist – Unplanned Event
2. Business Critical Functions & Personnel
3. Pandemic Containment Activities
4. Screening Checklist and Influenza Recording Templates
5. Public Area Notices
6. Survival Kit Inventories

## Key Points

- Wellnomics offices will remain open for business as long as you are not put at risk during any Critical Event, taking into account its responsibility under the Health & Safety in Employment Act Section 6: "Every employer shall take all practicable steps to ensure the safety of employees while at work....."
- Wellnomics has classified Critical Events into 2 types:
  - a. Planned – Pandemic (maybe days or weeks notice to plan), a tsunami, floods, storms, tornados etc (maybe only hours to plan) Refer Appendix 2A, and
  - b. Unplanned – Earthquakes, fire, (refer - Emergency Procedures Guidelines) collapsed building & terrorist attacks (we can plan for these events but will probably have no time for specific planning before the event) Refer Appendix 2B. Wellnomics will have procedures in place to ensure that Staff and the business are protected as much as possible in the event of a 'Planned' and 'Unplanned' Critical Event
- For any Critical Event, staff who are travelling overseas may be unable to return (due to quarantines or inaccessibility of airports etc). Wellnomics will cover approved costs (telephone approval from the GM or a Director) that he/she incurs overseas until he/she is able to return. The Staff Member's family situation will be considered and appropriate support will be provided with every situation considered on a case by case basis. It is probable that, for any disaster localised within New Zealand, staff located and/or stranded overseas will be enlisted into the CMT to assist with implementing any communication and business continuation plans.

## Planned Critical Events

- A Pandemic is an outbreak of an infectious disease that we are advised may last for 6 + weeks with an unknown advance notice timeframe and will affect people or animals over an extensive geographical area. It can include Influenza, Avian Influenza / Pandemic Influenza or Novel viruses. The Ministry of Health (DHB) started planning for a potential Pandemic in 2005. A Pandemic may not occur but the 'experts' say that the odds are that it will. Wellnomics wishes to be prepared for the worst and will hope for the best.

## Pandemic

- is likely to be widespread, and not localised to a single area. Could result in New Zealand being completely isolated

- could mean that within our communities we have a very high morbidity and chronic illness rate, severely impacting on our society and economy
- is not a physical Disaster, it has some unique characteristics that will require specific action to limit contact, such as restriction of movement, quarantine and closure of public gatherings
- is not a short, sharp event leading immediately to commencement of a recovery phase (as could be the case for Unplanned Critical Events)
- may come in waves of varying severity that may last about 8 weeks each over a period of time or may have a short warning period and if it spreads within New Zealand it will probably be some weeks before the full impact on the workforce will be felt. There may be some more immediate impacts resulting from closing of schools and similar containment measures
- is unlike natural Disasters, and it is anticipated that disruptions to business will be mainly human resource orientated - the Ministry of Health advises that businesses should plan for up to 50% Staff absences for periods of about two weeks at the height of a Pandemic wave, and lower levels of Staff absence for a few weeks either side of the peak.
- Health services may be under extreme pressure as an estimated 40% of the workforce may be sick, with further absenteeism if schools are closed
- Full community mobilisation may be necessary (as with the 1918 'flu') and all government and community agencies may be involved in a wide range of societal responses A Pandemic could result in the quarantine of the Central Business District (CBD) and the closure of all public transport and facilities etc. Wellnomics will endeavour to provide you with an opportunity to work from home if practicable. Some of you, due to the nature of your jobs, may not be able to work from home. Please refer to the Working From Home Guideline for further details.

## Tsunami, flood, storm, tornado etc

We may be provided with some notice time to plan for these Critical Events and Wellnomics will use as much as possible of the planning preparation in place for a Pandemic if time permits

## Unplanned Critical Events

- **Natural and Other Disasters can include** – earthquake, fire, collapsed building, terrorist attack, volcanic eruption, floods etc (if no notice is given) and other similar events – please refer: [www.civildefence.govt.nz](http://www.civildefence.govt.nz)
- **A Critical Event Survival Kit has been established.** The items contained within this kit and its location are detailed in Appendix 7. Note that the First Aid Kit is located in the stationery room.
- **A small store of non-perishable food and bottled water** is kept in the kitchen cupboard for use by Staff who may be stranded on Wellnomics premises under circumstances when no other food and/or source is feasible. The items contained within this store are also listed in Appendix 7. The majority of these items are nonperishable, however, those which are not are assessed and replaced every 3 months by the Administration Assistant. A reminder to do so is logged in the Boardroom calendar.
- Insurance Policies have been updated and the majority of our business transactions, including payment of salaries which are completed 'on line' so this will ensure business stability during any Critical Event

## Procedure - Business Critical Issues

As a small business, all functions performed by Wellnomics Staff are vital to the successful running of the business – as are the Staff within each role. With most functions fulfilled by only one Staff Member in small teams, we do not have a variety of unessential tasks or the luxury of Staff overlap enjoyed by larger organisations. However, in the occurrence of a Critical Event, we may be faced with the possibility of incapacitated Staff. We need to be pragmatic and identify Business Critical Processes and Personnel and have strategies in place to ensure that Wellnomics can continue to function:

- At the lowest level, there are certain Business Critical Processes without which Wellnomics would not be able to function nor maintain financial viability. Identifying and continuing these processes during a Critical Event is fundamental in maintaining the basic operation of the business.
- Likewise, there are Business Critical Personnel and assigned Backups (refer Appendix 3) identified to ensure Wellnomics can continue to function. It is essential that there are assigned Backup for Staff in these core roles, to ensure that the functions are still able to be carried out in the event of incapacitation of the defined Business Critical Personnel.
- While Backup Staff will have received training to enable them to maintain the essential functions of the applicable key role, it is important to remember that this is not their normal function and that constructive support from other Staff is vital.
- In preparation for a Critical Event, two Crisis Management Co-ordinators (CMC) have been appointed. These people will provide information and act as liaisons between Government and other agencies, Management and Staff. They essentially provide a hub through which the information flows, ensuring efficiency of communication. The CMC will be the point of

contact for all Staff wherever practical and directives and requests to and from the General Manager (GM) and Directors will be channelled through them.

The identified Business Critical Functions & Processes, Personnel, Crisis Management Co-ordinators and all identified Backup Staff are listed in Appendix 3 of this document.

When a Critical Event occurs, this information and all contact details will be available via the Wellnomics Website and/or Intranet.

## Procedure - Planned Event - Pandemic

The following websites are available for more information and you are encouraged to check out these websites and be well prepared for a Pandemic both personally and at work. Please advise all other Staff if you have any additional websites or information that would be of assistance to you or Wellnomics:

<http://www.moh.govt.nz/Pandemic>

<http://www.moh.govt.nz/Pandemicinfluenza>

<http://www.med.govt.nz><https://covid19.govt.nz/>

[http://www.pegasus.org.nz/pegasus\\_internet/](http://www.pegasus.org.nz/pegasus_internet/) (This has a good Family Checklist & FAQ Patient Information, we recommend you read this and take appropriate action. Refer Appendix 4)

Hard copies of Ministry of Health documents and information from other sources are on a file held by the Human Resources & Administration Manager (HRAM). You are welcome to borrow this file to go through, but please make sure that you advise the HRAM that you have done so and that it is returned no later than 2 working days after you borrow it.

- Please become familiar with and agree to follow the procedure in Appendix 2A if/when a Pandemic is declared for Canterbury (it is possible that an outbreak may be contained to a specific region). This will be considered to have occurred when there has been a declaration made to this effect by the Government.
- **Communication:**
  - Due to the infectious nature of a Pandemic, effective communication with you is vital and necessitates the development of a communications strategy that will involve you, your families, Wellnomics customers, suppliers and Resellers
  - Communication tools used by Wellnomics will include – telephone, Guidelines, websites, email from Wellnomics premises and email from your home
  - Public communication tools will include – print media, radio media, DHB pamphlets, 0800 hot lines, email and texting. The Ministry of Health website will be a primary information source - [www.moh.govt.nz](http://www.moh.govt.nz)

### Travel

- All non-essential travel will be stopped for the duration of any Pandemic occurrence
- Those returning to New Zealand may be required to undergo additional screening and quarantine and may be subject to exit screening at the point of their departure
- The Ministry of Foreign Affairs and Trade will provide travel advice which can be accessed via their website [www.mfat.govt.nz](http://www.mfat.govt.nz)

## Health Monitoring

- A chart is posted in the Staff room and in the men's and women's toilets (Appendix 6) which will assist you to identify whether symptoms indicate signs of a cold or influenza or COVID. Please familiarise yourself with these differences
- If you start to feel unwell at work and suspect that you may be suffering from the Pandemic illness:
  - i. Immediately put on your surgical mask
  - ii. Advise a Crisis Management Co-ordinator (CMC) – preferably by telephone
  - iii. The CMC will go through the Screening Checklist (Appendix 5) with you to determine whether you are a possible influenza case and follow with appropriate action. Please familiarise yourself with the three documents that make up this Checklist and notification forms so that you will be prepared for the actions and information required.
  - iv. Public transport should be avoided if at all possible – Wellnomics will pay for a taxi fare if necessary
- If you suspect that someone else may be suffering from the Pandemic illness:

i. Immediately advise a Crisis Management Co-ordinator (CMC)

- Returning to work:
- Staff Members who have not suffered from the Pandemic illness:
- A CMC will ensure that you are advised of the GM's or Director's notification of a specific day when you will be able to return to work on 'normal' work conditions.
- Staff Members who have suffered from the Pandemic illness:
  - A signed clearance from a GP is required before Staff Members who have been ill will be permitted to return to work
- Staff Members who have been in contact with other people who have suffered from the Pandemic illness, although they have not been sick themselves:
- An approved quarantine period must have been completed and/or a signed clearance from a GP is required before Staff Members who have been in contact with others who have been ill will be permitted to return to work

## Procedure - Planned Event or Unplanned Event – Natural or Other Disaster

### General

- a. Disruptions will be more physical – could be home or office relocations
- b. Security could be an issue for individuals and property e.g. anarchy & rioting after an earthquake etc
- c. Please become familiar with and agree to follow the procedure in Appendix 2B if/when a Disaster occurs
- d. When a Critical Event occurs, Wellnomics will provide you with an additional 3 days Sick Leave that can only be taken from a date provided by the GM or a Director

### Communication

- a. We anticipate this will be out of Wellnomics's control and you will be advised of the process etc via public communications systems
- b. A CMC will contact you as soon as practically possible after the Critical Event (refer Appendix 2B) and provide you with regular updates – your Manager will also be in contact with you and provide 'work' information when appropriate

### Earthquake - What to do:

- a. Before:
  - i. Identify safe places very close to your workstation such as under a solid desk or next to a short strong interior wall.
  - ii. Wellnomics will ensure property is protected by securing bookcases and other similar furniture as appropriate
- b. During:
  - i. Move no more than a few steps to a safe place (away from windows), cover and hold
  - ii. Do not go outside
  - iii. If in the lift, stop at the nearest floor and get out, get down as low and cover yourself as best you can and wait until the shaking stops.
  - iv. If you are driving, pull over to the side of the road. If you are in an open area where there is no danger of anything falling on your car, stay in the vehicle until the shaking stops. If you are in a situation where there is the possibility of something falling on our car – eg. building, trees – get out of your car and lie beside it until the shaking stops.
- c. When the shaking stops
  - i. Treat any injuries and put out small fires
  - ii. Work with other Staff and turn off all water, electricity, gas and heating at the mains
  - iii. Evacuate if fires cannot be controlled
  - iv. Check on your colleagues
  - v. Be prepared for after-shocks
  - vi. Listen to the radio for advice and information or check the internet and other public media which may be operational
  - vii. Get help if required by going to a Civil Defence Report Centre – nearest location is on the grassed area at Latimer Square, or to an Emergency Sector post – nearest location is Christchurch East School on the corner Madras and Gloucester streets. Note that in a severe emergency, help may not be available immediately.

## Volcanic Eruption - What to do

### a. Before:

- i. Take note of any public communication of any active volcano zone where you live or close to work Guidelines – Critical Events Page 6 of 18
- ii. When there is a warning of an imminent eruption, begin saving a supply of water as supplies may become contaminated by ash

### b. During:

- i. Stay indoors
- ii. If you must go outside, use protective clothing, cover your head, breathe through a cloth or mask and carry a torch – these items will be in the Stationery room with the first aid kit

## Storm

### a. When a storm warning is issued:

- i. GM or a Director (via a CMC) will advise you when it is advisable to go home
- ii. A CMC will advise you who and when (if possible) to make contact with at work, work from home (if applicable) if the storm is anticipated to last some time

## Flood

### a. Before:

- i. Find out about any flood risk close to your home and advise a CMC when/if you are unlikely to be able to travel to work
- ii. Ensure you are aware of the procedure to follow when there is flooding at home

### b. When a flood threatens:

- i. Listen to the radio (refer to Appendix 7 for its location), check the websites if electricity available and follow the Civil Defence instructions
- ii. Disconnect all electrical appliances and if no longer working in the offices leave electricity disconnected
- iii. If it is considered that there will be flooding or water leaking into the offices, shift valuable property out of danger

## Tsunami Warning

- a. The CMC will advise the appropriate action to be taken, as our offices are more than 1km from the sea we may be able to continue business at our offices. The CMC will need to know your personal circumstances so the appropriate decisions can be made to suit all Staff – refer Appendix 1
- b. Check the website [www.civildefence.govt.nz](http://www.civildefence.govt.nz) and listen to the radio for information and follow the Civil Defence instructions
- c. Go at least one kilometre inland or 35 metres above sea level
- d. Do not go sightseeing to the beach or river

## Travel

All non-essential travel will be stopped for the duration of any Disaster

## Additional Leave

When a Critical Event occurs, Wellnomics will provide you with an additional 3 days Sick Leave that can only be taken from the date the GM advises the Sick Leave can be taken

## Updating Guidelines

This document will be reviewed by the CMC and GM every 6 months. If an update – due to legislation or governmental recommendation – is required, all staff will be notified and the updated version will replace the previous version for both the electronic and hard copies. It is intended that the foundation of the Guidelines will remain unaltered. No consultation process will be implemented when updating Guidelines because of regulatory or practical requirements. However, if the document requires updating beyond these parameters, the standard consultation process will be followed unless there is a clear case for immediate implementation of the new Guidelines.

## Employee Responsibilities

The company is committed to providing and/or supporting the means and information to enable Staff to work from home on the occurrence of a Critical Event. However, it is up to individual Staff to ensure that they have Guidelines – Critical Events Page 7 of 18

followed or implemented the requirements specified in this document and the Working From Home Guideline or as otherwise instructed. Within the actual duration of Critical Event or its aftermath, Wellnomics Ltd is not obliged – nor will potentially be able – to implement practical or physical means to allow an Employee to work from home. As many measures as are practicable must be in place prior to the event. Please ensure that all information noted in the Staff Critical Event Form (Appendix 1) is maintained so that in the occurrence of a Critical Event the information on your file is current.

## FAQ's

Q – Can we take our Annual Leave if we are away from work for more than 3 days due to a Critical Event and are unable to work from home?

A – Yes

Q – Can you force me to take my Annual Leave in a Pandemic situation?

A – Under S9 of the Holidays Act an employer can require you to take accrued Annual Leave on at least 14 days notice. However, in a Pandemic situation there may be less time to make decisions. While Wellnomics cannot currently require you to take Annual Leave with less than 14 days notice, in a crisis situation you and Wellnomics will be expected to act in 'good faith'

Q – If there is a Pandemic of some kind can you make me work from home – or in a different place?

A – Clearly it is in your and Wellnomics's interests that our business survives a Pandemic. In a Pandemic, life will not be normal. Both you and Wellnomics need to respond flexibly to different scenarios that arise from a Pandemic. This is why we have established the Work from Home and Emergency Offsite plans that provide you with information and reference sites. This should enable us to continue to operate our business and remain open throughout any Pandemic. If Wellnomics asks you to arrive at solutions that are not covered in your current employment agreement we will both be expected to operate and act in 'good faith'

Q – If there is a Pandemic can you stop me coming to work when I may want to?

A – We are planning now so that this situation will not apply. However, we can stop you coming to work if we consider that the workplace is not a safe place for you. In a similar situation Wellnomics can ask you to stay at home if you are sick and represent a safety risk to the workplace or other Staff.

Q – In a Pandemic situation or other Critical Event, if I haven't any Annual Leave or Sick Leave and I am ready and willing to go to work and you will not allow me to - do I still get paid?

A – Wages are normally payable if you are ready and willing to come to work. However, a Pandemic scenario is likely to create some uncertainties. Wellnomics is not able to say how long it could continue to sustain salary payments if we are closed for a period of time. Obviously, in a serious Pandemic situation there will be limits for all employers. It is fortunate and an advantage that we have developed a process to enable working from home where possible, so that, if practicable, you can do so and therefore hopefully minimise the personal and business impacts

Q – If there is a Pandemic, are we entitled to redundancy if Wellnomics closes permanently?

A – Your entitlement, if any, will be as per your employment agreement.

Q – In a Disaster situation – like an earthquake – and I can't get to work for some reason – can I work from home?

A – In many cases that will be possible, but will have to be assessed on a case-by-case basis in reference to the magnitude of the event and the requirements of your role.

Q – Is it certain that we will be able to be paid during a Critical Event?

A – Although we can not guarantee a contingency for every unforeseen eventuality, we have done as much as is possible to ensure that salaries will be able to be paid during a Critical Event. Payroll has been identified as a Business Critical function and backups are in place to cover incapacitation of those who are normally involved in processing payroll. Westpac have provided confirmation that they have a Business Continuity Plan that will ensure that its online banking services – via which we will process all payments during a Critical Event – remain accessible and active as well as various alternative processes that the CMC will co-ordinate.

Guidelines – Critical Events Page 8 of 18



# Revision History

Date of change	Responsible	Summary of change	Next revision date
6th December 2016	Wayne Owens, Principal Consultant	Updated and converted to new format	10 Dec 2017 <a href="#">Wayne Owens (Unlicensed)</a>
08 Mar 2017	Wayne Owens	Amended contact lists	10 Dec 2017 <a href="#">Wayne Owens (Unlicensed)</a>
04 Dec 2017	Wayne OWens	Checked for up to date - all OK	05 Dec 2018 <a href="#">Chris MacKay (Deactivated)</a>
21 Nov 2018	<a href="#">Chris MacKay (Deactivated)</a>	Checked, all ok	<ul style="list-style-type: none"> <li>21 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
21 Nov 2019	<a href="#">Wayne Owens</a>	Reviewed to ensure contact and web links up to date	<ul style="list-style-type: none"> <li>26 Nov 2020 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
27 Nov 2019	Chris Mackay	Reviewed to ensure contact and web links up to date - minor changes only	<ul style="list-style-type: none"> <li>19 Nov 2020 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
31 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"> <li>31 Aug 2021 <a href="#">Corinne</a></li> </ul>
01 Sep 2021	Corinne Wright	Updated to reflect updated Govt COVID Guidelines	05 Sep 2022 <a href="#">Corinne</a>

## APPENDIX 1

### Planning for a Critical Event – Personal Information Form

If a Critical Event occurs, one assumption is that some of you may not be able to attend work due to the need to care for dependants or circumstances do not allow you to work at our offices. We are in a unique position where, if possible, Wellnomics can create an environment where you can work from home if your job allows. We can communicate by telephone to ensure that you have the option to continue to work (if it is available in this unknown territory) and retain an income in what could be a very difficult situation. To assist us in planning for this and to continue to support our customers and Resellers, who may or may not be affected by a Pandemic at the same time and any Disaster, we would appreciate an update of your personal details and an answer to the following questions. This information will be placed in hard-copy on your Personal File and in the Disaster Recovery manual as well as in soft-copy within the HR drive. All of these repositories are subject to strict confidentiality enforcement in accordance with the Wellnomics Privacy Guideline.

Name:  
Street Address:

Home Telephone: Home Fax:  
 Home Email Address: Mobile Telephone:  
 Next of Kin: Relationship to you:  
 Home Telephone: Mobile Telephone:  
 Contact Not Living with  
 You:  
 Relationship to you:  
 Home Telephone: Mobile Telephone:  
 Do you have any Dependants who rely on you for care? This information will help us to understand your needs during a Critical Event (e.g. children who would normally be at school etc) Yes No  
 If 'Yes' – Please detail and advise facilities normally attended/used: (Pre-School, School, University, Hospital, Retirement home, etc)  
 Do you have any other commitments that may affect your ability to work during a Critical Event? (E.g. Civil Defence or Community Warden, voluntary Fire Brigade etc) Yes No  
 If 'Yes' – Please detail  
 If Public Transport is unavailable, will you need transport assistance to get to work? Yes No  
 To assist Wellnomics in its response to a Critical Event:  
 Do you have any Civil Defence experience or other similar experience? Yes No  
 If 'Yes' – Please detail  
 Do you have a current First Aid Certificate? Yes No  
 Tsunami risk - Do you live less than 1 kilometre from the sea? Yes No  
 Other Relevant or Helpful Information:  
 Working from home:  
 Do you have facilities at home which will enable you to participate in any Work from Home Plan (please refer to the IT procedure "Remote Working" for technical recommendations)? Yes No  
 Have you read the Conditions of Employment, Wellnomics Resources and Working from Home Guidelines and do you understand and agree to any security requirements? Yes No  
 This Form must be updated with any changes as soon as they occur. Please notify your manager or the HR Manager if this is required. A full staff update will be undertaken periodically. Thank you  
 Guidelines – Critical Events Page 9 of 18

## APPENDIX 2a

### Process Summary & Checklist

#### Planned Critical Event – Pandemic & Forewarned Natural Disaster Procedure

1. The CMT will meet (either virtually or in person, depending on the level of the alert or escalation) to make an action assessment based on the level of alert declared.

It is likely that as soon as there is a verified case of a pandemic illness in New Zealand that the decision will be made to temporarily close the Wellnomics office and implement the 'Work from Home Plan' (refer Working from Home Guideline) procedures. However, other potential actions may be implementation of containment activities such as social distancing, extra cleaning etc (refer Appendix 4).

2. A CMC will advise all Staff of the assessment made by the CMT and confirm actions as soon as practicable

3. A CMC will ensure as much as practicable that all Business Critical Personnel and their Back Ups have the necessary information and logistical support to enable Business Critical Functions & Processes to continue.

#### Crisis Management Team's Checklist - Pandemic

##### Procedure Actioned By Date Actioned Time Actioned

Meet with all available team members immediately a Pandemic is imminent or suspected

CMC to advise all staff immediately to read this Guideline and prepare for a Pandemic

CMT to determine a Communication Plan to be communicated to all Staff

CMC to advise staff if/when it will be appropriate to action the 'Work from Home' plan

CMC to advise Staff of GM or Directors' approved "Return to Normal Work" date

Received Doctors' Certificates ' Clearance to Return to Work

Record any Quarantine requirements on the Personal File

#### Crisis Management Team's Checklist - Forewarned Natural Disaster

##### Procedure Actioned By Date Actioned Time Actioned

Meet with all available team members immediately a public warning has been announced

CMC to advise all staff immediately to read this Guideline and prepare for the event

CMT to determine a Communication Plan to be communicated to all Staff  
If appropriate, CMT to assess and action an 'Emergency Offsite' plan

CMC to advise staff if/when it will be appropriate to action the 'Work from Home' plan or other location as per the 'Emergency Offsite' plan

Guidelines – Critical Events Page 10 of 18

## APPENDIX 2b

Process Summary & Checklist

Unplanned Critical Event – Natural & Other Disasters

Procedure

1. Notification will come from the Civil Defence or a CMC

2. The CMT will meet (either virtually or in person, depending on the level of the alert or escalation) to make an action assessment based on the level of alert declared. The results of their assessment may range from recovery plan to a date to return to work (refer Appendix 4) to temporary closure of the Wellnomics Offices

3. A CMC will advise all Staff of the Disaster situation determined actions as soon as practicable

4. A CMC will ensure as much as practicable that all Business Critical Personnel and their Back Ups have the necessary information and logistical support to enable Business Critical functions to continue.

Crisis Management Team's Disaster Checklist

Procedure Actioned By Date Actioned Time Actioned

Meet with all available team members immediately a disaster occurs or is suspected

CMC to advise all staff immediately to read this Guideline and prepare for a Disaster if time

CMT to determine a Communication Plan to be communicated to all Staff

If appropriate, CMT to assess and action an 'Emergency Offsite' plan

CMC to advise staff if/when it will be appropriate to action the 'Work from Home' plan or other location as per the 'Emergency Offsite' plan

CMT to assess actions/requirements necessary to facilitate returning to normal work and implement as determined

CMC to advise Staff of GM or Directors' approved "Return to Normal Work" date

Guidelines – Critical Events Page 11 of 18

## APPENDIX 3

Business Critical Functions and Personnel

1. Business Critical Functions & Processes

Administration Accounts Payable, Accounts Receivable & Payroll

Sales Administration – Website & Email

IT/Product Development Back up data - retrievable in Critical Event situation

Continue Software Development & Key Deliveries

Sales Advising Customers & Resellers of 'Business Status' and maintain appropriate email/phone contact

Support Continue support and/or implementation services for critical clients

2. Business Critical Personnel & Assigned Back Ups

Business Critical Personnel: Back Ups

Management General Manager – Sue Brown Director – Kevin Taylor

Director – Rob Van Nobelen

Product Development Software Development Manager – Graham McMillan Director - Rob van Nobelen

Software Team Lead – Thomas Kux Snr Software Eng. – Bernard Darnton

IT Administrator – Support Team Lead – Tony Galbraith

Administration HR & Administration Manager – Barbara Watson Financial Controller – Philippa Green

Sales & Support USA - International Sales Director – Trevor Foster Head of Prod. & Spt – Wayne Owens

NL – Country Manager – Bart Broekhuis General Manager – Sue Brown

Marketing Officer – Astrid Groeneweg General Manager – Sue Brown

Head of Prod. & Spt – Wayne Owens Support Team Lead – Tony Galbraith

3. Crisis Management Co-ordinators

## APPENDIX 4

### Pandemic Containment Activities

There are strategies that can be employed as protection against the spread of a Pandemic. In the event of a Pandemic, the following Guidelines should be adhered to whenever practicable.

#### Properly Wash & Dry Your Hands

- after coughing or sneezing
- after grooming
- after using the toilet
- after handling used tissues
- after touching other surfaces used by infected or unknown people
- before and after eating

#### Use antiseptic hand wash

Wash hands thoroughly for minimum 10-20 seconds

Use a paper towel to turn off the tap and then to dry your hands well

Dispose of the paper towel in a lined and covered bin

#### Good Coughing and Sneezing Habits

Keep away from other people when coughing or sneezing.

Always use a tissue to cover your mouth and nose (Wellnomics has a supply of tissues if you run out)

Wash and dry your hands afterwards following the method detailed above

Go home if you are coughing or sneezing more than normal

#### Social Distancing

##### At work

- Do not come to work if you are unwell
- Avoid shaking hands etc
- Try to stay at least one metre away from other people
- Cancel any non-essential training sessions etc
- Avoid using another person's keyboard, telephone etc
- Avoid using another person's pens, staplers etc
- Avoid face-to-face meetings where possible. Use telephone, video-conferencing and email instead
- Where face-to-face meetings are necessary, keep them short, choose a large room and sit at least one metre away from each other
- Avoid any unnecessary travel
- Name your own coffee cup and do not share it with another person
- Bring your own lunch and eat it away from other people

#### Guidelines – Critical Events Page 13 of 1

- Use your own cutlery – do not share it
- Avoid congregation in the Staff room and common areas
- Magazines and newspapers will be removed from common areas to eliminate sharing. DO NOT lick your finger to turn pages in books in common use
- Use hygienic wipes before contacting a toilet seat

##### Outside work

- Avoid public transport. If you have to use it, try to avoid the “rush hour” – gain approval from your Manager for different start and finish times if you have to take public transport
- Avoid crowded places or large gatherings
- Where practical, avoid contact with sick people
- Avoid public toilet facilities. Where this is not possible, try not to touch anything after you have washed and dried your hands
- Avoid recreational activities where you could come into contact with infected persons
- Do not use magazines or toys in public places such as waiting rooms, at the checkout counter etc
- Avoid touching your face
- Always wash and dry your hands thoroughly after returning from public areas, shopping etc

#### Guidelines – Critical Events Page 14 of 18

## APPENDIX 5

### Screening Checklist & Influenza Recording Templates

As it is probable that the Wellnomics office will temporarily close and the “Work from Home Plan” will be

implemented immediately that there is a verified pandemic case in New Zealand, it is improbable that a case will be detected amongst Staff while they are at work. However, in this unlikely event, the following process will be followed:

#### Detection of Suspected Pandemic Influenza Cases

##### Process:

- a. The CMC receives a call from a person who suspects that they may have influenza
- b. The CMC should not visit this person if it can be avoided – manage the process over the telephone wherever possible
- c. The CMC will follow the flowchart below:
  - Ask the person if they have the following symptoms:
  - High fever (or feel feverish and hot)
  - Headache
  - Fatigue and weakness
  - Sore throat, cough, chest discomfort, difficulty in breathing
  - Muscle aches and pains
  - Been overseas recently
  - Been in contact with someone who has been diagnosed with influenza

Yes, two or more symptoms as

described above are present

No symptoms as described

above are present

Person should be considered as

possible case of influenza

Obtain details to complete Influenza Notification Form over the phone.

Obtain details to complete Contact List with details of those working within one metre or more or in an enclosed space for more than 60 minutes.

Advise that they should leave work immediately and contact their GP by telephone to advise that they have a suspected case of influenza.

Ask patient to ensure that you are updated with regard to their status ASAP.

Advise contacts that they have been in contact with a suspected case of influenza.

Ask contacts to go home and to stay there until they have received further advice.

Arrange for workstation cleanup

Unlikely to be influenza

• Reassure

• Advise to call again if concerned or visit their GP

Guidelines – Critical Events Page 15 of 18

Influenza Notification Form – Affected Person

Date: Name:

Date of Birth: Position:

Staff Member Y/N? If Visitor, note nationality:

Own Office Y/N? If No, note isolation site:

Home Address:

Home Phone: Mobile Phone:

Symptoms Noticed: Fever Headache Body Ache Dry Cough Fatigue

Cold Other (Details):

Time of fever onset: Time of isolation:

Travel History over the past 8 days: Countries:

Flights:

Where Referred: GP Name: GP Phone:

Details of Reporter:

Name: Position:

Home Phone: Mobile Phone:

Contact List

Persons whom affected person has interacted with since displaying symptoms. Include people who have had close physical (less than one metre) or confined airspace contact within 4 days of an infected person developing symptoms. These are likely to include family members, living companions, workmates and some recreational companions. If there are more than 15 contacts, please list on a separate piece of paper

Are there further Contacts on Attached Sheet/s? No Yes, (insert number) sheets

Guidelines – Critical Events Page 16 of 18

# APPENDIX 6

Public Area Notice:

## INFLUENZA NOTIFICATION

INFLUENZA IS A CONTAGIOUS DISEASE. THERE IS CURRENTLY AN INCREASE OF THE NUMBER OF PEOPLE IN NEW ZEALAND CONTRACTING INFLUENZA. IN ORDER TO REDUCE THE SPREAD OF INFLUENZA IN THE WORKPLACE, THE FOLLOWING IS REQUIRED OF EVERYBODY: DO NOT COME TO WORK IF YOU HAVE SOME OF THE FOLLOWING SYMPTOMS:

- Chills, Shivering and a Fever (temperature over 38o C)
- Onset of Muscle Aches and Pains
- Sore Throat
- Dry Cough
- Trouble Breathing
- Excessive Tiredness

When combined with some of the above (note that it is rare that these symptoms will be present in cases of influenza):

- Sneezing
- Stuffy or Runny Nose

If you have recently arrived or returned from overseas, please speak to a Crisis Management Co-ordinator.

If you start to feel ill at work, DO NOT leave your work area, telephone a Crisis Management Co-ordinator who will then follow the process detailed in the Critical Event Guideline.

## CRISIS MANAGEMENT CO-ORDINATORS:

Barbara Watson Ext.203

Wayne Owens Ext.222

Guidelines – Critical Events Page 17 of 18

Public Area Notice:

What is Influenza?

Influenza is a highly contagious viral disease of the respiratory tract.

What is the difference between Influenza and a Common Cold?

## SYMPTOM INFLUENZA COMMON COLD

Fever

Usual. Sudden onset, 38 – 40 degrees

Celsius, lasts 3 – 4 days

Rare

Headache Usual, can be severe Rare

Aches and Pains Usual, can be severe Rare

Fatigue & Weakness

Usual. Can last 2 – 3 weeks or more after the acute illness

Sometimes, but mild

Debilitating Fatigue Usual, early onset can be severe Rare

Nausea, Vomiting,

Diarrhoea

In children less than 5 years old Rare

Watery Eyes Rare Usual

Runny/Stuffy Nose Rare Usual

Sneezing Rare in early stages Usual

Sore Throat Usual Usual

Chest Discomfort Usual , can be severe

Sometimes, but mild to

moderate

Complications

Respiratory failure, can worsen a current condition, can be life threatening

Congestion, Earache

Fatalities Well recognized Not reported

Prevention

Influenza vaccine, frequent hand-washing, cover your cough

Frequent hand-washing, cover

your cough

How is Influenza Spread?

Influenza is spread from person to person via respiratory droplets generated in coughs and sneezes. It can also be spread when a person touches an item on which droplets are present and then touches their own eyes, mouth or nose (via which the virus enters the body) before washing their hands.

**THOROUGH AND REGULAR HAND WASHING IS THE MOST IMPORTANT THING THAT YOU CAN DO TO PROTECT YOURSELF**

The time from first exposure to when symptoms begin is one to four days. It is not certain whether people are infectious prior to developing symptoms, but they remain infectious for some days after. Children can remain infectious for up to 21 days, but this length of time is unusual in normally healthy adults.

Guidelines – Critical Events Page 18 of 18\

## APPENDIX 7

Critical Event Survival Kit Inventories

Personal Kit

The following is issued to each person working in the Wellnomics office. If any of the items are used, they should be immediately replaced or replenished out of the Master Kit.

The kit should always contain:

1. An unused surgical mask
2. A pair of unused latex gloves
3. A supply of anti-bacterial spray
4. A supply of alcohol evaporating hand cleanser

Master Kit

This is located next to the workbench in the safe.

When an item is removed from the kit, this must be recorded in the notebook attached to the lid so that supply levels can be easily identified and maintained.

The kit contains:

1. Rubbish bags
2. Tissues
3. Surgical masks
4. Latex gloves
5. Antibacterial spray
6. Alcohol evaporating hand cleanser
7. Paracetamol
8. Waterproof torch – spare batteries
9. Radio tuned to Civil Defence frequency – spare batteries

Note that supplies of paper towels are kept in the safe and toilet paper is kept in the cupboards in both the men's and women's toilets.

Food & Water Emergency Supply

This is located under the workbench in the safe. The supplies should ONLY be used in an emergency situation where no other source is available. It is intended to be a short term solution only. The kit mostly contains non-perishable food that doesn't require cooking (regardless of whether it would normally be eaten heated). The supply is not intended to be used as part of a personal evacuation kit although a small amount dehydrated stock has been included for this contingency.

The kit contains:

1. Canned Baked Beans
2. Canned Vegetables
3. Canned Fruit
4. Creamed Rice
5. Canned Fish
6. Canned Soup
7. High Energy Cereal
8. Fresh Noodles
9. Crackers
10. Water
11. Dehydrated Vegetables
12. Dried Meat
13. Dried Soup
14. 2 minute noodles
15. Milk Powder
16. Milo

- 17. Fruit & Nut Chocolate
- 18. Can Opener



# Monitoring - Internal - Guideline

Wellnomics has a range of monitoring services in place to monitor performance and availability of the [Wellnomics.com](https://www.wellnomics.com) website

## Website availability

An uptime monitor is used to monitor in real-time the availability of the site. Any downtime or unavailability is notified immediately to support staff 24/7.

## Wellnomics Status

The status of the Wellnomics website can be viewed at [status.wellnomics.com](https://status.wellnomics.com)



SUBSCRIBE TO UPDATES

All systems operational

Refreshed less than a minute ago

Wellnomics website

### Components

Wellnomics Website

Operational

### Monitors

Wellnomics Website

Operational

UPTIME 5 MINUTES 58 SECONDS

UPTIME OVER THE PAST 1 DAYS

100 % UPTIME

### Incident history

No Incidents reported.

# Website Terms & Conditions (not Hosting)

Generated by site

## 1. Terms

By accessing the website at <http://www.wellnomics.com>, you are agreeing to be bound by these terms of service, all applicable laws and regulations, and agree that you are responsible for compliance with any applicable local laws. If you do not agree with any of these terms, you are prohibited from using or accessing this site. The materials contained in this website are protected by applicable copyright and trademark law.

## 2. Use License

1. Permission is granted to temporarily download one copy of the materials (information or software) on Wellnomics' website for personal, non-commercial transitory viewing only. This is the grant of a license, not a transfer of title, and under this license you may not:
  - a. modify or copy the materials;
  - b. use the materials for any commercial purpose, or for any public display (commercial or non-commercial);
  - c. attempt to decompile or reverse engineer any software contained on Wellnomics' website;
  - d. remove any copyright or other proprietary notations from the materials; or
  - e. transfer the materials to another person or "mirror" the materials on any other server.
2. This license shall automatically terminate if you violate any of these restrictions and may be terminated by Wellnomics at any time. Upon terminating your viewing of these materials or upon the termination of this license, you must destroy any downloaded materials in your possession whether in electronic or printed format.

## 3. Disclaimer

1. The materials on Wellnomics' website are provided on an 'as is' basis. Wellnomics makes no warranties, expressed or implied, and hereby disclaims and negates all other warranties including, without limitation, implied warranties or conditions of merchantability, fitness for a particular purpose, or non-infringement of intellectual property or other violation of rights.
2. Further, Wellnomics does not warrant or make any representations concerning the accuracy, likely results, or reliability of the use of the materials on its website or otherwise relating to such materials or on any sites linked to this site.

## 4. Limitations

In no event shall Wellnomics or its suppliers be liable for any damages (including, without limitation, damages for loss of data or profit, or due to business interruption) arising out of the use or inability to use the materials on Wellnomics' website, even if Wellnomics or a Wellnomics authorized representative has been notified orally or in writing of the possibility of such damage. Because some jurisdictions do not allow limitations on implied warranties, or limitations of liability for consequential or incidental damages, these limitations may not apply to you.

## 5. Accuracy of materials

The materials appearing on Wellnomics' website could include technical, typographical, or photographic errors. Wellnomics does not warrant that any of the materials on its website are accurate, complete or current. Wellnomics may make changes to the materials contained on its website at any time without notice. However Wellnomics does not make any commitment to update the materials.

## 6. Links

Wellnomics has not reviewed all of the sites linked to its website and is not responsible for the contents of any such linked site. The inclusion of any link does not imply endorsement by Wellnomics of the site. Use of any such linked website is at the user's own risk.

## 7. Modifications

Wellnomics may revise these terms of service for its website at any time without notice. By using this website you are agreeing to be bound by the then current version of these terms of service.

## 8. Governing Law

These terms and conditions are governed by and construed in accordance with the laws of New Zealand and you irrevocably submit to the exclusive jurisdiction of the courts in that State or location.

# Passwords & Encryption - Employees & Contractors - Guidelines

**Review period:** Annual

## Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the network. This guideline provides best practices for creating secure passwords.

## Purpose

The purpose of this guidelines is to provide best practices for the created of strong passwords.

## Scope

This guideline applies to employees, contractors, consultants, temporary and other workers at Wellnomics, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

## Statement of Guidelines

All passwords should meet or exceed the following guidelines:

Strong passwords have the following characteristics:

- Contain at least 9 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !\$%^&\*()\_+|~-=: \ {} [] ; ' < > ? , /).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these examples as passwords!)

## Passphrases

Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access.

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was\*!\$ThisMorning!).

## Password Generation

The company password manager <https://wellnomicsdev.atlassian.net/wiki/spaces/AP/pages/1159594017/Password+Manager+-+BitWarden> should be used to generate and store all passwords in the appropriate organization folders.

# Policy Compliance

## Compliance Measurement

The Wellnomics management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Wellnomics Management team in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Related Standards, Policies and Processes

- [Acceptable Use - Employees & Contractors - Policy](#)
- [Passwords and Encryption - Employees & Contractors - Policy](#)

# Definitions and Terms

None.

# Revision History

Date of change	Responsible	Summary of change	Next revision date
6th December 2015	Wayne Owens, Principal Consultant	Separated out from the Password Policy and converted to new format.	December 2016
08 Dec 2016	Wayne Owens, Principal Consultant	Checked - no changes required	12 Dec 2017 <a href="#">Wayne Owens (Unlicensed)</a>
12 Jun 2017	Wayne Owens	Checked and reviewed	13 Jun 2018 <a href="#">Chris MacKay (Deactivated)</a>
05 Nov 2018	Chris MacKay, Support Consultant	Reviewed, no changes made	<ul style="list-style-type: none"><li>• 05 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li></ul>

20 May 2020	<a href="#">Chris MacKay (Deactivated)</a>	Reviewed, no changes made	<ul style="list-style-type: none"> <li>20 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
24 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"> <li>24 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
01 Dec 2020	Ian Bartram	Reviewed, changes to include reference to Password Manager generator	<ul style="list-style-type: none"> <li>01 Dec 2022 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	Ian Bartram	Reviewed, no changes required	<ul style="list-style-type: none"> <li>01 Feb 2024 <a href="#">Ian Bartram</a></li> </ul>

# Building Security - Documentation

There is a common key used to access the main door and keys to each office.

We also use the Arlo security system with two video cameras. This sets of an alarm and notifies several staff if there is a breach outside of normal hours via the arlo mobile app. The system is set to automatically alarm outside core business hours and during weekends. You can disable it temporarily with the app if you need to visit the office.

# Disaster Recovery and Business Continuity - Internal - Guide

## Objective

Outline business critical systems, disaster scenarios, a plan for restoration, and expected timeline.

## Contacts

Name; Title	DRT Role	Contact Option	Contact Info
Ian Bartram; Systems Administrator	Internal Systems restoration	Mobile Email	022-515-3633 <a href="mailto:ian.bartram@pm.me">ian.bartram@pm.me</a> , <a href="mailto:ian.bartram@wellnomics.com">ian.bartram@wellnomics.com</a>
Feng Zhou; Software Engineer	Internal systems restoration backup	Email	

## Business Critical Systems

The systems listed below are considered business critical;

- Main server
- Networking equipment; Switch, Firewall, Router, Access Points
- Critical VMs
  - VM - DC01 (Domain Controller 1)
  - VM - Delorean (Backup VM)
  - VM - Elysium (Dev WRM build)
  - VM - Falcon (Main QA)
  - VM - HallTest ( QA Second)
  - VM - Nautilus (Proxy/docker)
  - VM - Selma (MAC client Build)
  - VM - Unify (Unifi controller, AAD Sync)
- Workstations

## Scenarios

1. **Main office is inaccessible;** Due to natural disaster or emergency events (fire/flooding) the office is no longer safely accessible to Staff.
2. **Main office is accessible with loss of main server;** Due to hardware or software failure on the main server it is no longer functioning.
3. **Loss of Critical VM;** A VM has become corrupted or lost entirely.

### Scenario - 1 Loss of main office

System/ Task	Threat	Resolution	Timeline	DRT Contact
Main server	Fire, Flood, Earthquake	Restore VM's on Temporary employee workstations	1-2 Days	Ian & Feng
Workstations	Fire, Flood, Earthquake	Azure Windows VM workstations	1 Day	Ian



## Scenario - 2 Loss of Main server

System/ Task	Threat	Resolution	Timeline	DRT Contact
Host Server	Hardware/software failure, Fire, Flood,	Restore DC + backup VM on temporary desktop	1 Day	Ian & Feng
Critical VMs	Loss of host server	Once backup VM is online, restore critical VMs only	2 Days	Ian & Feng
Non Critical VMs	Loss of host server	Restore as needed	2 weeks	Ian & Feng
Diagnose failure			2 Days	Ian & Feng
Repair plan			2 Days	Ian & Feng

## Scenario - 3 Loss of Critical VM

System/ Task	Threat	Resolution	Timeline	DRT Contact
Critical VM	Data corruption, malice	Restore from back up	1 Day	Ian & Feng

## Related

- [Critical Events - Guidelines](#)
- [Business Continuity \(& Disaster Recovery Plan\) - Guideline](#)

Date of Change	Responsible	Summary of Change	Next Revision date
06 Jun 2022	Ian Bartram	New document established	<ul style="list-style-type: none"> <li>• 05 Dec 2022 <a href="#">Ian Bartram</a></li> </ul>
26 Jan 2023	Ian Bartram	Separated some information into guides.	<ul style="list-style-type: none"> <li>• 29 Feb 2024 <a href="#">Ian Bartram</a></li> </ul>

# Security & Privacy Training - Employees & Contractors - Guideline

Document	Description	Audience	Attachment	Last updated
Data and Systems Security	General requirements for data security and privacy	All staff	Wellnomics Staff Present...	Mar 2023
Data and Systems Security	General requirements for data security and privacy	System Admins	Wellnomics Staff Present...	Mar 2023
OWASP Best Practice	Best practice guidelines for software developers to ensure security in applications following OWASP guidelines	Development Team Members	Web_Application_Developm...	2018

# Employee Agreement & Contract - Example

**Review period:** Annual

## Main employment contract

Attached is the standard employment agreement that is signed by all Wellnomics staff when joining the company.

For clauses covering Information Security and Privacy refer specifically to

- Sections 6.6, 6.7 - Specific employee obligations relating to privacy and information security
- Section 23.4 - Care of documents

Wellnomics Standard Empl...

## Conditions of Employment

These are part of the signed employment agreement. The company and staff are required to also comply with the New Zealand Privacy Act 1993 which is quite specific with regard to confidentiality and privacy.

Refer in attached document to:

- Section 2 - Confidentiality
- Section 7 - Privacy
- New Zealand Privacy Act 1993

## Deed of Confidentiality

This is also part of the standard signed Wellnomics Employee Agreement.

Wellnomics Employment Ag...

## Revision History

Date of change/review	Responsible	Summary of change	Next Revision
-----------------------	-------------	-------------------	---------------

September 2019	Wayne Owens, Principal Consultant	Updated and converted to new format.	10 Sep 2020 <a href="#">Chris MacKay (Deactivated)</a>
16 Sep 2020	<a href="#">Wayne Owens</a>	Reviewed - no changes required	14 Sep 2021 <a href="#">Ian Bartram</a>
04 Oct 2021	Wayne Owens	None - review only	18 Oct 2022 <a href="#">Wayne Owens</a>

# Employee Position Description - Example

**Review period:** Annual

## Position Description - Wellnomics Consultant - Support and Implementation

### Purpose

To take the lead on reactive customer support and to provide exemplary customer support services to clients, partners and Wellnomics staff, maximising the satisfaction of those parties with the service provided. To undertake software implementation projects at a wide range of clients, both domestically and internationally. To act as a first point of contact for nominated customers and to execute agreed customer engagement plans.

Reporting To: Principal Consultant

Reporting Staff: None

External Contacts: Customers, Technical & Health & Safety Staff, Prospects, Resellers, Subject Experts

Internal Contacts: All staff

### Qualifications & Experience

- Relevant Tertiary Qualification preferred
- Experience in providing IT-related support services
- History of successful client relationships and achieving desired outcomes
- Experience in delivering remote customer service – i.e. by telephone, email, webex (or equivalent) etc.
- Demonstrated track record of successful implementation and support of software applications and solutions
- Experience with Change Management, Risk Management and Prioritisation and Impact Analysis
- Experience with Needs Analysis in commercial environments and a broad range of business processes
- Experience of a variety of corporate environments, ideally at international level
- Experienced in dealing with the demands of a high pressure deadline-oriented environment
- Advanced computer literacy and good knowledge of Microsoft Office applications and operating systems
- Experience with VMware, AuthorIT advantageous
  - Quality focussed and achievement orientated
  - Organised, structured and logical approach
  - Collaborative working style with proven relationship building skills at all levels
  - Good memory for product features/details/functionality
    - Ability to work with a wide variety of people
    - Ability to work outside normal NZ office hours, as required

### Person Specifications

- Customer Service sensibility
- Excellent written & oral communication skills
- Analysis and lateral thinking ability
- Technical translation ability
- Good Time Management
- Attention to detail & documentation

- Ability to quickly grasp concepts and requirements in a variety of environments
- Honesty & Integrity
- Initiative and the ability to respond to unexpected issues
- Clean Drivers Licence
- Valid passport and no travel restrictions

<b>Key Accountabilities</b>	<b>Expected Outcomes</b>
<b>Implementation and Project Management</b> <span style="float: right;"><b>“Build Lasting Customer Relationships”</b></span>	
Provide clients with appropriate product and process documentation and information and implementation and project management support	<ul style="list-style-type: none"> <li>• Clients are aware of and have access to product documentation (e.g. technical documentation, installation guides, product manuals, templates, etc.)</li> <li>• Take the lead, where requested, on customer implementation projects. Provide clear advice on the implementation process having regard to agreed internal processes and methodologies, approved documentation and specific customer requirements</li> <li>• As required, carry out on-site visits to customers (which may involve domestic and/or international travel)</li> </ul>
Facilitate and ensure that clients are provided with guidance on the best way to pilot or implement Wellnomics products	<ul style="list-style-type: none"> <li>• A standard process for ensuring a successful implementation is understood and adopted.</li> <li>• Clients are provided with standard project outlines and recommended implementation plans, including recommended configuration settings and options (ideally sourced from a standard list of options)</li> <li>• Clients are encouraged to follow a standard implementation process that guarantees success</li> <li>• Clients are provided with advice on the best ways to adjust their Health and Safety processes to maximise the use of the Wellnomics product.</li> <li>• Clients are provided with assistance and advice on the Change Management required to implement Wellnomics products successfully.</li> </ul>
<b>Communication Relationships</b> <span style="float: right;"><b>“Value People”, “Act with Integrity” &amp; “Build Lasting Customer Relationships”</b></span>	
Champion open channels of communication throughout the company	<ul style="list-style-type: none"> <li>• Communication is proactive and clear minimising any surprises for both the Solution Support Team and the business as a whole</li> <li>• Ensure early reporting of likely deadline overruns</li> <li>• Immediately advise relevant staff of any significant issues or hold-ups that may affect implementation success, and/or need to be discussed with the client - including any which may have been notified to the Support Team directly from the client</li> <li>• Proactively update the Implementation Director on any relevant issues</li> </ul>

<b>Key Accountabilities</b>	<b>Expected Outcomes</b>
	<ul style="list-style-type: none"><li>Facilitate open and honest communication at all levels</li></ul>
Participate in client communication activities as required	<ul style="list-style-type: none"><li>Liaise with Sales Team, support staff and other relevant Wellnomics staff and contractors involved in implementations to ensure excellent and consistent communication to and from clients.</li><li>Where required to accommodate the time zones of international clients be prepared to host and/or participate in required teleconferences/meetings etc.</li></ul>
<b>Support Desk Operations</b> <span style="float: right;"><b>“Value People” &amp; “Build Lasting Customer Relationships”</b></span>	
Answer all calls and emails to the Support Desk with excellent customer service sensitivity - promptly and professionally in an appropriate manner	<b>KPI, Calls Are Responded To Within 1 Working Day</b> <ul style="list-style-type: none"><li>The initial contact experience immediately introduces the client or other caller to superior service quality</li><li>All support enquiries are completed to the KPI or delegated to another person if off site<ul style="list-style-type: none"><li>Any calls or emails for non-support matters are forwarded to other appropriate staff</li><li>Listen to problems/issues to fully understand the customer’s question/need</li></ul></li><li>Provide advice and, where possible, extra value by offering complimentary services.<ul style="list-style-type: none"><li>Resolve Incidents quickly and efficiently</li><li>Specifically foster positive relationships with all clients</li><li>Escalate issues appropriately to ensure timely resolution, properly recording the escalation so that the issue is not lost in transition</li><li>Exceed client expectations wherever possible</li></ul></li></ul>
Develop excellent relationships with customer site management and technical staff	<ul style="list-style-type: none"><li>Maintain an excellent rapport with customers &amp; channel partners</li><li>Translate technical information into plain English – displaying excellent facilitation and communication skills<ul style="list-style-type: none"><li>Customer feedback is positive</li><li>No justifiable complaints are received</li><li>Ensure maximum use of Wellnomics products is achieved across the customer’s organization, upgraded to the latest build and maintenance renewed.</li></ul></li></ul>
Manage all ‘bug’ and/or issue notifications from clients and channel partners	<ul style="list-style-type: none"><li>Log ‘bug’ reports with test department and keep clients informed of progress/resolution<ul style="list-style-type: none"><li>Report any trends in enquiries that could indicate a potential or ongoing problem</li></ul></li></ul>

<b>Key Accountabilities</b>	<b>Expected Outcomes</b>
Provide regular and accurate reporting from approved software as requested by Implementation Director	Including, but not limited to: <ul style="list-style-type: none"> <li>• Case statistics</li> <li>• Escalation issues</li> <li>• Commonality and trending</li> <li>• Open/Closed jobs</li> </ul>
<b>Documentation</b> <b>“Think With Rigour”</b>	
Maintain and update Knowledge Base	<ul style="list-style-type: none"> <li>• Refer to the Knowledge Base initially for any issues which are unfamiliar and utilise common responses where practicable</li> <li>• Ensure that identified common solutions to common problems are properly recorded for easy reference when required</li> </ul>
Assist in the development and maintenance of external documentation, ensuring it is relevant, in context with the product objectives and available when required  Review documentation and product text to ensure ongoing accuracy and consistency	<ul style="list-style-type: none"> <li>• Relevant documentation includes (but is not limited to):</li> <li>• Pilot &amp; presales support material</li> <li>• Product Implementation &amp; Training documentation &amp; presentations               <ul style="list-style-type: none"> <li>• All documentation and written material is relevant and up to date</li> <li>• Requirements for timely product releases are met. No release is delayed due to late documentation</li> <li>• Documentation is appropriate to its audience and provides first class technical translation when required</li> <li>• All material reflects current company branding and marketing protocols</li> </ul> </li> <li>• Relevant staff are alerted to any identified inaccuracies or inconsistencies in terminology or process</li> <li>• No inaccurate or outdated information, recommendation or instruction remains within the product or relevant documentation</li> </ul>
<b>Pre and Post Sales Services</b> <b>“Value People” &amp; “Build Lasting Customer Relationships”</b>	
Products are thoroughly tested from a User and Implementation perspective prior to being released	<b>KPI, &gt; 90% of all Wellnomics® Risk Management and WorkPace installation issues are identified in-house before client site deployment</b> <ul style="list-style-type: none"> <li>• Create and maintain a library of different virtual server platforms used to simulate a variety of implementation and procedural scenarios</li> <li>• Utilise a variety of virtual scenarios to ensure a wide range of testing is undertaken</li> <li>• Testing is completed in a timely manner in liaison with the Development /Test Teams</li> </ul>



<b>Key Accountabilities</b>	<b>Expected Outcomes</b>
	<ul style="list-style-type: none"> <li>• Technical documentation is cross-checked against tested scenarios and is proof-read to ensure accuracy and completeness</li> </ul>
Provide technical expertise to satisfy all prospective customer requirements	<ul style="list-style-type: none"> <li>• Enhance the technical expertise reputation of Wellnomics Ltd</li> <li>• Promote maximum use of Wellnomics' products across the customer's organization <ul style="list-style-type: none"> <li>• There are no outstanding support requests whereby the client cannot move forward.</li> </ul> </li> </ul>
Prepare, develop and implement training solutions and customer specific training presentations.	<ul style="list-style-type: none"> <li>• Presentations are accurate, visually stimulating and completed on time <ul style="list-style-type: none"> <li>• Presentations are carried out professionally and always with a customer focus</li> </ul> </li> </ul>
Contribute to and participate in customer site visits as appropriate, ensuring a high level of service and professionalism is maintained at all times	<ul style="list-style-type: none"> <li>• Provide client support history and technical background to the Salesteam prior to any customer visits</li> <li>• Complete one-off reports on specific sites prior to sales visits or when an issue is raised</li> <li>• In liaison with the sales team and the Implementation Director, undertake visits to client sites to assist with the provision of implementation and/or training services and the enhance customer relationships.</li> </ul>
<b>Other</b> <span style="float: right;"><b>“Go For Balance” &amp; “Think with Rigour”</b></span>	
Update the CRM / issue tracking applications etc. – logging technical issues, times, resolutions, clearances and escalations etc.	<ul style="list-style-type: none"> <li>• Customer enquiries are tracked, actioned promptly and passed on to the appropriate person immediately <ul style="list-style-type: none"> <li>• Maintain an up-to-date, easily accessible, accurate database at all times using the corporately approved software tools</li> </ul> </li> </ul>
Carry out recommended regular routine administrative tasks.	<ul style="list-style-type: none"> <li>• All administration completed on time and accurately.</li> <li>• Reports are run as required – including regular weekly or monthly activity reports.</li> </ul>
Manage all activities within budget guidelines	<ul style="list-style-type: none"> <li>• Comply with Wellnomics Financial Authority and Purchasing Guidelines</li> </ul>
Recommendation and Suggestions	<ul style="list-style-type: none"> <li>• Advise on significant trends, problems, issues and opportunities as soon as they become known</li> <li>• Forward product improvement ideas to the development issue tracking system</li> </ul>

<b>Key Accountabilities</b>	<b>Expected Outcomes</b>
	<ul style="list-style-type: none"> <li>Make recommendations where you have identified potential improvements in efficiency or any other benefit to Wellnomics</li> </ul>
Ensure Wellnomics' Intellectual Property (IP) disclosure is in line with Wellnomics policy	<ul style="list-style-type: none"> <li>Protect all Wellnomics IP</li> <li>Immediately report any infringement or loss of IP to management</li> </ul>
Ensure that all customer data is kept secure at all time	<ul style="list-style-type: none"> <li>Adherence to all Wellnomics policies and processes relating to data security, protection and privacy and in particular: - <ul style="list-style-type: none"> <li>Keeping all usernames passwords secure and not sharing with others</li> <li>Not using generic accounts</li> <li>Changing all relevant password on a regular basis as prescribed by relevant policies</li> <li>Ensuring that all virus and malware utilities are updated daily</li> <li>Ensuring that any data not kept within the Wellnomics domain is encrypted.</li> </ul> </li> </ul>
From time to time other duties not listed in this Position Description may be required to be performed as determined by business needs.	<ul style="list-style-type: none"> <li>All projects are completed with enthusiasm, accurately and on time in consultation with your Manager.</li> </ul>

## Revision History

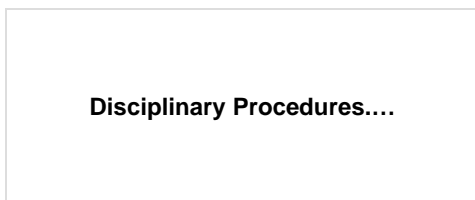
<b>Date of change</b>	<b>Responsible</b>	<b>Summary of change</b>	<b>Next Revision</b>
September 2019	Wayne Owens, Principal Consultant	Updated and converted to new format.	10 Sep 2020 <a href="#">Chris MacKay (Deactivated)</a>
08 Sep 2020	<a href="#">Wayne Owens</a>	Reviewed - no changes required	15 Sep 2021 <a href="#">Ian Bartram</a>
14 Sep 2021	Wayne Owens	Reviewed - no changes required	14 Sep 2022

# Disciplinary Procedures - Employees & Contractors - Guidelines

**Review Period:** Annual

The Disciplinary Procedures Guideline below is one of Wellnomics official guidelines and is included as an addendum to each employees signed Employment Agreement.

Section 10b specifically states that a breach of **Wellnomics Information Security and Privacy Policies and Procedures** may constitute Serious misconduct.



## Revision History

Date of change	Responsible	Summary of change	Next Revision
September 2019	Wayne Owens, Principal Consultant	Updated and converted to new format.	10 Sep 2020 <a href="#">Chris MacKay (Deactivated)</a>
10 Sep 2020	<a href="#">Wayne Owens</a>	Reviewed - no changes required	30 Sep 2021 <a href="#">Ian Bartram</a>
12 Oct 2021	Ian Bartram	No changes - reflects current policy	12 Oct 2022 <a href="#">Ian Bartram</a>

# INTERNAL ONLY

The below documentation exists, but is not provided externally due to containing potentially confidential information.

- [Business Continuity \(& Disaster Recovery Plan\) - Guideline](#)
- [Backup of Wellnomics Company Data - Guideline](#)

# Business Continuity (& Disaster Recovery Plan) - Guideline

Also referred to as **Business Impact Assessment (BIA)**

**Review period:** Annual

## Overview

Disasters happen rarely however disruptions that cause interruptions to normal business can take a number of forms and can happen more frequently. Having a contingency plan in the event of a disaster or business disruption gives Wellnomics Ltd a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning and business disruption efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered.

## Purpose

To prepare for disruption to IT and related services to ensure that Wellnomics as a business can continue to operate as optimally as possible in the event of unforeseen or planned critical events. All business critical functions should be restored as soon as possible after any disruption with a further aim to have all desirable functionality (80% or more) restored within one week.

## Key Points

Disruption to Wellnomics business can be categorised in four different contexts:

1. Failure of individual or limited items of equipment - e.g. equipment breakdown, small scale power disruption
2. Communication services failure – e.g. telephone or internet disruption
3. Large scale physical damage to property and/or equipment – e.g. fire, earthquake
4. Staff availability limitations – e.g. pandemic, disaster affecting transportation

The scale, length of time and likelihood of particular disruptive events are also important factors in determining where and how much effort should be made – both in proactive preparation and reactive recovery.

Business Continuity priorities have been based on the critical business processes which are defined as:

## Administration

Accounts Payable & Receivable & Payroll

- Xero (accounts)
- Smartpayroll
- Internet access
- E-mail (ideal, although not essential)

Sales Administration – Website & E-mail

- Microsoft CRM
- Hubspot
- Internet access
- E-mail (ideal, although not essential)
- Ability to print documents

## IT / Product Development

- Back up data – retrievable in Critical Event situation.
- Continue Software Development & Key Deliveries

## Sales & Support

- Advising Customers & Resellers of 'Business Status' and maintain appropriate e-mail / phone contact
- Continued access to Wellnomics hosted servers - server hosted by Microsoft Azure in London, Sydney and Chicago\*

## Procedures

### Procedure 1 – Preventative and Contingency Precautions

- All items in the server room which are not connected to the UPS are fitted with a power surge protector plug
- Data is backed up daily on an incremental basis to an external USB drive which is swapped out three times a week and stored offsite.
- Backup discs of all virtual machines are kept offsite and are cycled through both short and long term rotations
- Test restorations of the data backed up online are undertaken quarterly to ensure the integrity and completeness of the back-ups
- A spare desktop (with development level specifications) and a spare laptop are pre-configured ready for deployment in the event of equipment failure for a single employee
- Regular maintenance which may involve downtime is scheduled company-wide to ensure that software and application patches are regularly implemented.
- All servers are virtualised, allowing easier transition to alternative hardware. Snapshots of these virtual servers are saved to external hard discs for immediate recovery elsewhere.
- All travelling staff have been issued with USB memory drives to load critical files onto prior to their departure on any trip.

### Procedure 2 – Short Term Disruptions (less than five business days)

#### Equipment Failure (non-Critical Event)

##### Items requiring immediate replacement

###### Desktop Computer or Laptop for Individual Employee

The spare equipment is deployed.

###### Monitor for Individual Employee

Sourced as required prior to permanent replacement (maybe from an employee who can spare a dual monitor, or maybe purchased)

##### Items requiring immediate recovery

###### Virtual Host

The virtualised server is moved to alternative on-site hardware whilst the disruption cause is investigated and fixed.

###### Router

Router is replaced with alternative on-site hardware, whilst sourcing a replacement.

As part of future risk mitigation strategies, a dual-communication configuration device may be implemented.

#### Switch

Connections on other switches are shuffled to enable continuation of critical services.

Faulty switch is replaced or serviced by our current service provider (refer **Appendix 1**). Note that replacement is the probable option due to the comparative cost of service and repair.

#### Laptop

If this disruption occurs on-site, the spare laptop or desktop is deployed whilst the disruption cause is investigated and fixed.

For travellers, a replacement laptop with Windows pre-installed should be purchased and the IT Remote Working procedure should be followed to connect and work remotely on the Wellnomics network.

Additionally, prior to travelling, travellers should save all potentially required documents to a USB memory drive for easy access if the original files become unavailable. These drives should be kept separate from the laptop and protected with a secure password that complies with our current password policy.

## Staff Unavailability

### Planned emergency

Implement the Work from Home Plan (refer to Working from Home Guideline) in conjunction with Critical Event procedures (refer [Critical Event Guideline](#))

### Unplanned emergency

Refer [Critical Events - Guidelines](#)

## Related Documents

- [Critical Events - Guidelines](#)
- [Disaster Recovery and Business Continuity - Internal- Guide](#)
- [Remote Access Policy](#)

## Management Approval

Originally approved by management on 6th December 2013. Subject to annual management approval on an annual basis.

## Revision/Approval History

Date of change	Responsible/Updated by	Summary of change	Date of Next Revision
6th December 2013	Wayne Owens, Principal Consultant	Updated and converted to new format.	December 2014
12th December 2014	Wayne Owens, Principal Consultant	Annual management re-approval	December 2015

9th January 2015	Wayne Owens, Principal Consultant	Updated to make reference to new policies that have been created and auctioned	January 2016
10th December 2015	Wayne Owens, Principal Consultant	Annual management re-approval	December 2016
3rd February 2016	Wayne Owens, Principal Consultant	Updated and Linked new policies and procedures under Section 5	February 2017
November 2016	Wayne Owens, Principal Consultant	Updated and linked new policies under Section 5, removed proposed ones from Section 6	
6th December 2016	Wayne Owens, Principal Consultant	Annual management re-approval	December 2017
12 December 2017	Wayne Owens, Principal Consultant	Created new document <a href="#">User Management - Employees &amp; Contractors - Policy</a> and transferred authorization matrix from this document to the new document.  Annual management re-approval given by KT, CEO	12 Dec 2018  <a href="#">Wayne Owens (Unlicensed)</a> Chris Mackay
14 Jun 2017	Wayne Owens	Amended contact lists	19 Dec 2017  <a href="#">Wayne Owens (Unlicensed)</a>
12 Dec 2017	Wayne Owens	Checked and up to date	18 Jun 2018  <a href="#">Chris MacKay (Deactivated)</a>
21 Nov 2018	Chris MacKay	Reviewed, no changes made	<ul style="list-style-type: none"> <li>• 21 Nov 2019 <a href="#">Chris MacKay (Deactivated)</a></li> <li>•</li> </ul>
05 Jun 2020	Wayne Owens	Reviewed and updated minor contact details. No material change in policy	07 Jun 2021
09 Oct 2020	Kevin Taylor	Updated supplier list and correct systems for accounts/payroll (Xero instead of SAP)	<ul style="list-style-type: none"> <li>• 01 Oct 2021 <a href="#">Angeli Arino (Deactivated)</a></li> </ul>
30 Oct 2020	Angeli Arino	Updated supplier details for telephony (VoIPline instead of Digital Island)	30 Oct 2021 <a href="#">Ian Bartram</a>
14 Jan 2022	Corinne Wright	Revised for hosted servers info	12 Jan 2023 <a href="#">Corinne</a>

#### Notifications Record - Staff awareness of procedures

- 08 Jan 2014 - creation of this page notified to all staff
- 17 Dec 2014 - Reminder note to all staff regarding required knowledge of this document
- 15 Dec 2015 - Reminder note to all staff regarding required knowledge of this document
- 07 Jun 2016 - Checked and updated

For all future notifications and training of staff - see [Staff Training Record - Data and Systems Security and Privacy](#)



# Backup of Wellnomics Company Data - Guideline

**Review Period:** Annual

This document outlines the steps taken to backup the data used and required by Wellnomics Ltd as a company that creates and sells software.

The data repositories and databases are many and varied however they can be split into 2 main categories:-






- those held internally within Wellnomics own network and firewall
- those held externally in cloud or externally hosted systems

Internally hosted and stored systems are mounted on 1 of 3 physical servers (Network names "Omega", "Holly" and "Serenity", respectively) . Within these physical servers are mounted a number of "virtual" server or "VMs" that represent each system.

## General Description of Backup Processes

Other than the general operating system, nothing exists on either of the 2 physical servers other than systems represented in the form of virtual systems of VMs. To manage and support a "mean and lean" and efficient backup processes decisions have been made to determine what it is necessary to backup and what it is not necessary to back up.

At this time (see last revision date below) the following systems were deemed to be essential to be able to restore in the event of failure (as represented by their VM name and description) :-

Server Name	Description	Action	Offsite Backup Required?	Onsite Backup	Used by
vm-Atlantis	Test Server	Backup required		yes - weekly updates	Dev - Server team
vm-basestar	Windows Admin centre	Backup required		yes - weekly updates	IT/Support
vm-Buran	Linux build server	Backup required		yes - weekly updates	Dev - Client
vm-calculator	Calculator Automation	Backup required		yes - weekly updates	QA
vm-DC01	Primary Domain Server	Backup required		yes - weekly updates	IT/Support
vm-DC02	Secondary Domain Server	Backup required		yes - weekly updates	IT/Support
vm-delorean	Backup server	Backup required		yes - weekly updates	IT/Support
vm-discovery	Firmware build server	Backup required		yes - weekly updates	Dev - Client
vm-elysium	Current Build Server for Server	Backup required		yes - weekly updates	Dev - Server Team
vm-Falcon	Test Server	Backup required		yes - weekly updates	QA

vm-Glossary	Internal glossary IIS host	No Backup required		yes - weekly updates	IT/Support
vm-halltest	Test Server	Backup required	✓	yes - weekly updates	Dev - Server Team
vm-nautilus	Portainer Host	Backup required	✓	yes - weekly updates	IT/Support
vm-newindia	Test server	No Backup required		yes - weekly updates	QA
vm-odyssey	wc Doxygen host	Backup required		yes - weekly updates	Dev - Client
vm-regression	Test Server	Backup required		yes - weekly updates	QA
vm-release	Mainly to deploy WRM RCs	Backup required		yes - weekly updates	QA
vm-securityTest	NetSparker	Backup required		yes - weekly updates	QA
vm-selma	SVN Server used for WP Mac and WP QT	Backup required	✓	yes - weekly updates	Dev - Client
vm-timezone	WRM timezone tests	Backup required		yes - weekly updates	QA
vm-unify	AAD Connect + Unify Controller	Backup required	✓	yes - weekly updates	IT/Support
vm-voyager	manufacture tool build server	Backup required		yes - weekly updates	Dev - Client
vm-Welltest	Test Server	Backup required		yes - weekly updates	QA

## Internal Systems

Backups are made to an Azure Back up storage account using the Azure backup agent. These are full images of all VMs running on the main server NORMANDY. These backups are copied redundantly to local NAS devices weekly ensuring we have on and offsite back ups. They can be restored on any machine running Hyper-V should there be a critical hardware failure on the host server. This transmission uses a secure https/TLS1.2 connection.

## Hosted Systems

All backups are automatically taken as part of the Service Level Agreement with Microsoft and stored in an encrypted form securely within the Microsoft Azure server environment protected by a Cisco firewall. If any system has to be restored from backup, the backup is accessed and re-installed without leaving the Azure environment, however during transmission within that environment it is transmitted in an encrypted form. (this is part of the service level agreement with Microsoft for Azure)

## Revision History

Date of change	Responsible	Summary of change	Next revision date
16 Oct 2016	Wayne Owens, Principal Consultant	Updated and additional screen shots added for illustration	04 Oct 2017 <a href="#">Wayne Owens (Unlicensed)</a>

08 Feb 2018	Kevin Taylor, CEO	Added information on hosted servers	08 Feb 2019 <a href="#">Chris MacKay (Deactivated)</a>
19 Mar 2019	<a href="#">Chris MacKay (Deactivated)</a>	Added information about Serenity Physical Server	<ul style="list-style-type: none"> <li>19 Mar 2020 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
20 May 2020	<a href="#">Chris MacKay (Deactivated)</a>	Reviewed. No changes required	<ul style="list-style-type: none"> <li>24 May 2021 <a href="#">Chris MacKay (Deactivated)</a></li> </ul>
24 Aug 2020	Angeli Arino	Converted to a new page	<ul style="list-style-type: none"> <li>24 Aug 2021 <a href="#">Ian Bartram</a></li> </ul>
24 Sep 2021	Ian Bartram	reviewed no changes required	<ul style="list-style-type: none"> <li>29 Jul 2022 <a href="#">Ian Bartram</a></li> </ul>
24 Jan 2022	Ian Bartram	Updated to reflect current servers and backup standards	<ul style="list-style-type: none"> <li>24 Jan 2024 <a href="#">Ian Bartram</a></li> </ul>

# RESOURCES & TEMPLATES - Due Diligence Checklists, Templates and Training Resources

Pages under this are templates and forms to be used to follow specific policies and procedures. Copies of completed forms should be stored in [COMPLETED RECORDS - INTERNAL - Due Diligence Checklists and Templates](#) to provide evidence of compliance.

- [PRODUCT & SOFTWARE DEVELOPMENT - Templates & Resources](#)
- [DEPLOYMENT & HOSTING - Templates & Resources](#)
- [INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Templates & Resources](#)

# PRODUCT & SOFTWARE DEVELOPMENT

## - Templates & Resources

- [Third Party Components Review - Template](#)
- [App Security Testing Record - Template](#)
- [Penetration Testing Record - Template](#)
- [Dynamic Analysis Security Testing \(DAST\) Record - Template](#)

# Third Party Components Review - Template

Enter (or copy existing list) of 3rd party components used in product being reviewed

Last updated	
Product version	

Refer to [Third Party Components - Policy](#) and [Third Party Components - App - Documentation](#)

## Guide to updating form

Review list to ensure all components used in product are listed. Add any new components not in the list and delete any that product no longer uses.

**Security Importance:** Make a call on how important the component is from a security perspective - High, Medium or None.

**Reason:** Provide a short explanation for why the component is considered a High, Medium or None.

**Latest version:** Enter the latest version available if known, and then indicate how new this is compared to the the version being used in the product is e.g. are we just 1 or multiple versions behind, are we 2 months or 2 years behind the latest version . Some components may be old for example, but there may be no recent updates. What is important is how far out of date the component is compared to the latest versions available.

**Up to Date Security Judgement:** Make a judgement call on whether the component version being used is current enough from a security point of view. If we are deliberately using older versions of the component, then explain why this is (briefly) and also explain why this isn't considered a security issue, or if it is an issue, note the action we should take.

**Pass/Fail:** Indicate if its a pass or fail. If its a fail, meaning the component needs to be updated, add a Jira item number to track need to update component.

Component	Security Importance	Reason?	Version used	Latest version	Up to Date Security Judgement	Pass / Fail	Copyright	Licence	Links
	High								
	Medium								
	None								

# App Security Testing Record - Template

Testing below is based upon verifying we meet [Product Security and Best Practice - App - Guidelines](#) .

<b>Security Test Risk Assessment</b>	
<b>Date</b>	
<b>Risk Assessment completed by</b>	
<b>Product name and version</b>	
<b>Risk Assessment Details: (provide risk assessment details to support security test decision)</b>	
<b>Security test required</b>	<b>YES / NO</b>
<b>Signed off by</b>	

<b>Security test Completion Details (if test needs to be completed)</b>	
<b>Date</b>	
<b>Tester</b>	
<b>Product name and version</b>	
<b>Network/Environment</b>	

Test Type	Tests Executed	Result	Evidence	Description of Issues found / Jira link (if any)	Risk Assessment	Action Required
Certificate validation – Trust Chain	Issue a Non Trusted SSL certificate <b>before</b> WPC first contacts the server, WPC refuses to connect with server and communication log shows Trust Chain validation error.					
Certificate validation – Trust Chain	Issue a Non Trusted SSL certificate <b>after</b> WPC first contacts the server, WPC refuses to sync with server and communication log shows Trust Chain validation error.					
Certificate validation – Domain name	Issue a Trusted SSL certificate with mis-matched domain name <b>before</b> WPC first contacts the server, WPC refuses to connect with server and communication log displays error.					
Certificate validation – Domain name	Issue a Trusted SSL certificate with mis-matched domain name <b>after</b> WPC first contacts the server, WPC refuses to sync with server and communication log displays error.					
Security protocol is TLS 1.0 or above	WPC is able to communication with server successfully if server communication using TLS 1.2 or above.					

Security protocol is TLS 1.0 or above	WPC is able to communication with server successfully if server communication using TLS 1.1 or above.					
Security protocol is TLS 1.0 or above	WPC is able to communication with server successfully if server communication using TLS 1.0 or above.					

For guidance on assessing risk level refer to [Wellnomics Product Security Evaluation Matrix](#)

<b>Risk Assessment</b>	<b>Action Required</b>
<b>High risk</b>	Release fix required and consideration for patch if existing versions have this vulnerability
<b>Medium risk</b>	A vulnerability that needs fixing in the next version, no need to patch existing versions
<b>Low risk</b>	A theoretical or technical security issue (e.g. out of date 3rd party libraries) but not of sufficient risk to require a future fix

<b>Signed off by</b>	
<b>Position</b>	
<b>Date</b>	



# Penetration Testing Record - Template

Testing below is based upon verifying we meet [Wellnomics Product Security Guidelines and Best Practice - Server](#) .

Copy this page and create as a child page under [Completed Records for Product Security and Penetration Testing](#) . Complete the page there and save as a due diligence record.

<b>Penetration or Security Risk Assessment</b>	
Date	
Risk Assessment completed by	
Product name and version	
Risk Assessment Details: <i>(provide risk assessment details to support penetration test decision)</i>	
Penetration test required	<b>YES / NO</b>
Signed off by	_____
	Date: _____

<b>Penetration or Security Test Completion Details (if test needs to be completed)</b>	
Date	
Tester	
Product name and version	
Server Type	
Network/Environment	

## Findings

Test Type / Tests Executed	Findings /Vulnerabilities	Significance/ Comments	Risk Assessment (High, Medium, Low)*	Action (if any) / Fix Version (if fix required)	JIRA Job # (link)

For guidance on assessing risk level refer to [Wellnomics Product Security Evaluation Matrix](#)

<b>Risk Assessment</b>	
High risk	Release fix required and consideration for patch if existing versions have this vulnerability

Medium risk	A vulnerability that needs fixing in the next version, no need to patch existing versions	
Low risk	A theoretical or technical security issue (e.g. out of date 3rd party libraries) but not of sufficient risk to require a future fix	
Signed off by		
Position		
Date		

# Dynamic Analysis Security Testing (DAST) Record - Template

Testing below is based upon verifying we meet [Dynamic Analysis Security Testing \(DAST\) - Guide](#) .

Copy this page and create as a child page under [Dynamic Analysis Security Testing \(DAST\) - Results](#) . Complete the page there and save as a due diligence record.

**Date of Netsparker Test:**

**Server Version Tested:**

Rating	Description
<b>Must Fix</b>	Issue must be fixed. Code cannot be committed with any items at this level present.
<b>Try to Fix</b>	Try to fix if possible and effort/cost not too high.
<b>Can Ignore</b>	Can be ignored (as long as there aren't hundreds of them)

## Findings

Warning Type	Risk Assessment (Must Fix, Try to Fix, Can Ignore)*	Action (if any) / Fix Version (if fix required)	JIRA Job # (link)

Signed off by	
Position	
Date	

# DEPLOYMENT & HOSTING - Templates & Resources

- [Hardening Checklist - Windows Server OS - Template](#)
- [Disaster Recovery Report - Hosting - Template](#)
- [Hardening Checklist - SQL Server - Template](#)
- [Hardening Checklist - IIS Server - Template](#)

# Disaster Recovery Report - Hosting - Template

Use the attached document when running DR tests. Save a completed and signed copy into the completed section.

## Disaster Recovery (DR) Test Report

*A disaster recovery test is a process of implementing detailed testing to ensure that a business can restore or recover critical applications, data and continue business operations in the event of a severe interruption of any type.*

Disaster Recovery Test Basic Information	
Date of the Disaster Recovery Test:	Time of DR Test Initiation:
Date of the Last DR Test:	Closure Time of DR Test:
Locations Involved:	
Recovery Participants:	
Disaster Recovery Scenario/Test Type & Information	
The Subject of the Simulated Disaster:	<input type="checkbox"/> Ransomware <input type="checkbox"/> Power Disruption <input type="checkbox"/> Natural Disaster (Weather/Hurricane/Flood/Wildfire/Earthquake/Drought) <input type="checkbox"/> Pandemic (Move to remote work) <input type="checkbox"/> Human-Caused (Administrator/Employee Data Deletion) <input type="checkbox"/> Hardware Failure (Mass Storage/Server Failure) <input type="checkbox"/> Key staff loss (Organizational Departure/Death/Illness)
Type of DR Test:	<input type="checkbox"/> Plan Review – Detailed plan review to find/discover inconsistencies <input type="checkbox"/> Tabletop Exercise – Stakeholders walk through all components of a DR plan to ensure everyone knows their role in the event of an emergency <input type="checkbox"/> Simulation – Running through a scenario to see if your IT teams can promptly restart systems, networks, technologies, or business operations.

Describe the Test Scenario:			
Will the DR Test Impact Live Business Operations?  <i>If the answer is yes, the test needs to be coordinated with applicable business partners and any preparations for lasting business impact.</i>		<input type="checkbox"/> Yes	<input type="checkbox"/> No
If a simulation, has the plan been reviewed with stakeholders? (Initiator, local participants, local management, etc.)?	<input type="checkbox"/> Yes  <input type="checkbox"/> No	If the simulation test could impact local operations in production, has the test been reviewed and approved by necessary leadership?	<input type="checkbox"/> Yes  <input type="checkbox"/> No
What are the Goals for this Test?	<input type="checkbox"/> Testing DR Plan Function  <input type="checkbox"/> New Systems or Personnel Being Tested  <input type="checkbox"/> Gaining Feedback on Effectiveness of Policy/Procedure  <input type="checkbox"/> Updating DR Plan Process/Information		
Does this test simulate any potential data loss? If yes, what type?	<input type="checkbox"/> No  <input type="checkbox"/> Loss of Data (Folder/Database/Drive)  <input type="checkbox"/> Loss of an Application (Security misconfiguration/Bad Application Update/Negative System Configuration)  <input type="checkbox"/> Loss of a System (Hardware Failure/Virtual Server Failure)  <input type="checkbox"/> Loss of a Business Location  <input type="checkbox"/> Loss of Operations (Worst-Case Scenario)		
<b>Recovery Objectives &amp; Outcomes</b>			
Recovery Point Objective:  <i>A measure of backup frequency. Can you afford to lose 5 minutes of data, a full day, an entire week? How much data will be lost or need to restore after an outage?</i>			
Recovery Point:  <i>If a real disaster occurred, how much data would have to be restored and from where?</i>			

<p>Recovery Time Objective:</p> <p><i>The duration of time within which business systems must be restored after a disaster to avoid unacceptable consequences to the business. May include the maximum time before the operations are no longer financially viable.</i></p>	
<p>Actual Recovery Time:</p> <p><i>How much time did it take teams to restore service and close the incident from the initial call, email, or notification to spur the disaster?</i></p>	
<p>Describe the outcomes of the disaster recovery test.</p> <p><i>The description should include how the test played out in detail—the report should help in future planning, revisions to policy, training, etc.</i></p>	
<p>Did the disaster recovery test cause any lasting impact on the location or service?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>If yes, please describe:</p>
<p><b>Policy or Procedure Changes</b></p>	
<p>Are there any necessary changes to the disaster recovery plan in question?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No, the plan worked in whole</p> <p>If yes, please describe:</p>

<p>Are any other changes required?</p> <p><i>These changes could include staffing, policy, hardware, etc.</i></p>	
<p>Was there any human error during the test?</p> <p><i>Please note that any names should be anonymized. The purpose of the test is not to place blame, only to improve for a real disaster.</i></p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>If yes, please describe a follow-up plan for training/remediation:</p>
<p><b>Disaster Recovery Testing Closure</b></p>	
<p>Was the test completed with incident closure and complete restoration?</p> <p><i>Testing might not have been achieved if a problem arises in carrying out a test if something interrupted the test, a location requests to reschedule, or otherwise. An interruption may require a DR test to be rescheduled.</i></p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>If no, please describe:</p>
<p>Should the test be reconducted in short order based on results?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>

Disaster\_Recovery\_Test\_R...



# Hardening Checklist - Windows Server OS - Template

Designed for Windows Server 2016

<b>Server Name</b>	
<b>Date completed</b>	
<b>By</b>	

√	<b>To Do</b>
	<b>Preparation and Installation</b>
•	If machine is a new install, protect it from hostile network traffic, until the operating system is installed and hardened.
•	Consider using the <a href="#">Microsoft Security Configuration Wizard</a> to assist in hardening the host.
	<b>Service Packs and Hotfixes</b>
•	Install the latest service packs and hotfixes from Microsoft.
•	Enable automatic notification of patch availability.
	<p>Disable Auto Install/Restart of Updates. They will need to manually be installed as per policy.</p> <p>Computer Configuration\Administrative Templates\Windows Components\Windows update\Configurate Automatic Updates</p> <p>If this setting is set to Disabled, any updates that are available on Windows Update must be downloaded and installed manually. To do this, users must go to Settings &gt; Update &amp; security &gt; Windows Update.</p>
	<b>User Account Policies</b>
•	Set minimum password length.
•	Enable password complexity requirements.
•	Do not store passwords using reversible encryption. (Default)

•	Configure account lockout policy.
<b>User Rights Assignment</b>	
•	Restrict the ability to access this computer from the network to Administrators and Authenticated Users.
•	Do not grant any users the 'act as part of the operating system' right. (Default)
•	Restrict local logon access to Administrators.
•	Deny guest accounts the ability to logon as a service, a batch job, locally, or via RDP.
<b>Security Settings</b>	
•	Disallow users from creating and logging in with Microsoft accounts.
•	Disable the guest account. (Default)
•	Require Ctrl+Alt+Del for interactive logins. (Default)
•	Configure machine inactivity limit to protect idle interactive sessions.
•	Configure Microsoft Network Client to always digitally sign communications.
•	Configure Microsoft Network Client to digitally sign communications if server agrees. (Default)
•	Disable the sending of unencrypted passwords to third party SMB servers.
•	Configure Microsoft Network Server to always digitally sign communications.
•	Configure Microsoft Network Server to digitally sign communications if client agrees.
<b>Network Access Controls</b>	
•	Disable anonymous SID/Name translation. (Default)
•	Do not allow anonymous enumeration of SAM accounts. (Default)

•	Do not allow anonymous enumeration of SAM accounts and shares.
•	Do not allow everyone permissions to apply to anonymous users. (Default)
•	Do not allow any named pipes to be accessed anonymously.
•	Restrict anonymous access to named pipes and shares. (Default)
•	Do not allow any shares to be accessed anonymously.
•	Require the "Classic" sharing and security model for local accounts. (Default)
<b>Network Security Settings</b>	
•	Allow Local System to use computer identity for NTLM.
•	Disable Local System NULL session fallback.
•	Configure allowable encryption types for Kerberos.
•	Do not store LAN Manager hash values.
•	Set LAN Manager authentication level to only allow NTLMv2 and refuse LM and NTLM.
•	Enable the Windows Firewall in all profiles (domain, private, public). (Default)
•	Configure the Windows Firewall in all profiles to block inbound traffic by default. (Default)
<b>Audit Policy Settings</b>	
•	Configure Account Logon audit policy.
•	Configure Account Management audit policy.
•	Configure Logon/Logoff audit policy.

•	Configure Policy Change audit policy.
•	Configure Privilege Use audit policy.
	<b>Event Log Settings</b>
•	Configure Event Log retention method and size.
•	Configure log shipping (e.g. to Splunk).
	<b>Additional Security Protection</b>
•	Disable or uninstall unused services.
•	Disable or delete unused users.
•	Configure user rights to be as secure as possible.
•	Ensure all volumes are using the NTFS file system.
•	Configure file system permissions.
•	Configure registry permissions.
•	Disallow remote registry access if not required.
	<b>Additional Steps</b>
•	Install software to check the integrity of critical operating system files.
•	If RDP is utilized, set RDP connection encryption level to high.
	<b>Physical Security</b>
•	Configure a screen-saver to lock the console's screen automatically if the host is left unattended.

Note: Refer to <https://security.utexas.edu/os-hardening-checklist/windows-r2> for details.

# Hardening Checklist - SQL Server - Template

Adapted

from [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cust\\_contact/contact\\_center/icm\\_enterprise/icm\\_enterprise\\_11\\_0\\_1/Configuration/Guide/UCCE\\_BK\\_SFE05DDE\\_00\\_security-best-practices-guide-ucce/UCCE\\_BK\\_SFE05DDE\\_00\\_security-best-practices-guide-ucce\\_chapter\\_0110.pdf](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_11_0_1/Configuration/Guide/UCCE_BK_SFE05DDE_00_security-best-practices-guide-ucce/UCCE_BK_SFE05DDE_00_security-best-practices-guide-ucce_chapter_0110.pdf)

<b>Server Name</b>	
<b>Date completed</b>	
<b>By</b>	

Item	Set Correctly
Do not install SQL Server on an Active Directory Domain Controller	•
Set a strong password for the sa account b	•
Disable the SQL guest account.	•
Block TCPport 1433 and UDPport 1434 at the network firewall, unless the Administration & DataServer is not in the same security zone as the Logger.	•
Run the KillPwd utility to remove password data from setup files. Detailed instructions on how to run this utility can be found in the Microsoft article <a href="#">KB 263968</a> .	•
Delete or archive these setup files after installation: • sqlstp.log • sqlsp.log • setup.iss  The files are in :\\Program Files\\Microsoft SQL Server\\MSSQL\\Install for a default installation or :\\Program Files\\Microsoft SQL Server\\MSSQL\$\\Install for named instances	•
Change the recovery actions of the Microsoft SQL Server service to restart after a failure	•
Remove all sample databases.	•
Enable auditing for failed logins.	•

# Hardening Checklist - IIS Server - Template

This checklist was taken from the CIS Center for Internet Security, <https://www.cisecurity.org/>.

Only Level 1 tasks need to be completed, see [glossary page](#) for explanations.

<b>Server Name</b>	
<b>Date completed</b>	
<b>By</b>	

## Appendix: Summary Table

Item	Set Correctly
Ensure Advanced IIS logging is enabled (Scored)	•
Ensure SSLv2 is disabled (Scored)	•
Ensure SSLv3 is disabled (Scored)	•
Ensure TLS 1.0 is disabled (Not Scored)	•
Ensure TLS 1.1 is enabled (Not Scored)	•
Ensure TLS 1.2 is enabled (Scored)	•
Ensure NULL Cipher Suites is disabled (Scored)	•
Ensure DES Cipher Suites is disabled (Scored)	•
Ensure RC2 Cipher Suites is disabled (Scored)	•
Ensure RC4 Cipher Suites is disabled (Scored)	•
Ensure Triple DES Cipher Suite is configured (Not Scored)	•

Ensure AES 128/128 Cipher Suite is configured (Not Scored)	•
Ensure AES 256/256 Cipher Suite is enabled (Scored)	•
Ensure TLS Cipher Suite ordering is configured (Scored)	•
<p>Microsoft IIS Tilde Vulnerability</p> <p>Change the below Registry Key value from 0 to 1</p> <p>NtfsDisable8dot3NameCreation to HKLM\SYSTEM\CurrentControlSet\Control\FileSystem</p> <p><b>PLEASE NOTE FOLDER/FILES WILL NEED TO BE RECREATED AFTER REGISTRY CHANGE (E.G CUTTING FOLDER, AND THEN COPYING IT BACK TO LOCATION.)</b></p>	•
Use Request Filtering to disable IIS from Serving any XML files, thereby denying access to anyone Deep Linking the dbersion.xml file	

# IIS 8/8.5 Server Hardening Glossary of Information

## 5 IIS Logging Recommendations

### 5.2 Ensure Advanced IIS logging is enabled (Scored)

#### Profile Applicability:

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

#### Description:

IIS Advanced Logging is a module which provides flexibility in logging requests and client data. It provides controls that allow businesses to specify what fields are important, easily add additional fields, and provide policies pertaining to log file rollover and Request Filtering. HTTP request/response headers, server variables, and client-side fields can be easily logged with minor configuration in the IIS management console. It is recommended that Advanced Logging be enabled, and the fields which could be of value to the type of business or application in the event of a security incident, be identified and logged.

#### Rationale:

Many of the fields available in Advanced Logging many can provide extensive, real-time data and details not otherwise obtainable. Developers and security professionals can use this information to identify and remediate application vulnerabilities/attack patterns.

#### Audit:

Browse to the location of the Advanced Logs and verify .log files are being generated. Note that logs will be written to disk after a non-determined period of time. They can be written into their specified directory immediately if, in the Log Definition, the Publish real-time events and Write to disk options are selected.

#### Remediation:

IIS Advanced Logging can be configured for servers, Web sites, and directories in IIS Manager. To enable Advanced Logging using the UI:

1. Open Internet Information Services (IIS) Manager
2. Click the server in the Connections pane
3. Double-click the Advanced Logging icon on the Home page
4. Click Enable Advanced Logging in the Actions pane

The fields that will be logged need to be configured using the Edit Logging Fields action. As with IIS's standard log files, their location should be changed.

Note: There may be performance considerations depending on the extent of the configuration. Advanced logging requires installation using Web Platform Installer or manually form the download link in the References section.

#### References:

1. <http://learn.iis.net/page.aspx/579/advanced+-logging-for-iis-70---customhttp://learn.iis.net/page.aspx/579/advanced-logging-for-iis-70---custom-logging#openlogging#open> [ <http://learn.iis.net/page.aspx/579/advanced-logging-for-iis-70---custom-logging#open> ]
2. <http://technet.microsoft.com/en+-us/library/cc732826%28WS.10%29.aspx> [ <http://technet.microsoft.com/en-us/library/cc732826%28WS.10%29.aspx> ]
3. <https://www.iis.net/downloads/microsoft/advanced+-logging> [ <https://www.iis.net/downloads/microsoft/advanced-logging> ]

#### Notes:

IIS Advanced Logging is not enabled by default.

## 7 Transport Encryption

This section contains recommendations for configuring IIS protocols and cipher suites.

### 7.1 Ensure HSTS Header is set (Not Scored)



## Profile Applicability:

- Level 2 - IIS 8.0
- Level 2 - IIS 8.5

## Description:

HTTP Strict Transport Security (HSTS) allows a site to inform the user agent to communicate with the site only over HTTPS. This header takes two parameters: max-age, "specifies the number of seconds, after the reception of the STS header field, during which the user agent regards the host (from whom the message was received) as a Known HSTS Host [speaks only HTTPS]"; and includeSubDomains. includeSubDomains is an optional directive that defines how this policy is applied to subdomains. If includeSubDomains is included in the header, it provides the following definition: this HSTS Policy also applies to any hosts whose domain names are subdomains of the Known HSTS Host's domain name.

## Rationale:

HTTP Strict Transport Security (HSTS) is a simple and widely supported standard to protect visitors by ensuring that their browsers always connect to a website over HTTPS. HSTS exists to remove the need for the common, insecure practice of redirecting users from http:// to https:// URLs. HSTS relies on the User Agent/Browser to enforce the required behavior. All major browsers support it. If the browser doesn't support HSTS, it will be ignored.

When a browser knows that a domain has enabled HSTS, it does two things:

1. Always uses an https:// connection, even when clicking on an http:// link or after typing a domain into the location bar without specifying a protocol.
2. Removes the ability for users to click through warnings about invalid certificates.

A domain instructs browsers that it has enabled HSTS by returning an HTTP header over an HTTPS connection.

## Audit:

The recommended max age is 8 minutes (480 seconds) or greater. Any value greater than 0 is acceptable. Perform the following in IIS Manager to view host headers configured for the server:

1. Open IIS Manager
2. In the Connections pane, select your server
3. In the Features View pane, double click HTTP Response Headers
4. Verify an entry exists named Strict-Transport-Security
5. Double click Strict-Transport-Security and verify the Value: box contains any value greater than 0
6. Click OK.

Perform the following in IIS Manager to view host headers configured for the *Website*:

1. Open IIS Manager
2. In the Connections pane, expand the tree and select *Website*
3. In the Features View pane, double click HTTP Response Headers
4. Verify an entry exists name Strict-Transport-Security
5. Double click Strict-Transport-Security and verify the Value: box contains any value greater than 0
6. Click OK.

## Remediation:

Any value greater than 0 meets this recommendation. The examples below are specific to 8 minutes but can be adjusted to meet your requirements.

To set the HTTP Header at the server level using an `AppCmd.exe` command, run the following command from an elevated command prompt:

```
%systemroot%\system32\inetsrv\appcmd.exe set config -  
section:system.webServer/httpProtocol /+"customHeaders.[name='Strict-TransportSecurity',value='max-age=480']"
```

To set the HTTP Header and include subdomains at the server level using an `AppCmd.exe` command, run the following command from an elevated command prompt:

```
%systemroot%\system32\inetsrv\appcmd.exe set config -  
section:system.webServer/httpProtocol /+"customHeaders.[name='Strict-TransportSecurity',value='max-age=480;  
includeSubDomains']"
```

To set the HTTP Header at the *Website* level using an `AppCmd.exe` command, run the following command from an elevated command prompt:

```
%systemroot%\system32\inetsrv\appcmd.exe set config -  
section:system.webServer/httpProtocol /+"customHeaders.[name='Strict-TransportSecurity',value='max-age=480']"
```

To set the HTTP Header and include subdomains at the *Website* level using an `AppCmd.exe` command, run the following command from an elevated command prompt:

```
%systemroot%\system32\inetsrv\appcmd.exe set config "Website" -
```

section:system.webServer/httpProtocol /+ "customHeaders.[name='Strict-TransportSecurity',value='max-age=480; includeSubDomains']"

**References:**

1. <http://tools.ietf.org/html/rfc6797#section-5.1> [ <http://tools.ietf.org/html/rfc6797#section-5.1> ]
2. <https://https.cio.gov/hsts/> [ <https://https.cio.gov/hsts/> ]
3. <https://www.iis.net/configreference/system.webserver/httpprotocol/customheaders#006> [ <https://www.iis.net/configreference/system.webserver/httpprotocol/customheaders#006> ]

## 7.2 Ensure SSLv2 is disabled (Scored)

**Profile Applicability:**

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

**Description:**

This protocol is not considered cryptographically secure. Disabling it is recommended. This protocol is disabled by default if the registry key is not present. A reboot is required for these changes to be reflected.

**Rationale:**

Disabling weak protocols will help ensure the confidentiality and integrity of in-transit data.

**Audit:**

Perform the following to verify SSL 2.0 is disabled.

1. If the following key is not present, SSL 2.0 is disabled.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0

1. Ensure the following key is set to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server\Enabled

**Remediation:**

Perform the following to disable SSL 2.0:

1. If the following key is not present, SSL 2.0 is disabled. You can delete the key to disable the protocol. If you delete the key, steps 2 and 3 are not necessary.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0

1. If the key exists, set it to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server\Enabled

**Default Value:**

Enabled

**References:**

1.
  - a. <http://technet.microsoft.com/en-us/library/dn786419.aspx> [ <http://technet.microsoft.com/en-us/library/dn786419.aspx> ]
  - b. <http://technet.microsoft.com/en-us/library/dn786433.aspx> [ <http://technet.microsoft.com/en-us/library/dn786433.aspx> ]
  - c. <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> [ <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> ]
  - d. [https://www.owasp.org/index.php/Testing\\_for\\_SSL-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL-TLS_%28OWASP-CM-001%29) [ [https://www.owasp.org/index.php/Testing\\_for\\_SSL-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL-TLS_%28OWASP-CM-001%29) ]

## 7.3 Ensure SSLv3 is disabled (Scored)

**Profile Applicability:**

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

**Description:**

This protocol is not considered cryptographically secure. Disabling it is recommended.

**Rationale:**

Disabling weak protocols will help ensure the confidentiality and integrity of in-transit data.

**Audit:**

Perform the following to verify SSL 3.0 is disabled:

1. Ensure the following key is set to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server\Enabled

**Remediation:**

Perform the following to disable SSL 3.0:

1. Set the following key to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server\Enabled

**Default Value:**

Enabled

**References:**

1. <https://www.openssl.org/~bodo/ssl+-poodle.pdf> [https://www.openssl.org/~bodo/ssl-poodle.pdf]
2. <http://technet.microsoft.com/en+-us/library/dn786419.aspx> [http://technet.microsoft.com/en-us/library/dn786419.aspx]
3. [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) [https://www.owasp.org/index.php/Testing\_for\_SSL-TLS\_%28OWASP-CM-001%29]
4. <http://technet.microsoft.com/en+-us/library/dn786433.aspx> [http://technet.microsoft.com/en-us/library/dn786433.aspx]
5. <http://msdn.microsoft.com/en+-us/library/aa374757%28v=vs.85%29.aspx> [http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx]

7.4 Ensure TLS 1.0 is disabled (Not Scored)

**Profile Applicability:**

- Level 2 - IIS 8.0
- Level 2 - IIS 8.5

**Description:**

The PCI Data Security Standard 3.1 recommends disabling "early TLS" along with SSL:

SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016.

**Rationale:**

This item is Not Scored for the following reasons:

- Enabling TLS 1.2 is recommended.
- These protocols do not suffer from known practical attacks.

**Audit:**

Review the following registry locations to verify that TLS 1.0 is configured as expected. Disabled settings - Enabled to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\Enabled

**Remediation:**

Set the following registry locations to configure TLS 1.0. To disable, set Enabled to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\Enabled

**References:**

1. <http://msdn.microsoft.com/en+-us/library/aa374757%28v=vs.85%29.aspx> [http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx]
2. [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) [https://www.owasp.org/index.php/Testing\_for\_SSL-TLS\_%28OWASP-CM-001%29]
3. <http://technet.microsoft.com/en+-us/library/dn786419.aspx> [http://technet.microsoft.com/en-us/library/dn786419.aspx]
4. <http://technet.microsoft.com/en+-us/library/dn786433.aspx> [http://technet.microsoft.com/en-us/library/dn786433.aspx]
5. [https://www.pcisecuritystandards.org/document\\_library?category=pcidss&document=pci\\_dss#agreement](https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss#agreement) [https://www.pcisecuritystandards.org/document\_library?category=pcidss&document=pci\_dss#agreement]

## 7.5 Ensure TLS 1.1 is enabled (Not Scored)

### Profile Applicability:

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

### Description:

Enabling TLS 1.1 is required for backward compatibility.

### Rationale:

This item is Not Scored for the following reasons:

- Enabling TLS 1.2 is recommended.
- This protocol does not suffer from known practical attacks.

### Audit:

Review the following registry locations to verify that TLS 1.1 is enabled. Enabled settings: Enabled to 1.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server\Enabled

### Remediation:

Set the following registry locations to enable TLS 1.1. Set Enabled to 1.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server\Enabled

### References:

1. <http://technet.microsoft.com/en-us/library/dn786433.aspx> [ http://technet.microsoft.com/en-us/library/dn786433.aspx ]
2. [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) [ https://www.owasp.org/index.php/Testing\_for\_SSL-TLS\_%28OWASP-CM-001%29 ]
3. <http://technet.microsoft.com/en-us/library/dn786419.aspx> [ http://technet.microsoft.com/en-us/library/dn786419.aspx ]
4. <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> [ http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx ]

## 7.6 Ensure TLS 1.2 is enabled (Scored)

### Profile Applicability:

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

### Description:

TLS 1.2 is the most recent and mature protocol for protecting the confidentiality and integrity of HTTP traffic. Enabling TLS 1.2 is recommended. This protocol is enabled by default if the registry key is not present. As with any registry changes, a reboot is required for changes to take effect.

### Rationale:

Enabling this protocol will help ensure the confidentiality and integrity of data in transit.

### Audit:

Perform the following to verify TLS 1.2 has been enabled:

1. Ensure the following key is not present. If it is present, see step 2.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\

1. Ensure the following key is set to 0xFFFFFFFF

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server\Enabled

### Remediation:

Perform the following to enable TLS 1.2:

1. Check to see if the following key exists. If it doesn't, TLS 1.2 is enabled by default. If it does, you can delete it or follow step 2.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\

1. If the key exists, set the following key to 0xFFFFFFFF

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server\Enabled

**References:**

1.
  - a. <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> [ <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> ]
  - b. [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) [ [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) ]
  - c. <http://technet.microsoft.com/en-us/library/dn786419.aspx> [ <http://technet.microsoft.com/en-us/library/dn786419.aspx> ]
  - d. <http://technet.microsoft.com/en-us/library/dn786433.aspx> [ <http://technet.microsoft.com/en-us/library/dn786433.aspx> ]

### 7.7 Ensure NULL Cipher Suites is disabled (Scored)

**Profile Applicability:**

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

**Description:**

The NULL cipher does not provide data confidentiality or integrity. It is recommended that the NULL cipher be disabled.

**Rationale:**

By disabling the NULL cipher, there is a better chance of maintaining data confidentiality and integrity.

**Audit:**

To verify the NULL cipher has been disabled, ensure the following key does not exist or is set to 0:

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL\Enabled

**Remediation:**

To disable the NULL cipher, ensure the following key is absent. If the key is present, ensure it is set to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL\Enabled

**References:**

1. [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) [ [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) ]
2. <http://technet.microsoft.com/en-us/library/dn786419.aspx> [ <http://technet.microsoft.com/en-us/library/dn786419.aspx> ]
3. <http://technet.microsoft.com/en-us/library/dn786433.aspx> [ <http://technet.microsoft.com/en-us/library/dn786433.aspx> ]
4. <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> [ <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> ]

### 7.8 Ensure DES Cipher Suites is disabled (Scored)

**Profile Applicability:**

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

**Description:**

DES is a weak symmetric-key cipher. It is recommended that it be disabled.

**Rationale:**

By disabling DES, there is a better chance of maintaining data confidentiality and integrity.

**Audit:**

To verify the DES<sub>56/56</sub> cipher has been disabled, ensure the following key does not exist or is set to 0:

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56

**Remediation:**

To disable DES<sub>56/56</sub>, ensure the following key is absent. If the key is present, ensure it is set to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56\Enabled

**References:**

1. [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) [[https://www.owasp.org/index.php/Testing\\_for\\_SSL-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL-TLS_%28OWASP-CM-001%29)]
2. <http://technet.microsoft.com/en+-us/library/dn786433.aspx> [<http://technet.microsoft.com/en-us/library/dn786433.aspx>]
3. <http://technet.microsoft.com/en+-us/library/dn786419.aspx> [<http://technet.microsoft.com/en-us/library/dn786419.aspx>]
4. <http://msdn.microsoft.com/en+-us/library/aa374757%28v=vs.85%29.aspx> [<http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx>]

## 7.9 Ensure RC2 Cipher Suites is disabled (Scored)

### Profile Applicability:

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

### Description:

RC2 is a weak symmetric-key block cipher. It is recommended that it be disabled.

### Rationale:

By disabling RC2, there is a better chance of maintaining data confidentiality and integrity. **Audit:**

To verify the `RC2_40/128` cipher has been disabled, ensure the following key does not exist or is set to 0:

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2\_40/128\Enabled

To verify the `RC2_56/128` cipher has been disabled, ensure the following key does not exist or is set to 0:

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2\_56/128\Enabled

### Remediation:

To disable `RC2_40/128`, ensure the following key is absent. If the key is present, ensure it is set to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2\_40/128\Enabled

To disable `RC2_56/128`, ensure the following key is absent. If the key is present, ensure it is set to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2\_56/128\Enabled

### References:

1. <http://technet.microsoft.com/en+-us/library/dn786419.aspx> [<http://technet.microsoft.com/en-us/library/dn786419.aspx>]
2. <http://technet.microsoft.com/en+-us/library/dn786433.aspx> [<http://technet.microsoft.com/en-us/library/dn786433.aspx>]
3. <http://msdn.microsoft.com/en+-us/library/aa374757%28v=vs.85%29.aspx> [<http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx>]
4. [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) [[https://www.owasp.org/index.php/Testing\\_for\\_SSL-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL-TLS_%28OWASP-CM-001%29)]

## 7.10 Ensure RC4 Cipher Suites is disabled (Scored)

### Profile Applicability:

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

### Description:

RC4 is a stream cipher that has known practical attacks. It is recommended that RC4 be disabled. The only RC4 cipher enabled by default on Server 2012 and 2012 R2 is RC4 128/128.

### Rationale:

The use of RC4 may increase an adversaries' ability to read sensitive information sent over SSL/TLS.

### Audit:

To verify the `RC4_40/128` cipher has been disabled, ensure the following key does not exist or is set to 0:

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4\_40/128\Enabled

To verify the `RC4_56/128` cipher has been disabled, ensure the following key does not exist or is set to 0:

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4\_56/128\Enabled

To verify the `RC4_64/128` cipher has been disabled, ensure the following key does not exist or is set to 0:

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4

64/128\Enabled

To verify the `RC4_128/128` cipher has been disabled, ensure the following key is set to 0:

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4\_128/128\Enabled

### Remediation:

To disable `RC4_40/128`, ensure the following key is absent. If the key is present, ensure it is set to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4\_40/128\Enabled

To disable `RC4_56/128`, ensure the following key is absent. If the key is present, ensure it is set to 0.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4\_56/128\Enabled

To disable RC4 64/128, ensure the following key is absent. If the key is present, ensure it is set to 0.  
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128\Enabled  
To disable RC4 128/128, ensure the following key is set to 0.  
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128\Enabled  
**References:**

1. <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> [ <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> ]
2. <http://technet.microsoft.com/en-us/library/dn786433.aspx> [ <http://technet.microsoft.com/en-us/library/dn786433.aspx> ]
3. <http://technet.microsoft.com/en-us/library/dn786419.aspx> [ <http://technet.microsoft.com/en-us/library/dn786419.aspx> ]
4. [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) [ [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) ]

## 7.11 Ensure Triple DES Cipher Suite is configured (Not Scored)

### Profile Applicability:

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

### Description:

Enabling Triple DES Cipher Suites may be required for client compatibility. Enable or disable this cipher suite accordingly.

### Rationale:

This item is Not Scored for the following reasons:

- Enabling AES 256/256 is recommended.
- This cipher does not suffer from known practical attacks.

### Audit:

To verify the Triple DES 168/168 cipher has been enabled, ensure the following key either does not exist or is set to 0xFFFFFFFF:  
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168/168\Enabled

### Remediation:

To enable Triple DES 168/168, ensure the following key is not present or is set to 0xFFFFFFFF.  
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168/168\Enabled

### References:

1. [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) [ [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) ]
2. <http://technet.microsoft.com/en-us/library/dn786419.aspx> [ <http://technet.microsoft.com/en-us/library/dn786419.aspx> ]
3. <http://technet.microsoft.com/en-us/library/dn786433.aspx> [ <http://technet.microsoft.com/en-us/library/dn786433.aspx> ]
4. <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> [ <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> ]

## 7.12 Ensure AES 128/128 Cipher Suite is configured (Not Scored)

### Profile Applicability:

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

### Description:

Enabling AES 128/128 may be required for client compatibility. Enable or disable this cipher suite accordingly.

### Rationale:

This item is Not Scored for the following reasons:

- Enabling AES 256/256 is recommended.
- This cipher does not suffer from known practical attacks.



**Audit:**

To verify the AES 128/128 cipher has been enabled, ensure the following key is set to 0xFFFFFFFF:  
 HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128\Enabled

**Remediation:**

To enable the AES 128/128 cipher, ensure the following key is set to 0xFFFFFFFF:  
 HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128\Enabled

**References:**

1. <http://technet.microsoft.com/en-us/library/dn786419.aspx> [ <http://technet.microsoft.com/en-us/library/dn786419.aspx> ]
2. <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> [ <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> ]
3. [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) [ [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) ]
4. <http://technet.microsoft.com/en-us/library/dn786433.aspx> [ <http://technet.microsoft.com/en-us/library/dn786433.aspx> ]

## 7.13 Ensure AES 256/256 Cipher Suite is enabled (Scored)

**Profile Applicability:**

- Level 1 - IIS 8.0
- Level 1 - IIS 8.5

**Description:**

AES 256/256 is the most recent and mature cipher suite for protecting the confidentiality and integrity of HTTP traffic. Enabling AES 256/256 is recommended. This is enabled by default on Server 2012 and 2012 R2.

**Rationale:**

Enabling this cipher will help ensure the confidentiality and integrity of data in transit.

**Audit:**

To verify the AES 256/256 cipher has been enabled:

1. Ensure that the following key does not exist. If it does exist, you can either delete the key or proceed to step 2.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256\

1. If the following key exists, ensure the following is set to 0xFFFFFFFF:

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256\Enabled

**Remediation:**

To enable the AES 256/256 cipher:

1. Ensure that the following key does not exist. If it does exist, you can either delete the key or proceed to step 2.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256\

1. If the key exists, ensure the following is set to 0xFFFFFFFF.

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256\Enabled

**References:**

1.
  - a. <http://technet.microsoft.com/en-us/library/dn786419.aspx> [ <http://technet.microsoft.com/en-us/library/dn786419.aspx> ]
  - b. <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> [ <http://msdn.microsoft.com/en-us/library/aa374757%28v=vs.85%29.aspx> ]
2. [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) [ [https://www.owasp.org/index.php/Testing\\_for\\_SSL+-TLS\\_%28OWASP-CM-001%29](https://www.owasp.org/index.php/Testing_for_SSL+-TLS_%28OWASP-CM-001%29) ]
3. <http://technet.microsoft.com/en-us/library/dn786433.aspx> [ <http://technet.microsoft.com/en-us/library/dn786433.aspx> ]

## 7.14 Ensure TLS Cipher Suite ordering is configured (Scored)

**Profile Applicability:**



- Level 2 - IIS 8.0
- Level 2 - IIS 8.5

**Description:**

Cipher suites are a named combination of authentication, encryption, message authentication code, and key exchange algorithms used for the security settings of a network connection using TLS protocol. Clients send a cipher list and a list of ciphers that it supports in order of preference to a server. The server then replies with the cipher suite that it selects from the client cipher suite list.

**Rationale:**

Cipher suites should be ordered from strongest to weakest in order to ensure that the more secure configuration is used for encryption between the server and client.

**Audit:**

To verify the cipher suite order is set correctly, ensure the following key is set to:

```

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
HKLM\System\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002\Fu nctions

```

**Remediation:**

To order the cipher suites correctly, ensure the following key is set to:

```

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
HKLM\System\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002\Fu nctions

```

**Impact:**

Cipher ordering is important to ensure that the most secure ciphers are listed first and will be applied over weaker ciphers when possible.

# INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Templates & Resources

- [Employee Leaving Checklist - Template](#)
- [Information Security Policy Acknowledgment and Agreement - Employees & Contractors - Template](#)
- [Risk Assessment - Template](#)
- [Application for Access to Non Anonymised Customer Data - Employees & Contractors - Template](#)
- [Change Request Form - Internal - Template](#)
- [Equipment De-Commissioning Form - Internal - Template](#)
- [Disaster Recovery Report - Internal - Template](#)
- [Incident Investigation Form - Internal - Template](#)

# Employee Leaving Checklist - Template

Last updated 16 Feb 2021

See also [Employee Leaving Completed Checklists](#)

Checklist Item	Date	Confirmed By:
Disable Active Directory account		
Move user from "Staffs" to "Old Staff" in Active Directory		
Set up an email redirect, if necessary, to a relevant staff member		
Archive emails		
Remove any Office 365 / CRM licenses they may be using.		
Reset the Office 365 password and ensure no external email accounts are linked. See <a href="https://support.office.com/en-us/article/Remove-a-former-employee-from-Office-365-44d96212-4d90-4027-9aa9-a95eddb367d1">https://support.office.com/en-us/article/Remove-a-former-employee-from-Office-365-44d96212-4d90-4027-9aa9-a95eddb367d1</a> for a full list of steps to take for email and Office 365		
Remove them from the printer ( <a href="http://192.168.22.152">http://192.168.22.152</a> )		
All door keys returned		
Remove them from August Smart lock access (if they had access)		
Computer returned - password provided		
Phone account transferred		
Reset both WiFi passwords - WellnomicsWifi and WellnomicsGuest		
Disable their Confluence and JIRA accounts as applicable.		
Remove any MSDN access, if applicable ????		
Archive/disable Atlassian account		
Remove them from Freshdesk, if applicable		

## Further actions if employee had support or IT Admin Access

Reset following passwords	Location	Notes	Date	Confirmed By:
Wellnomics\Administrator password	vm-dc3	Administrator		
Wellnomics\Welladmin password	vm-dc3	Domain Administrator		
Welladmin	<a href="https://192.168.22.254/">https://192.168.22.254/</a>	Firewall		
<username>@wellnomics.com	vm-dc3	The users account – disable		

<username>@wellnomics.com	<a href="https://portal.office.com">portal.office.com</a>	The users email and Office 365 admin login		
<a href="mailto:GlobalAdmin@wellnomics.com">GlobalAdmin@wellnomics.com</a>	Office 365 / CRM – <a href="https://portal.office.com">portal.office.com</a>	Global login for Exchange and CRM		
Administrator	ALL WRM Hosting Servers	May not be Administrator – whatever the login name is.		
Office 365 Global Admin password				
GoDaddy password				
DNSMadeEasy password				
EuroDNS password				
VMware password	<a href="https://my.vmware.com">https://my.vmware.com</a>	VMWare licensing		
MSDN and other Microsoft account passwords				
<a href="mailto:support@wellnomics.com">support@wellnomics.com</a> password	All WRM instances			
<a href="mailto:itadmin@wellnomics.com">itadmin@wellnomics.com</a> password				
<a href="mailto:wellnomics.admin@wellnomics.com">wellnomics.admin@wellnomics.com</a>	All WRM instances			

# Information Security Policy Acknowledgment and Agreement - Employees & Contractors - Template

All Wellnomics staff and, if relevant, seconded contractors and other that may have temporary access to potentially confidential information, are required to read and agree, through signature, their acceptance of the Wellnomics [Privacy Policy](#) and other documents relating to data protection, data privacy and confidentiality covered by the [\(OLD\) WELLNOMICS INFORMATION SECURITY POLICIES](#) and its related documents.

<b>Name</b>	
<b>Position</b>	
<b>Date of commencement of employment with Wellnomics</b>	
<b>Organization (if not Wellnomics)</b>	
<b>Position</b>	

I \_\_\_\_\_ hereby acknowledge that I :-

- have received training in aspects of Wellnomics policies and procedures as they relate to data privacy and confidentiality
- have understood my responsibilities under the various policies and procedures as they relate to data privacy and confidentiality
- undertake to ensure complacence with the Wellnomics policies and procedures as they relate to data privacy and confidentiality
- agree to comply with any checks or audits carried out under the relevant policies and procedures as they relate to data privacy and confidentiality

Signed \_\_\_\_\_ Date: \_\_\_\_\_

Checked and countersigned

I \_\_\_\_\_ as a designated Privacy Officer under the Wellnomics [Privacy Policy](#) hereby certify that the above signed has been provided with prescribed the data privacy and confidentiality training as set out in Wellnomics [Privacy Policy](#) and has accepted their responsibilities under the policy and other related policies as they apply to data privacy and confidentiality

Signed \_\_\_\_\_ Date: \_\_\_\_\_

(Wellnomics Privacy Officer)

\*\*\* END \*\*\*

# Risk Assessment - Template

Assessment Date.....

Completed by

Wellnomics Ltd	Code	Threat	Detail	Probability	Impact	Risk
People	P1	Disappearance staff	foreseeable, unforeseeable			
	P2	Unintentional errors (even others)	ignorance, carelessness, stress			
			Faulty procedures			
			complex and / or error-prone operation			
			dealing with passwords			
	P3	Intentional mistakes	Ignore rules			
			Breach of privacy			*see footnote 1 below
			Unauthorized access (hacking)			
	Equipment	E1	Spontaneously technical failure	Aging, wear, poor maintenance		
interruption/ stoppage						
Errors in delivered product						
E2		Environmental Factors	Base utilities			
			Utilities failure			
			temperature, humidity, dirt, dust			
E3		Cause – human factor	remote work			
			bring your own device			
			deliberate change function equipment			
			damage, destruction, theft			
Software	S1	Software errors	development or maintenance			
			maintenance			

			unintentional damage (bugs etc.)			
	S2	Software damage	virus, malware			
			Illegal third party software			
			illegal use of software			
Data	D1	Via data transmission	Accidental loss (negligence)			
			theft (physical)			
			theft (digital)			
			crash			
			Careless destruction			
	D2	Via software	Faulty or compromised software (malware)			** see footnote 2 below
	D3	Through people	erroneous data mutation			

**Classification:**

**PROBABILITY**

<b>High</b>	3	2	
<b>Average</b>	1	2	
<b>Low</b>	1	1	
	<b>Low</b>	<b>Average</b>	

**IMPACT**

**Completed Actions Following Risk Assessment on**

**Areas Classified as Risk Level 3 or higher:-**

*Insert actions list and plan of action here.....*

-



Viewed and Approved by CEO Signed..... Date .....

Acknowledged as complete by CEO Signed ..... Date) .....

Next Risk Assessment Date: .....

#### Footnote 1: Intentional Mistakes - unauthorized access

Whilst the likelihood of unauthorized access is low, it has to be accepted that should it happen the consequences in terms of impact could be high. For these reasons, the following protections are in place to protect against unauthorized access to environment, workstations, software in productions and software in use on externally hosted servers:-

- 
- Checked restrictions regarding access and passwords and ensured that staff only have access to what they need and such access requires unique usernames and passwords (no generic accounts in use). See authorization matrix - section 4.3 of [\(OLD\) WELLNOMICS INFORMATION SECURITY POLICIES](#)
- Emailed staff regarding current password policies around password construction and strength and password change frequency
- Enforce password change frequency through group policies ( see Section 4.2 of [Passwords and Encryption - Employees & Contractors - Policy](#))
- Unattended/unused automatic workstation lockout after 10 minutes (though staff are trained to log out of their workstation if they leave their desks)
- Intrinsic protections built into the Wellnomics software when in use:-
  - Protection against XSS (Cross site scripting)
  - Protection against SQL injection via user interfaces
  - Use of secure connection protocols and standards (HTTPS/TLS) in external and internal software communications
- Physical isolation of development environment - doors of rooms locked when unattended
- Physical isolation of workstations capable of accessing hosting servers. locked door policy when room unattended.
- Authorized entry only policy. All visitors must be signed in and out of general office environment and must be accompanied at all times.

#### Footnote 2: Software Damage (virus/malware) / Faulty or compromised software

- 
- Randomly checked a variety of workstations to ensure up to date virus and malware signatures - all OK. See also :-
  - [Firewall - Internal Security - Policy](#)
- Checked firewall settings software version up to date
- Re-enforced existing corporate policies (through staff meeting opportunity) around the use of portable devices and the need to ensure that only Wellnomics approved devices are allowed to connect to the network.

#### Footnote 3: Residual Risks

Wellnomics accepts that whilst elevated risks can be identified and steps taken to minimize the likelihood of occurrence, residual, low level risks (categorized as 1 in the above risk assessments) do remain. In this context, "residual risks" are risks that remain after performing the risk analysis and the Plan of Action. The risks are not measures that can be eliminated or reduced. Because no objective actions can be taken for such residual risks, there exists the Wellnomics [Business Continuity \(& Disaster Recovery Plan\) - Guideline](#). This document covers the likely consequence of residual risks occurring and the impact that they might have.



# Application for Access to Non Anonymised Customer Data - Employees & Contractors - Template

This form must be completed by any staff member requiring access to non-anonymized customer data. Completed forms must be submitted to the Chief Executive or the Principal Consultant for consideration.

<b>Application Date</b>	
<b>Staff Member Requiring Access</b>	
<b>Customer Name</b>	
<b>Description of Data</b>	
<b>Date Data Originally Received</b>	
<b>Reason(s) for access</b>	
<b>Dates between which access is required</b>	
<b>Will data be deleted after this access period</b>	Yes / No
<b>If data not to be deleted, provide reason(s) for continued storage</b>	

Request Approved by: .....

Date .....

# Change Request Form - Internal - Template

<b>Change Request Form</b>	<b>Please complete</b>
Submitted by:	
Date Submitted	
Nature of change	Process / System / Equipment / Software / Other (please delete as appropriate)
Details of Proposed Change	
Expected benefits of change	
Possible costs or savings of change	

# Equipment De-Commissioning Form - Internal - Template

**Note:** This form relates to [Equipment Disposal - Policy](#) . When required, this form should be printed completed, saved as a .pdf file and then saved as a child page under [Equipment De-Commissioning - Completed Records](#)

This form is to be used to record the decommissioning of any equipment that, at the end of its period of use at Wellnomics, contains, or may contain information or data relating to the business or activities of Wellnomics or any of its associations or customers. In this context, equipment includes but is not limited to computer/server memory devices (HDD, portable drives, pen drives etc.), tablets, and smart devices (phones etc.).

NB Use attached Word document to create and save completed form

Equipment De-commission ...

<b>Date</b>	
<b>Equipment/asset type</b>	
<b>Asset tag number (if any)</b>	
<b>Description of data on the device (if any)</b>	
<b>Reason for decommissioning</b>	
<b>Method of decommissioning</b>	<p>Tick as appropriate (more than one may be ticked)</p> <ul style="list-style-type: none"> <li>• mechanical destruction</li> <li>• reformatting</li> <li>• removal of recording media</li> <li>• Other (please describe)</li> </ul> <p>Comments:</p>
<b>Person carrying out decommissioning</b>	

I confirm that the equipment/media detailed above has been decommissioned in accordance with the Wellnomics policy.

Name: ..... Date: .....

Signature: .....

# Disaster Recovery Report - Internal - Template

Use the attached document when running DR tests. Save a completed and signed copy into the completed section.

## Disaster Recovery (DR) Test Report

*A disaster recovery test is a process of implementing detailed testing to ensure that a business can restore or recover critical applications, data and continue business operations in the event of a severe interruption of any type.*

Disaster Recovery Test Basic Information	
Date of the Disaster Recovery Test:	Time of DR Test Initiation:
Date of the Last DR Test:	Closure Time of DR Test:
Locations Involved:	
Recovery Participants:	
Disaster Recovery Scenario/Test Type & Information	
The Subject of the Simulated Disaster:	<input type="checkbox"/> Ransomware <input type="checkbox"/> Power Disruption <input type="checkbox"/> Natural Disaster (Weather/Hurricane/Flood/Wildfire/Earthquake/Drought) <input type="checkbox"/> Pandemic (Move to remote work) <input type="checkbox"/> Human-Caused (Administrator/Employee Data Deletion) <input type="checkbox"/> Hardware Failure (Mass Storage/Server Failure) <input type="checkbox"/> Key staff loss (Organizational Departure/Death/Illness)
Type of DR Test:	<input type="checkbox"/> Plan Review – Detailed plan review to find/discover inconsistencies <input type="checkbox"/> Tabletop Exercise – Stakeholders walk through all components of a DR plan to ensure everyone knows their role in the event of an emergency <input type="checkbox"/> Simulation – Running through a scenario to see if your IT teams can promptly restart systems, networks, technologies, or business operations.

Describe the Test Scenario:			
Will the DR Test Impact Live Business Operations?  <i>If the answer is yes, the test needs to be coordinated with applicable business partners and any preparations for lasting business impact.</i>		<input type="checkbox"/> Yes	<input type="checkbox"/> No
If a simulation, has the plan been reviewed with stakeholders? (Initiator, local participants, local management, etc.)?	<input type="checkbox"/> Yes  <input type="checkbox"/> No	If the simulation test could impact local operations in production, has the test been reviewed and approved by necessary leadership?	<input type="checkbox"/> Yes  <input type="checkbox"/> No
What are the Goals for this Test?	<input type="checkbox"/> Testing DR Plan Function  <input type="checkbox"/> New Systems or Personnel Being Tested  <input type="checkbox"/> Gaining Feedback on Effectiveness of Policy/Procedure  <input type="checkbox"/> Updating DR Plan Process/Information		
Does this test simulate any potential data loss? If yes, what type?	<input type="checkbox"/> No  <input type="checkbox"/> Loss of Data (Folder/Database/Drive)  <input type="checkbox"/> Loss of an Application (Security misconfiguration/Bad Application Update/Negative System Configuration)  <input type="checkbox"/> Loss of a System (Hardware Failure/Virtual Server Failure)  <input type="checkbox"/> Loss of a Business Location  <input type="checkbox"/> Loss of Operations (Worst-Case Scenario)		
<b>Recovery Objectives &amp; Outcomes</b>			
Recovery Point Objective:  <i>A measure of backup frequency. Can you afford to lose 5 minutes of data, a full day, an entire week? How much data will be lost or need to restore after an outage?</i>			
Recovery Point:  <i>If a real disaster occurred, how much data would have to be restored and from where?</i>			



<p>Recovery Time Objective:</p> <p><i>The duration of time within which business systems must be restored after a disaster to avoid unacceptable consequences to the business. May include the maximum time before the operations are no longer financially viable.</i></p>	
<p>Actual Recovery Time:</p> <p><i>How much time did it take teams to restore service and close the incident from the initial call, email, or notification to spur the disaster?</i></p>	
<p>Describe the outcomes of the disaster recovery test.</p> <p><i>The description should include how the test played out in detail—the report should help in future planning, revisions to policy, training, etc.</i></p>	
<p>Did the disaster recovery test cause any lasting impact on the location or service?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>If yes, please describe:</p>
<p><b>Policy or Procedure Changes</b></p>	
<p>Are there any necessary changes to the disaster recovery plan in question?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No, the plan worked in whole</p> <p>If yes, please describe:</p>

<p>Are any other changes required?</p> <p><i>These changes could include staffing, policy, hardware, etc.</i></p>	
<p>Was there any human error during the test?</p> <p><i>Please note that any names should be anonymized. The purpose of the test is not to place blame, only to improve for a real disaster.</i></p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>If yes, please describe a follow-up plan for training/remediation:</p>
<p><b>Disaster Recovery Testing Closure</b></p>	
<p>Was the test completed with incident closure and complete restoration?</p> <p><i>Testing might not have been achieved if a problem arises in carrying out a test if something interrupted the test, a location requests to reschedule, or otherwise. An interruption may require a DR test to be rescheduled.</i></p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>If no, please describe:</p>
<p>Should the test be reconducted in short order based on results?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>

Disaster\_Recovery\_Test\_R...

# Incident Investigation Form - Internal - Template

This form is to be used for any investigation of incidents recorded and reported under [Incident Management Process - Internal - Policy](#), [Security Incident Response - Internal - Policy](#) or [Incident Reporting and Resolution - Hosting & Customers - Policy](#) that are not handled within other tools (like our Support ticketing system)

The prime responsibility for the investigation any incident rests with the Chief Executive Officer (CEO) however the CEO may delegate the investigation to another person they suitable to carry out the investigation. Any corrective action identified as result of the investigation must be agreed and signed off by the CEO.

Required	Information
Incident Date	
Reported by	
Brief description of incident	
Classification of incident	People / Equipment / Application / Data (delete as appropriate)
If customer system incident specify Type (tick as appropriate)	<ul style="list-style-type: none"> <li>• "Critical Error" means an error, defect, or omission, which causes the Wellnomics Software to be completely unusable by all Users.</li> <li>• "Significant Error" means an error, defect or omission that causes the Wellnomics Software to be unusable in large part by Users</li> <li>• "Discrepancy" means an error or defect in the distribution media or material difference between the operation of the Wellnomics Software and the description of the operation of the Wellnomics Software as contained in the documentation provided for the Wellnomics Software by Wellnomics.</li> </ul>
Date reported to CEO	
Investigated by	(If not CEO, date delegated by CEO) Date:
Investigation Notes or linked documents	
Summary of findings	
Remedial action identified	
Signed off by CEO	
Remedial action completed	Date:
Closed date	Date:

# COMPLETED RECORDS - EXTERNAL - Due Diligence Checklists & Templates

This is for executive summaries of reports that are OK to be sent to customers.

See also [COMPLETED RECORDS - INTERNAL - Due Diligence Checklists and Templates](#)

- [PRODUCT & SOFTWARE DEVELOPMENT - Records - External](#)
- [DEPLOYMENT & HOSTING - Records - External](#)
- [INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Records - External](#)
- [Summary of COMPLETED RECORDS - INTERNAL - Due Diligence Checklists and Templates, etc](#)

# PRODUCT & SOFTWARE DEVELOPMENT

## - Records - External

This section contains records of completed processes done in compliance with Wellnomics policies and procedures.

### Externally available records

The below records are those that are available for public review. Note that for confidentiality reasons there may be no records that can be made available for public review.

- [Dynamic Application Security Testing \(DAST\) - Records Summary](#)
- [Static Application Security Testing \(SAST\) - Records Summary](#)
- [Independent Penetration Testing - Records](#)

### Internal only records

The below records are internal only, but can be reviewed and accessed for auditing purposes.

- [Product Security Risk Assessments - Completed Records](#)
  - [Product Security Risk Assessment - Gadget \(Aug 2022\)](#)
  - [Product Security Risk Assessment - App \(Mar 2021\)](#)
  - [Product Security Risk Assessment - SaaS \(Sep 2020\)](#)
- [Third Party Components Review - Records](#)
  - [Third Party Components Review - SaaS 4.14.0 \(Nov 2022\)](#)
  - [Third Party Components Review - SaaS 4.13.0 \(May 2022\)](#)
  - [Third Party Components Review - App 1.3.1 \(Dec 2021\)](#)
  - [Third Party Components Review - WPC 5.5.9 \(Dec 2021\)](#)
  - [Third Party Components Review - WPC 5.5.7 \(Dec 2021\)](#)
  - [Third Party Components Review - SaaS 4.1.0 \(Sep 2020\)](#)
- [Static Analysis Security Testing \(SAST\) - Records](#)
  - [SAST Record - SaaS 4.15.0 \(Jan 2023\)](#)
  - [SAST Record - SaaS 4.11.0 \(May 2022\)](#)
  - [SAST Record - SaaS 4.5.0 \(Jul 2021\)](#)
- [Dynamic Analysis Security Testing \(DAST\) - Records](#)
  - [DAST Record - SaaS 4.14.0 \(Nov 2022\)](#)
  - [DAST Record - SaaS 4.12.0 \(Nov 2022\)](#)
  - [DAST Record - SaaS 4.5.0 \(May 2021\)](#)
- [Software Development Lifecycle - Records](#)
- [Penetration Testing - Independent - Records](#)
  - [Penetration Testing - Independent - SaaS 4.12.0 \(Jul 2022\)](#)
  - [Penetration Testing - Independent - SaaS 4.5.0 Regression \(Jul 2021\)](#)
  - [Penetration Testing - Independent - SaaS 4.5.0 \(May 2021\)](#)
- [Product Security and Internal Penetration Testing - Records](#)
  - [Security Testing - Record - WPC 5.5.5 \(Nov 2020\)](#)
  - [Security Testing - Record - WPC 5.5.7 \(Nov 2020\)](#)
  - [Penetration Testing - Internal - Record - WRM 3.3 \(Oct 2017\)](#)
  - [Penetration Testing - Internal - Record - WRM 3.2/3.3 \(Apr 2017\)](#)

# Dynamic Application Security Testing (DAST) - Records Summary

DAST is completed following the processes outlined in [Dynamic Analysis Security Testing \(DAST\) - Guide](#) Issues are reviewed by Wellnomics engineers and classified using the the [Wellnomics Product Security Risk Assessment Matrix](#)

The table below are the summary outcomes of these tests. Full detailed results listing the exact issues found and details of resolutions implemented are available at [Dynamic Analysis Security Testing \(DAST\) - Records](#) (note this information is not published and is only available on request).

Date	Application / Version	Issues found	Comments
27/05/2021	Wellnomics SaaS 4.5.0	13	<p>DAST Netsparker tool was run on the release and 13 issues were identified by the tool. These issues were reviewed by Wellnomics engineers following Wellnomics Risk Assessment Matrix and guidelines.</p> <p>This review classified 10 issues as <b>Low Risk</b> and 3 issues as <b>Medium Risk</b>.</p> <p>Jira items were created for the product development work required to resolve the Medium Risk issues. These items have been added to the product backlog and scheduled for implementation in the next scheduled release of Wellnomics SaaS 4.6</p>
	Wellnomics SaaS 4.6.0	n/a	not released
6/09/21	Wellnomics SaaS 4.7.0	n/a	Test not triggered due to limited risk
17/11/21	Wellnomics SaaS 4.8.0	n/a	Test not triggered due to limited risk
4/02/22	Wellnomics SaaS 4.9.0	n/a	Test not triggered due to limited risk
25/03/22	Wellnomics SaaS 4.10.0	n/a	Test not triggered due to limited risk
18/05/22	Wellnomics SaaS 4.11.0	16	All issues were reviewed. 1 Jira item was created for development work required to successfully resolve 30 issues classified as <b>Medium Risk</b> the remaining 15 issues will be resolved via continuous refactoring.
8/06/22	Wellnomics SaaS 4.12	n/a	Test not triggered due to limited risk
2/09/22	Wellnomics SaaS 4.13	n/a	Test not triggered due to limited risk

# Static Application Security Testing (SAST) - Records Summary

SAST is completed as part of our release life cycle based on our policy [Static Analysis Security Testing \(SAST\) - Guide](#)

All issues that are identified in testing are reviewed by Wellnomics software engineers and rated either a High, Medium or Low Risk based on the [Wellnomics Product Security Risk Assessment Matrix](#) .

Below are the testing summaries. Full detailed results listing the exact issues found and details of resolutions implemented are available at [Static Analysis Security Testing \(SAST\) - Records](#) (note this information is not published and is only available on request)

Date	Product	Version	Number of Issues by Risk Rating after Classification			Comments	Jira items created for resolution
			High	Medium	Low		
03/11/2020	Desktop Client	WC 1.1.0.997	0	0	57	All issues were reviewed and classified as Low Risk - no further action is required.	0
26/05/2021	SaaS Solution	SaaS 4.5.0	0	19	94	All issues were reviewed. 1 Jira item was created for the development work required to successfully resolve all 19 issues classified as <b>Medium Risk</b> . This Jira item will also resolve 12 of the <b>Low Risk</b> issues.  This Jira item has been scheduled for implementation in the next Wellnomics SaaS release (SaaS 4.6)	1
06/07/2021	Desktop Client	WC 1.1.7.2051	0	0	56	All issues were reviewed and classified as <b>Low Risk</b> - no further action is required.	0
18/05/2022	SaaS Solution	SaaS 4.11.0	0	45	150	All issues were reviewed. 1 Jira item was created for development work required to successfully resolve 30 issues classified as <b>Medium Risk</b> the remaining 15 issues will be resolved via continuous refactoring.	1
19/05/2022	Desktop App	App 1.6.0.3790	0	0	48	All issues were reviewed and classified as <b>Low Risk</b> - no further action is required.	0

# Independent Penetration Testing - Records

Below are reports for completed independent penetration testing. Note these are summary reports that can be published to customers. Detailed reports for internal use or audit purposes are stored under [Independent Penetration Testing - Results](#)

Our next independent penetration test is due July 2022

- [Independent Penetration Testing - Record - SaaS Version 4.12.0, August 2022](#)
- [Independent Penetration Testing - Record - SaaS Version 4.5.0, July 2021](#)
- [Independent Penetration Testing - Record - WRM Version 3.4.5, May 2019](#)



# Independent Penetration Testing - Record - SaaS Version 4.12.0, August 2022

<b>Date</b>	August 2022
<b>Tester</b>	CyberCX
<b>Product</b>	Wellnomics SaaS
<b>Version</b>	Wellnomics Saas 4.12.0 Web Applications and API Testing
<b>Tested Components</b>	<ul style="list-style-type: none"><li>• Web portals/applications</li><li>• Web server API</li></ul>
<b>Server</b>	Azure hosted
<b>Status at Report Date</b>	<a href="https://wellnomicsdev.atlassian.net/l/cp/q0Tti7WH">https://wellnomicsdev.atlassian.net/l/cp/q0Tti7WH</a>
<b>Issue Summary</b>	0 High Priority 6 Medium Priority 3 Low priority Intention to be resolved with 4.16 release scheduled for release Mar 2023.

## Independent Penetration Testing Summary Report from CyberCX

CyberCX New Zealand Ltd.  
PO Box 62061  
Sylvia Park, Auckland  
New Zealand



18 November 2022

**Re: Wellnomatics Application Security review**

At the request of Wellnomatics, CyberCX NZ conducted a security assessment against the Wellnomatics external facing applications between the 20<sup>th</sup> July and the 8<sup>th</sup> August 2022. The purpose of the testing was to identify security vulnerabilities within the applications and their underlying infrastructure and to provide recommendations and solutions.

Testing comprised web application and network penetration testing, utilising user accounts provided for testing. Innomia Security used a combination of automated tools and manual testing techniques to complete this testing. Testing performed used the OWASP standards as a base minimum, and covered testing for web application security bug classes. Application testing included verifying and checking of vulnerabilities including Authentication and Authorisation, Parameter tampering, HTTPS examination, Application mapping, Directory manipulation, Session management, Cookie handling, Cross site scripting, SQL/MSL/LDAP injection and Error handling.

While the review did identify several security vulnerabilities within the scope of the review, the review did not identify any high- or critical-risk security findings that would compromise the security of the application, it's users or it's platform.

The assessment did note a number of areas where the application and its infrastructure did not meet best practices. These issues include some common weaknesses around areas such as defence in depth, attack surface reduction and error handling. While these did not have a security impact directly observable during the review, these have been raised in the resulting report alongside recommendations to remediate.

At the completion of the review, it was concluded that the systems and applications assessed within the scope of the engagement should be considered sufficiently secure to meet the business requirements for security.

Signed by a duly authorised delegate of CyberCX New Zealand Ltd.

Signature

Name: Adam Boleau

Title: Executive Director, Security Testing & Assurance

---

CyberCX New Zealand  
www.cybercx.co.nz

CONFIDENTIAL

# Independent Penetration Testing - Record - SaaS Version 4.5.0, July 2021

<b>Date</b>	02 Jul 2021
<b>Tester</b>	Insomnia
<b>Product</b>	Wellnomics SaaS
<b>Version</b>	Wellnomics SaaS 4.5.0 Web Application and API Testing
<b>Tested Components</b>	<ul style="list-style-type: none"><li>• Web portals/applications</li><li>• Web server API</li></ul>
<b>Server</b>	Azure hosted
<b>Status at Report Date</b>	<a href="#">Wellnomics SaaS 4.5.0 - Independent Penetration Test Results</a>
<b>Issue Summary</b>	1 High Priority 3 Medium Priority 7 Low priority
<b>Regression report commissioned</b>	28 July 2021
<b>Status at Regression Date</b>	<a href="#">Wellnomics SaaS 4.5.0 - Independent Penetration Test Results (Regression)</a>
<b>Issue Summary</b>	7 Low Priority

## Independent Penetration Testing Summary Report from Insomnia

Insomnia Security Group Ltd.  
PO Box 62061  
Sylvia Park, Auckland  
New Zealand



20 August 2021

**Re: Application Security Review**

At the request of Wellnoms, Insomnia Security performed security testing against the Wellnoms external facing application portals between the 17th and the 25th of June 2021. The purpose of the testing was to identify security vulnerabilities within the applications and their underlying infrastructure and to provide recommendations and solutions.

Testing comprised web application and network penetration testing, utilising user accounts provided for testing. Insomnia Security used a combination of automated tools and manual testing techniques to complete this testing. Testing performed used the OWASP standards as a base minimum, and covered testing for web application security bug classes. Application testing included verifying and checking of vulnerabilities including: Authentication and Authorisation, Parameter tampering, HTTPS examination, Application mapping, Directory manipulation, Session management, Cookie handling, Cross site scripting, SQL/SQLi, LDAP injection and Error handling.

The review subsequently identified several security vulnerabilities within the scope of the review; however none of these weaknesses would allow an adversary to obtain unauthorised access to the applications or the data they contained.

Comparing the application to others that Insomnia Security has reviewed in the past, and the type of vulnerabilities identified, the overall appraisal was similar that commonly seen. Although there were vulnerabilities discovered, these were deemed to align more with policy and configuration issues, rather than the result of insecure application development standards.

After receiving and reviewing the report internally, Wellnoms prioritised remediation actions to address the necessary reported vulnerabilities. Insomnia Security completed further review work to repeat the necessary tests to confirm that any fixes put in place had correctly resolved the relevant issues.

At the completion of the review, it was concluded that the portions of the system that are externally facing are considered to be sufficiently secure to meet the business requirements for security.


Signed by a duly authorised delegate of Insomnia Security Group Ltd.

Signature: Brett Moore  
Brett Moore  
Managing Director

---

INSOMNIA SECURITY  
www.insomniasec.com

# Independent Penetration Testing - Record - WRM Version 3.4.5, May 2019

<b>Date</b>	9 May 2019
<b>Tester</b>	Phew Cyber Security L:td
<b>Product</b>	WRM
<b>Version</b>	WRM 3.4.5 Web Application and API Testing
<b>Tested Components</b>	<ul style="list-style-type: none"><li>• Web portal/application</li><li>• Web server API</li><li>• Windows client application</li></ul>
<b>Server</b>	Windows server 2008 R2 Standard
<b>Testing Frameworks, References</b>	<ul style="list-style-type: none"><li>• OWASP ASVS v4 on Level-1</li><li>• OWASP Testing Guide v4</li><li>• OSSTM</li><li>• OWASP Top-10</li><li>• CWE/SANS Top-25</li></ul>
<b>Testing URL</b>	<a href="http://pentest.wellnomicdemo.com">pentest.wellnomicdemo.com</a>
<b>Status at Report Date</b>	No outstanding vulnerabilities of any type for tested version at tested URL as at reporting date 



Click on link below to download PDF.

phew Wellnomics WRM Pen-...

# DEPLOYMENT & HOSTING - Records - External

This section contains records of completed processes done in compliance with Wellnomics policies and procedures.

## Externally available records

The below records are those that are available for public review. Note that for confidentiality reasons there may be no records that can be made available for public review.

## Internal only records

The below records are internal only, but can be reviewed and accessed for auditing purposes.

- [Windows Server OS/IIS/SQL Hardening Checklists - Completed Records](#)
  - [Windows Server OS Checklists - Completed](#)
    - [Windows Server OS Hardening Checklist - Azure US \(23/09/20\)](#)
    - [Windows Server OS Hardening Checklist - Azure EU \(23/09/20\)](#)
    - [Windows Server OS Hardening Checklist - Azure AU \(23/09/20\)](#)
    - [Windows Server OS Hardening Checklist - Azure INTEL \(23/09/20\)](#)
    - [Windows Server OS Hardening Checklist - AMER-WEB-1 \(11/04/23\)](#)
    - [Windows Server OS Hardening Checklist - AMER-WEB-4 \(11/04/23\)](#)
    - [Windows Server OS Hardening Checklist - APAC-WEB-1 \(11/04/23\)](#)
    - [Windows Server OS Hardening Checklist - EU-WEB-1 \(11/04/23\)](#)
    - [Windows Server OS Hardening Checklist - AMER-DB-1 \(11/04/23\)](#)
    - [Windows Server OS Hardening Checklist - APAC-DB-1 \(11/04/23\)](#)
    - [Windows Server OS Hardening Checklist - EU-DB-1 \(11/04/23\)](#)
  - [SQL Server Hardening Checklists - Completed](#)
    - [SQL Server Hardening Checklist - Azure US \(23/09/20\)](#)
    - [SQL Server Hardening Checklist - Azure EU \(23/09/20\)](#)
    - [SQL Server Hardening Checklist - Azure AU \(23/09/20\)](#)
    - [SQL Server Hardening Checklist - Azure INTEL \(23/09/20\)](#)
  - [IIS 8/8.5 Server Hardening Checklists - Completed](#)
    - [IIS 8/8.5 Server Hardening Checklist - Azure US \(23/08/20\)](#)
    - [IIS 8/8.5 Server Hardening Checklist - Azure EU \(23/08/20\)](#)
    - [IIS 8/8.5 Server Hardening Checklist - Azure AU \(23/08/20\)](#)
    - [IIS 8/8.5 Server Hardening Checklist - Azure INTEL \(23/08/20\)](#)
- [Disaster Recovery & Business Recovery - Hosting - Records](#)
  - [Disaster Recovery & Business Recovery Test - Hosting - Record \(Dec 2022\)](#)

# INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Records - External

This section contains records of completed processes done in compliance with Wellnomics policies and procedures.

## Externally available records

The below records are those that are available for public review. Note that for confidentiality reasons there may be no records that can be made available for public review.

## Internal only records

The below records are internal only, but can be reviewed and accessed for auditing purposes.

- Risk Assessments - Internal - Completed Records
  - VoIPline Risk Assessment - Nov 2020
  - Company Risk Assessment - July 2020
  - Company Risk Assessment - June 2019
  - Company Risk Assessment - 5th May 2017
  - Company Risk Assessment: 6th October 2016
- Employee Leaving Checklist - Records
  - Employee Leaving Checklist - Mark Garcia (Oct 2022)
  - Employee Leaving Checklist - Mitchell Denton (Oct 2022)
  - Employee Leaving Checklist - Pramod Mani (Mar 2022)
  - Employee Leaving Checklist - Tristan Irons (Mar 2022)
  - Employee Leaving Checklist - Angeli Arino (Jun 2021)
  - Employee Leaving Checklist - Chris Mackay (Mar 2021)
  - Employee Leaving Checklist - Till Peters (Dec 2020)
  - Employee Leaving Checklist - Tony Galbraith (Nov 2017)
  - Employee Leaving Checklist - Anna T Taylor (Oct 2017)
- Business Continuity Plan - Auditing and Testing Records
- Equipment De-Commissioning - Completed Records
  - Equipment Decommission Form 23 Sep 2021
  - Equipment De-commissioning Form - 19th April 2021
  - Equipment De-Commission Form - HDD March 2021(1)
  - Equipment De-commission Form - HDD, March 2021 (2)
  - Equipment De-Commission Form - HDD March 2021(3)
  - Equipment De-commissioning Form - 7 July 2017
  - Equipment De-commissioning Form - 7th March 2017
- Authorizations Review Record
- Security & Privacy Training - Employees & Contractors - Records
- Disaster Recovery and Business Continuity - Testing Records



# Summary of COMPLETED RECORDS - INTERNAL - Due Diligence Checklists and Templates, etc

Below is a list of completed records for material that cannot be shared publicly due to confidentiality and security reasons. These records are accessible internally for auditing purposes and some may be provided on request if needed.

## COMPLETED RECORDS - INTERNAL - Due Diligence Checklists and Templates

- **PRODUCT & SOFTWARE DEVELOPMENT - Completed Records - Internal**
  - **Product Security Risk Assessments - Completed Records**
    - Product Security Risk Assessment - Gadget (Aug 2022)
    - Product Security Risk Assessment - App (Mar 2021)
    - Product Security Risk Assessment - SaaS (Sep 2020)
  - **Third Party Components Review - Records**
    - Third Party Components Review - SaaS 4.14.0 (Nov 2022)
    - Third Party Components Review - SaaS 4.13.0 (May 2022)
    - Third Party Components Review - App 1.3.1 (Dec 2021)
    - Third Party Components Review - WPC 5.5.9 (Dec 2021)
    - Third Party Components Review - WPC 5.5.7 (Dec 2021)
    - Third Party Components Review - SaaS 4.1.0 (Sep 2020)
  - **Static Analysis Security Testing (SAST) - Records**
    - SAST Record - SaaS 4.15.0 (Jan 2023)
    - SAST Record - SaaS 4.11.0 (May 2022)
    - SAST Record - SaaS 4.5.0 (Jul 2021)
  - **Dynamic Analysis Security Testing (DAST) - Records**
    - DAST Record - SaaS 4.14.0 (Nov 2022)
    - DAST Record - SaaS 4.12.0 (Nov 2022)
    - DAST Record - SaaS 4.5.0 (May 2021)
  - **Software Development Lifecycle - Records**
  - **Penetration Testing - Independent - Records**
    - Penetration Testing - Independent - SaaS 4.12.0 (Jul 2022)
    - Penetration Testing - Independent - SaaS 4.5.0 Regression (Jul 2021)
    - Penetration Testing - Independent - SaaS 4.5.0 (May 2021)
  - **Product Security and Internal Penetration Testing - Records**
    - Security Testing - Record - WPC 5.5.5 (Nov 2020)
    - Security Testing - Record - WPC 5.5.7 (Nov 2020)
    - Penetration Testing - Internal - Record - WRM 3.3 (Oct 2017)
    - Penetration Testing - Internal - Record - WRM 3.2/3.3 (Apr 2017)
- **DEPLOYMENT & HOSTING - Completed Records - Internal**
  - **Windows Server OS/IIS/SQL Hardening Checklists - Completed Records**
    - **Windows Server OS Checklists - Completed**
      - Windows Server OS Hardening Checklist - Azure US (23/09/20)
      - Windows Server OS Hardening Checklist - Azure EU (23/09/20)
      - Windows Server OS Hardening Checklist - Azure AU (23/09/20)
      - Windows Server OS Hardening Checklist - Azure INTEL (23/09/20)
      - Windows Server OS Hardening Checklist - AMER-WEB-1 (11/04/23)
      - Windows Server OS Hardening Checklist - AMER-WEB-4 (11/04/23)
      - Windows Server OS Hardening Checklist - APAC-WEB-1 (11/04/23)
      - Windows Server OS Hardening Checklist - EU-WEB-1 (11/04/23)
      - Windows Server OS Hardening Checklist - AMER-DB-1 (11/04/23)
      - Windows Server OS Hardening Checklist - APAC-DB-1 (11/04/23)
      - Windows Server OS Hardening Checklist - EU-DB-1 (11/04/23)

- SQL Server Hardening Checklists - Completed
  - SQL Server Hardening Checklist - Azure US (23/09/20)
  - SQL Server Hardening Checklist - Azure EU (23/09/20)
  - SQL Server Hardening Checklist - Azure AU (23/09/20)
  - SQL Server Hardening Checklist - Azure INTEL (23/09/20)
- IIS 8/8.5 Server Hardening Checklists - Completed
  - IIS 8/8.5 Server Hardening Checklist - Azure US (23/08/20)
  - IIS 8/8.5 Server Hardening Checklist - Azure EU (23/08/20)
  - IIS 8/8.5 Server Hardening Checklist - Azure AU (23/08/20)
  - IIS 8/8.5 Server Hardening Checklist - Azure INTEL (23/08/20)
- Disaster Recovery & Business Recovery - Hosting - Records
  - Disaster Recovery & Business Recovery Test - Hosting - Record (Dec 2022)
- INTERNAL SECURITY, EMPLOYEES & CONTRACTORS - Completed Records - Internal
  - Risk Assessments - Internal - Completed Records
    - VoIPline Risk Assessment - Nov 2020
    - Company Risk Assessment - July 2020
    - Company Risk Assessment - June 2019
    - Company Risk Assessment - 5th May 2017
    - Company Risk Assessment: 6th October 2016
  - Employee Leaving Checklist - Records
    - Employee Leaving Checklist - Mark Garcia (Oct 2022)
    - Employee Leaving Checklist - Mitchell Denton (Oct 2022)
    - Employee Leaving Checklist - Pramod Mani (Mar 2022)
    - Employee Leaving Checklist - Tristan Irons (Mar 2022)
    - Employee Leaving Checklist - Angeli Arino (Jun 2021)
    - Employee Leaving Checklist - Chris Mackay (Mar 2021)
    - Employee Leaving Checklist - Till Peters (Dec 2020)
    - Employee Leaving Checklist - Tony Galbraith (Nov 2017)
    - Employee Leaving Checklist - Anna T Taylor (Oct 2017)
  - Business Continuity Plan - Auditing and Testing Records
  - Equipment De-Commissioning - Completed Records
    - Equipment Decommission Form 23 Sep 2021
    - Equipment De-commissioning Form - 19th April 2021
    - Equipment De-Commission Form - HDD March 2021(1)
    - Equipment De-commission Form - HDD, March 2021 (2)
    - Equipment De-Commission Form - HDD March 2021(3)
    - Equipment De-commissioning Form - 7 July 2017
    - Equipment De-commissioning Form - 7th March 2017
  - Authorizations Review Record
  - Security & Privacy Training - Employees & Contractors - Records
  - Disaster Recovery and Business Continuity - Testing Records