## POLICY

This policy defines the mandatory minimum information security requirements for the Wellwise Group, and acts as an umbrella document to all other information security procedures and associated standards. This policy defines the responsibility to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets
- manage the risk of security exposure or compromise
- assure a secure and stable information technology (IT) environment
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure
- monitor systems for anomalies that might indicate compromise
- promote and increase the awareness of information security

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions; compromise data; and result in legal and regulatory non-compliance.

This policy defines a framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.

## PROCEDURE

### A Purpose and Scope

This policy encompasses all systems, automated and manual, for which the Wellwise Group has administrative responsibility. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

### B Responsibility

**The CEO is responsible for**

- identifying information security risks and responsibilities, supporting information, security policies and standards.

**The QHSE Advisor is responsible for:**

- Implementing information security policies and promoting awareness and best practices and determining the appropriate levels of protection for that information.
- Participating in the response to security incidents
- Complying with notifications requirements in the event of a breach of private information
- Implementing business continuity and disaster recovery plans

**Strident (our third-party IT Consultants) will be responsible for:**

- providing expertise as security consultants as needed
- monitoring networks for anomalies
- monitoring external sources for indications of data breaches, defacements, etc.
- providing timely notification of current threats and vulnerabilities
- providing training to their appropriate technical staff on secure operations (e.g., secure coding, secure configuration)

**All WWG employees will be responsible for:**

- understanding the basic information security controls necessary to protect the confidentiality, integrity and availability of information entrusted
- protecting information and resources from unauthorized use or disclosure
- protecting personal, private, sensitive information from unauthorized use or disclosure
- reporting suspected information security incidents or weaknesses to the QHSE Advisor and/or CEO for investigation.
- Undertake any in-house training as deemed necessary by management

## C Definitions

**WWG** Wellwise Group
**GDPR** General Data Protection Regulations
**Strident** Strident Technology, IT Consultants employed by Wellwise Group

## D Related Documents

P026 Audit Procedure
P030 Document Control Procedure
P040 Privacy Policy
P068 Non-Conformance Procedure
P105 IT Asset Management Procedure
P118 Business Continuity Plan
P120 Cyber Security Framework
RA044 Data Security and Privacy Risk Assessment

## E Overview and Controls

### E.1 Organisational Security

Technical information security function is outsourced to Strident a third-party company, Wellwise Group retains overall responsibility for the security of the information that it owns.

## E.2 Separation of Duties

a. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility is implemented where appropriate, especially in accounting functions.

b. Whenever separation of duties is not technically feasible, other compensatory controls are implemented, such as monitoring of activities, audit trails and management supervision.

## E.3 Information Risk Management

a. Wellwise Group are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.

b. Risk assessment results, and the decisions made based on these results, will be documented, e.g. RA044 Data Security and Privacy Risk Assessment.

## E.4 Information Classification and Handling

a. All information, which is created, acquired or used in support of business activities, will only be used for its intended business purpose.

b. Information will be properly managed from its creation, through authorized use, to proper disposal. See P066 Control of Records and P030 Document Control Procedure.

c. All information will be classified where appropriate on an ongoing basis based on its confidentiality, integrity and availability characteristics necessitated by its data content.

d. An electronic inventory of all IT assets will be maintained in the Wellwise Group SAM Database. I:QHSE/Document Control/SAM

e. Content made available to the general public via company websites will be reviewed, defined and approved by Wellwise Group management.

f. Personal Data shared with Clients will be controlled via the GDPR legislation. See P040 Privacy Policy and RA044 Data Security and Privacy Risk Assessment, for further details. Large amounts of personal data are not sent at once (separate emails). When emailing sensitive information such as passports/ethnicity/financial information the recipient email is double checked to ensure it is correct. Staff are trained not to give out personal or confidential information over the telephone/email unless they can verify the caller. Contractors can only access their own personal data on the company website via a unique username and password.

## E.5 IT Asset Management

a. Wellwise Group maintains an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. See Software Asset Management Database I:QHSE/Document Control/SAM, and P105 IT Asset Management (for the purchasing and selling of IT hardware and software).

b. Strident also have their own dashboard listing our IT Equipment and software versions which we can call on at any time. These are cross matched for accuracy at regular intervals by the QHSE Advisor.

c. All our servers have a 5-year manufacturer's warranty. After five years we will either extend the warranty for a further year or replace the hardware. The manufacturer warranty gives a next day SLA for a hardware failure. Strident provide a 4-hour SLA for all critical outages, ie Server off-line. However, five of a total of eight servers are now virtual.

## E.6 Personnel Security Awareness

a. All employees will receive general information security awareness training, to include recognizing and reporting threats.

b. All employees will sign the company's Privacy Policy, and a signed copy will be filed in their personal file. See P040 Privacy Policy and Declaration for further details.

c. All Wellwise Contractors will also sign a Privacy Policy Declaration before their first job, and this will be recorded in the Contractor Database (CBD) and will be controlled via the "Contractor Status Report", which records the date the signed declaration was returned.

d. All job positions have been evaluated by the CEO and deemed to require access to sensitive information and/sensitive information technology assets. Wellwise Group is a small company employing only 8 staff and accordingly security can be adequately controlled.

e. Wellwise Group will ensure that all issued property is returned prior to an employee leaving the company, and email accounts are disabled, and access is removed immediately upon termination of employment.

f. Wellwise will ensure all Contractors are formally inactivated or deactivated when they are no longer working for the company. See F133 Admin Checklist for Inactivating or Deactivating Contractors, which will remove their access to the company website log in area and hide/remove their personal data from our database. Similarly, Client contacts are controlled using F183 Admin Checklist for deactivating Client Contacts.

## E.7 Cyber Incident Management

a. Wellwise Group have an incident response plan to effectively respond to security incidents. See P068 Non-Conformance Procedure.

b. All observed or suspected information security incidents or weaknesses are reported to appropriate management as quickly as possible.

*c.* Wellwise Group maintains a Cyber Security Framework (P118) to control Cyber Security Awareness, threats, confidentiality, integrity, and availability. The framework ensures our data remains protected, accurate, and exclusively accessible to authorised members. This framework is reviewed annually for suitability and relevance.

## E.8 Physical and Environmental Security

a. IT equipment will be physically protected from security threats and environmental hazards. A UPS is installed to protect the electricity supply to our servers.

b. Wellwise Group Broadband is provided via two dedicated leased lines with 100 mb bandwidth each, which is more than sufficient for our business use. One acts as a failover in the event of a major failure. The two lines are supplied by BT but are on different networks to add another level of protection.

c. Wellwise Group premises are protected by an ACT Entry System which only allows access using an authorised key fob. Entry and exit is monitored by the ACT Monitor. All visitors are signed in and out.

d. Visitors to the company server room, including maintenance personnel, will be escorted at all times.

## E.9 Account Management and Access Control

a. Access to systems is provided through the use of individually assigned unique identifiers, known as user-IDs.

b. Associated with each user-ID is an authentication password which is used to authenticate the identity of the person or system requesting access.

c. Automated techniques and controls are implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. (e.g. automatic screen saver).

d. MFA (Multi-functional Authentication) is set up for all employees needing remote access.

e. Building Access is controlled by an ACT Door Entry Control System which requires authorised key fobs to gain access. Key fobs are issued to all employees and date issued is recorded for control purposes. Visitors are issued with visitor badges and recorded on the ACT System accordingly. The ACT records entry and exit and is able to give an automatic print out when the fire alarm is triggered. All employees are instructed to enter and leave the building via the main door to enable this control.

f. Remote desktop connections are offered to all relevant personnel to allow them to work from home. These connections are set up by Strident and require pre-authorisation from the CEO.

## E.10 Systems Security

Systems include but are not limited to servers, websites, networks, communications, databases and software applications.

1. System security and network architecture is maintained by Strident.
2. SSL Certificates are in place protect our sensitive information such as usernames, passwords etc., and keep data secure between our servers. The certificates also encrypt our remote connections.
3. Remote access is also controlled via Active Directory and a Draytek Firewall Router.
4. All systems are developed, maintained and decommissioned in a secure manner, using bone fide contractors, ie Strident and Corvidae Solutions.
5. The purchasing and selling of all IT Assets (including software) are managed with P105 Asset Management Procedure.

## E.11 Vulnerability Management

Strident are appointed as our third-party contractors to carry out appropriate action, such as patching or updating the system, and to address discovered vulnerabilities. All the servers are updated with the latest Microsoft update as soon as possible (usually the evening that they are released, so they can reboot if required) and the hardware is monitored through our monitoring agent for example, PSU status, Temps and Raid statuses.

## E.12 Operations Security

a. Strident have the responsibility for the management of all IT Systems Security to ISO 27001 standard. Including system configurations.

b. Host based firewalls are installed and enabled on all workstations to protect from threats and to restrict access to only that which is needed.

c. ESET Anti-virus, software integrity checkers, web filtering across systems are implemented where technically feasible to prevent and detect the introduction of malicious code or other threats.

d. Controls are in place to allow only approved software to run on a system and prevent execution of all other software.

e. Systems and applications are monitored and analyzed to detect deviation from the access control requirements outlined in this policy, and record events to provide evidence and to reconstruct lost or damaged data. Our servers are not currently accessible from outside the Office without the use of a VPN and Strident use their monitoring agent to detect any breaches.

f. Wellwise employs Microsoft Defender - Trustwave Secure Email Gateway to provide total email content security through unified threat management, anti-spam, content security, policy enforcement and data loss prevention. It filters all incoming and outgoing email at the perimeter and uses deep content inspection to scan all content – even within attachments. This gives control to ensure our organization can safely exchange information without worrying about harmful data loss. See Appendix I for a list of Microsoft Defender features.

g. Microsoft Defender is configured to alert our CEO to indications of compromise or potential compromise.

h. No confidential information is left on desks out of hours, and contractor passports in transit (for Visa purposes) are locked in a fireproof safe.

i. A Privacy Policy Declaration is signed by all employees and Wellwise Contractors (P040)

j. A Business Continuity Plan (P118) with disaster recovery information for IT Systems is established and reviewed annually.

k. Strident provide an on-line nightly backup solution which encrypts and takes copies of server information, software, and system images, which are stored off-site to their Data Management Centre. Strident hold 7 days of backup offsite in their data centre in Claydon for disaster recovery purposes. Up to three years of Back-up data is also stored locally on a NAS on our premises, this is remotely accessible by Strident to enable them to restore historic data.

   Their data centre is on an isolated network protected by several firewalls in a controlled environment which is only accessible to approved Strident colleagues. They also have CCTV and key cards to access the data centre which is all logged so follows the same strict ISO 27001 polices they use at Strident on their internal network.

# Appendix 1

## Microsoft Defender Features

| | |
|---|---|
| • Access Control Management<br>• Advanced Threat Protection<br>• Anti-Malware<br>• Anti-Spam<br>• Anti-Virus<br>• Audit, Analysis and Compliance<br>• Breach Detection<br>• Content Filtering<br>• Data Destruction<br>• Data Loss Prevention<br>• Data Recovery<br>• Database Activity Monitoring<br>• Device Control<br>• Digital rights management (DRM)<br>• Email Encryption<br>• End-user awareness and training<br>• Endpoint Detection and Response<br>• Endpoint Protection Platform<br>• File Access Auditing<br>• File Encryption | • Mobile Forensics<br>• Network Access Control<br>• Network Security, Firewall and Packet Analyzers<br>• Password Management<br>• Patch Management<br>• Penetration Testing<br>• Physical Security<br>• Proximity Readers<br>• Public Key Infrastructure (PKI)<br>• SIEM, Log Management<br>• Single Sign-on<br>• Threat Protection<br>• Unified Threat Management (UTM)<br>• User Monitoring<br>• Virtual Private Network (VPN)<br>• Vulnerability Scanners |

| | |
|---|---|
| • Identity Management<br>• Intrusion Detection and Prevention (IDS/IPS) | |