IT SECURITY POLICY

Version 8.1

Date of publication: 24th February 2026

Date of Review: February 2026

Next scheduled Review: June 2027

Version	Date	Author	Reviewed By	Approved By	Description of Change
8	24/2/26	JW	KOR	K O'Reilly	New Version

Index

1.0. Responsibilities....3
2.0. Definitions....4
3.0. Associated Documents....6
4.0. Acceptable Use of Assets Policy....6
5.0. Access Control Policy....8
6.0. Backup Policy....12
7.0. Clear Desk and Clear Screen Policy....13
8.0. Cryptographic Controls Policy....14
9.0. Information Classification, Labelling and Handling Policy....15
10.0. Mobile Devices Policy....16
11.0. Physical and Environmental Security Policy....18
12.0. Protection from Malware Policy....20
13.0. Removable Media....22
14.0. Protection of Personal Information Policy....22
15.0. Suppliers Policy....31
16.0. Teleworking Policy....32
17.0. Use of Software Policy....35
18.0. Network Policy....35
19.0. Physical Media....35
20.0. Vulnerability Management....36
21.0. Policy Review....36

1.0. Responsibilities

1.0. It is the responsibility of the Operations Director to ensure that this policy is implemented and that any resources required are made available.

1.1. It is the responsibility of the Operations Director to monitor the effectiveness of this policy and report the results at management reviews.

1.2. It is the responsibility of the Operations Director to create and maintain an **Asset and Risk Assessment Register** and to ensure all assets that need to be covered by this policy are identified.

1.3. It is the responsibility of all employees and subcontractors, and employees and subcontractors of information security critical suppliers, to adhere to this policy and report to the Operations Director any issues they may be aware of that breach any of its contents.

2.0. Definitions

2.0. **Anti-virus software**: Software used to prevent, detect and remove malware. Anti-virus can also mean anti-malware and/or anti-spyware.

2.1. **Asset**: Any physical entity that can affect the confidentiality, availability and integrity of the organisation's information assets.

2.2. **Availability**: The accessibility and usability of an information asset upon demand by an authorised entity.

2.3. **Automated decision making:** Processing of information that results in decisions being made about Information Subjects without any review of the information being made by an individual.

2.4. **Beyond use**: Controls placed on Personal Information that it is no longer necessary for One Resourcing to keep where it is not reasonably feasible to delete the information. These controls must comply with guidance from the Information Commissioner's Office (see **Information Commissioner's Office Guidance on GDPR Compliance**).

2.5. **Computer systems**: A system of one or more computers and associated software, often with common storage, including servers, workstations, laptops, storage and networking equipment.

2.6. **Confidential information**: Any type of information that has been specified by the organisation's **Information Classification, Labelling and Handling Policy** as requiring protection through the application of cryptographic controls when it is stored or transferred electronically.

2.7. **Confidentiality**: The restrictions placed on the access or disclosure of an information asset.

2.8. **Controller:** A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of a set of Personal Information.

2.9. **Electronic communication facilities (ECF)**: Any asset that can be used to electronically transfer information.

2.10. **Electronic messages**: The electronic transfer of information by means such as email, texts, blogs, message boards and instant messaging.

2.11. **Equipment**: Any asset that can be used to electronically store and/or process information.

2.12. **High risk processing:** Processing of Personal Information (in particular using new technologies) that is likely to result in a high risk to the rights and freedoms of Information Subjects (see **Information Commissioner's Office Guidance on GDPR Compliance**).

2.13. **Identifiable Natural Person:** A natural person who can be identified directly or indirectly, in particular with 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 person.

2.14. **Information asset**: Any information that has value to the organisation's stakeholders and requires protection.

2.15. **Information processing facility (IPF)**: Any network of assets that can be used to electronically store, process or transmit information.

2.16. **Information security critical supplier (ISCS)**: Any supplier of goods or services that as part of their scope of supply will potentially have unsupervised access to any of the organisation's premises**,** access to the one or more of the organisation's information assets**,** or provides software or hardware used in the organisation's information processing facilities or electronic communication facilities.

2.17. **Information security incident**: Any event that has a potentially negative impact on the confidentiality and/or integrity and/or availability of an information asset.

2.18. **Information subject**: An Identifiable Natural Person who has Personal Information that One Resourcing is the Controller of or is a Processor of on behalf of a Controller.

2.19. **Integrity**: The accuracy and completeness of an information asset.

2.20. **Mail serve**r: A system based on software and hardware that sends, receives and stores electronic mail.

2.21. **Malware**: Malicious software, such as viruses, trojans, worms, spyware, adware, macros, mail bombs and rootkits which are specifically designed to disrupt or damage a computer system.

2.22. **Mobile device**: Laptop computers, tablet computers, smart telephones, mobile telephones and any other handheld or portable devices capable of processing or transmitting information.

2.23. **Operating facility**: Any physical location containing assets owned by the organisation that the organisation controls, including buildings, offices, departments and locations affiliated with the organisation that are used to create, access, store or process any of the organisation's information assets.

2.24. **Personal Information**: Any information relating to an Identifiable Natural Person.

2.25. **Personal Information protection principles**: Principles that shall be applied in relation to all Personal Information as laid down in the Data Protection Act 2018, the General Data Protection Regulation (EU 2016/679) and any subsequent amendments.

2.26. **Processor:** A natural or legal person, public authority, agency or other body which processes Personal information on behalf of a Controller.

2.27. **Remote users**: Users accessing the organisation's assets at locations other than its operating facilities, such as home offices, shared locations, hotels and where users are travelling, including standalone access and remote connections to the organisation's information processing facilities.

2.28. **Restricted access**: Any physical location where access is restricted to named personnel only.

2.29. **Software**: All programs and operating information used by equipment, including those being developed in accordance with the customer's requirements for the user.

2.30. **Supply of goods and services agreement**: A legally binding contract between the organisation and a supplier for the supply of a defined scope of goods and services.

2.31. **Teleworker**: Any person that undertakes teleworking on behalf of the organisation.

2.32. **Teleworking**: The access, processing and storage of information assets at locations that are not under the control of the organisation.

2.33. **User**: An individual or organisation that uses one or more of the organisation's assets, including software once it is post-General Availability (GA).

2.34. **Visual aids**: Any asset used to display information to the occupants of a room.

3.0. Associated Documents

3.0. All associated documents referred to in this policy are highlighted in bold and underlined.

4.0. Acceptable Use of Assets Policy

4.0. **This sub-policy specifies the controls that need to be applied to:**

4.0.1. Authorise the use of any asset owned by, or under the control of, the organisation; and

4.0.2. Minimise the risks to information security arising from the misuse or unauthorised use of the organisation's assets.

4.1. **Use of Software and applications**

8.1.1. Users are not permitted to use software or applications that would overide, bypass or remove any of the technical controls put in place as part of the organisation's BMS
8.1.2 User must follow guidance and training when using applications and software and only use them as intend and instructed.
8.1.3.

4.2. **Use of electronic communication facilities (ECFs)**

4.2.1. All users of ECFs must be authorised to do so in accordance with the organisation's **Access Control Policy**.

4.2.2. Users must only use assets to access and transfer information for which they have been authorised in accordance with the **Access Control Policy** and the **Information Classification, Labelling and Handling Policy**.

4.2.3. Users must apply extreme caution when opening email attachments received from unknown senders. If in doubt, please ask the Operations Director for advice.

4.2.4. Users must not:

- Disclose user IDs and personal passwords which give access to the organisation's assets unless authorised by the Operation Director;
- Allow any third party to access the organisation's ECFs;

- Use any access method other than the method provided to them by the organisation;
- Deliberately cause damage to any of the organisation's ECFs, including maliciously deleting, corrupting or restricting access to the data contained therein;
- Deliberately introduce viruses or other harmful sources of malware into the organisation's ECFs;
- Deliberately access external sources that are not authorised and not related to the organisation's activities;
- Knowingly access, download or store materials from the internet that are illegal, immoral, unethical or deemed to be indecent or gross in nature;
- Send unsolicited, unauthorised or illegal materials to any internal or external recipient;
- Install, modify, delete or remove software in a way that contravenes the **Use of Software Policy**;
- Download any electronic files whose size exceeds any guidance provided by the Operations Director;
- Assist or create a potential security breach or disruption to the organisation's ECFs in any way;
- Use any ECFs for any personal reasons, other than those authorised by the organisation.

4.2.5. Any user supplied equipment must be approved by the Operations Director for connection to any of the organisation's ECFs.

4.2.6. The organisation reserves the right to monitor the use of all ECFs.

5.0. Access Control Policy

5.0. This sub-policy specifies the access controls that need to be applied to all information assets that contain information held by the organisation.

5.1. **Access to the information assets, operating facilities and information processing facilities**

5.1.1. Access to information assets, operating facilities and information processing facilities must only be provided to individuals who need it to complete tasks specified in their **Job Description** or as instructed by a Director of the organisation.

5.1.2. All user access must be attributed to an identifiable person.

5.1.3. All unsupervised access to information assets, operating facilities and information processing facilities must be authorised by the person specified in, and recorded on, the **Access Control Register**.

5.1.4. The Operations Director is responsible for:

- Ensuring no single person can access, modify or use the organisation's assets without authorisation or detection;
- Authorising and recording the use of any software that might be capable of overriding this sub-policy;
- Authorising and recording access to any software source codes;
- Authorising and recording individual user access to information processing facilities, electronic communication facilities, mobile devices, operating facilities and restricted access areas using an **Asset and Access Control Review Form**;
- Ensuring that individuals who enable and disable access to an organisation asset do not have access to any software that monitors the use of the asset;
- Ensuring that the access control for specific assets and information processing facilities meets the security requirements of each information asset owner;
- Regularly reviewing the logs of system administrator access and actions.

5.2. **Control of access to information processing facilities**

5.2.1. The Human Resources Manager is responsible for:

- Arranging access with the IT Supplier as part of the induction of new starters, and as part of any role changes within the organisation;
- Arranging the removal of access by notifying the IT Supplier of leavers from the organisation and as part of any role changes;
- Ensuring access to any asset is not provided to an individual who has not received formal training in the **Information Security Policy**;

- Ensuring individual access privileges are reviewed upon a change of role or change in responsibilities;
- Recording the status of each user's access privileges in the **Access Control Register**;
- Ensuring redundant user access IDs are not issued to other users;
- Ensuring the immediate removal of all access rights of a user upon termination of their **Employment Contract** or **Supply of Goods and Services Agreement**, or in the event of a security incident that relates to their access rights.

5.2.2. The IT Supplier is responsible for:

- Responding in a timely manner to requests for the activation and deactivation of user account access made to them by the Human Resources Manager;
- Configuring and reviewing user access to the organisation's assets and information processing facilities as specified in the **Access Control Register**;
- Removing any expired or unused accounts;
- Testing that deactivated, deleted and removed accounts are no longer accessible;
- Implementing access control systems and mechanisms for the organisation's assets and information processing facilities as directed by the Operations Director;
- Logging and monitoring all access to the organisation's assets and information processing facilities and providing access logs where requested to do so;
- Ensuring that access log files cannot be edited or deleted.

5.2.3. Any password rules and user security controls implemented must satisfy the following criteria:

- Passwords must be at least 12 characters in length;
- Passwords must be a combination of Uppercase, Lowercase, Numbers and symbols;
- Historic passwords cannot be repeated;
- Users must be asked to change their passwords on initial access or if access needs to be re-established for any reason;
- Passwords must be obscured on any access point that displays them, typically marked with an asterisk;
- Password files or data must be stored in encrypted secure areas and encrypted whilst transferred;

- All displays must have a timeout of 5 minutes or less where the user is prompted to enter a password to access the system.

5.2.4. The IT Supplier is responsible for:

- Granting permanent or temporary access to restricted areas;
- Reviewing access to restricted areas every 12 months and authorising changes where required;
- Leading and providing support to incident investigations where required.

5.2.5. All access requests to restricted areas must be made in writing and, as a minimum, include the following information:

- Reason for access;
- Areas of access required;
- Start and finish date (if permanent please state this);
- Line manager's approval (in writing);
- Any specific requirements, including restrictions and limitations of access.

5.3. **Access to remote users**

5.3.1. All users must adhere to the **Physical and Environmental Security Policy**, **Mobile Devices Policy** and **Acceptable Use of Assets Policy** when using the organisation's assets in remote locations.

5.3.2. Remote access to the organisation's network and information processing facilities must:

- Only be provided to authorised users;
- Only be used with approved assets, in accordance with the **Acceptable Use of Assets Policy**, **Teleworking Policy** and **Mobile Devices Policy**;
- Be set to timeout after 15 miniutes of inactivity;
- Log events and attempted logins

5.4. **Access to the organisation's operating facilities**

5.4.1. Access to the organisation's operating facilities must be authorised by Operations Director.

5.4.2. Access to the organisation's operating facilities will be processed and granted by the Operations Director.

5.4.3. Access controls must be implemented at all the organisation's operating facilities and must be:

- Appropriate and proportionate to the area under control;
- Updated at set intervals to prevent the transfer of access methods to unauthorised persons and third parties;
- Monitored and logged for security purposes.

5.4.4. All employees are responsible for:

- Strictly adhering to the access controls for each location;
- Not tailgating or allowing tailgating through any secure access door;
- Not forcibly opening doors and other access controls;
- Not deliberately holding open a controlled access door by wedging, latching or placing an item against it;
- Promptly reporting any problems relating to access controls to their manager;
- Accompanying visitors that are in their care at all times, and not allowing them to enter any unauthorised location;
- Immediately reporting to their manager and challenging, if confident and safe to do so, any person who is suspected of being in an area that they are not authorised to be in.

5.4.5. Authorisation must be granted to hold open a controlled access door for longer than the time required for an individual to enter or exit the area.

5.5. **Visitors and suppliers**

5.5.1. All visitors accessing non-public areas must:

- Sign in at reception;
- Be accompanied by a member of the organisation's staff at all times;
- Not be allowed access to any restricted areas without the relevant authorisation to do so;
- Not attempt to access any of the organisation's assets and information processing facilities or view any of the organisation's information without authorisation to do so.

5.5.2. All suppliers working in an operating facility must:

- Sign in at reception;
- Be managed and approved in accordance with the **Suppliers Policy**;
- Be appropriately inducted into the organisation by the relevant authority;
- Not access areas other than those identified as appropriate to perform the contracted tasks;
- Immediately report any accidental breaches of this policy to the Operations Director;
- Not access or view any information that has not been provided as part of the contracted task.

5.6. **Remote access to customer networks**

5.6.1. At present the organisation do not provide any services that require them to access customer networks directly.

6.0. Backup Policy

6.0. This sub-policy specifies the controls that need to be applied to ensure that copies of all software and information assets stored using electronic media, are taken and held so that the risk to their confidentiality, availability and integrity is minimised.

6.1. **Software**

6.1.1. Backup copies of all software, including previous versions, must be made prior to their first use, stored by Kingfisher system and retained for 6 months. The backup copies made must ensure that all information assets that require the use of software can be accessed, processed and distributed with minimal disruption.

6.1.2. Backups must be made in accordance with the **business continuity plan**.

6.2. **Electronic files**

6.2.1. Backup copies of all electronic files that contain information assets, including previous versions, must be made daily, stored at the data centre of backup provider and retained for 6 Months.

6.2.2. All backup copies of electronic files must be encrypted in accordance with the **Use of Cryptographic Controls Policy**.

6.2.3. All users must ensure that all electronic files are stored on the organisation's information processing facilities.

6.3. **Storage of backups**

6.3.1. The backup copies should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.

6.3.2. The backup information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site.

6.3.3. Any third parties used to store and maintain backups should comply with the **Suppliers Policy**.

6.4. **Testing of backups**

6.4.1. Backups of software and electronic files, and media used to store them, must be tested at least twice a year in accordance with the **Business Continuity Plan** and the **Electronic Data Backup Register**.

7.0. Clear Desk and Clear Screen Policy

7.0. This sub-policy specifies the controls that need to be applied to minimise the risks to information security arising from unauthorised access to the organisation's information assets located on desks, visual aids and display screens.

7.1. **Paper assets, visual aids and portable storage media**

7.1.1. Information assets held on paper or portable storage media must be stored in cabinets and/or drawers, in accordance with the **Information Classification, Labelling and Handling Policy**, when not in immediate use and whenever the room they are being used in is vacated unless the room is vacated in accordance with the **Fire Evacuation Procedure**.

7.1.2. All information assets stored on visual aids should be removed from display immediately after used and before vacating the room in which they are held.

7.2. **Display screens**

7.2.1. Equipment that utilises display screens must have a screensaver enabled with password protection that activates automatically after 5 minutes of inactivity.

7.2.2. Users of equipment that utilises display screens must enable a screensaver whenever they leave the room in which they are held.

7.3. **Reproduction devices (printers, photocopiers and scanners)**

7.3.1. Media used, or created using reproduction devices, must be removed from them immediately after use.

8.0. Cryptographic Controls Policy

8.0. This sub-policy specifies the cryptographic controls that must be applied to confidential information.

8.1. **General principles**

8.1.1. The organisation's computer systems and information processing facilities must be appropriately protected to prevent unauthorised access by applying a level of encryption to sensitive or critical information which is proportionate to the level of business risk.

8.1.2. All confidential information transferred outside of the organisation must be encrypted prior to transfer.

8.1.3. All removable media, including memory sticks, must be encrypted.

8.1.4. Mobile device hard drives must be encrypted.

8.1.5. Mobile devices must be protected by passwords or PIN codes.

8.1.6. Emails must be encrypted whenever confidential information is contained or attached.

8.1.7. Attachments to emails must be encrypted whenever confidential information is contained.

8.1.8. The use of encryption must comply with all legislative requirements.

8.2. **Encryption of data in transit**

8.2.1. Confidential information in transit must always be encrypted. Data which is already in the public domain, or would be of no adverse significance if it were to be so, may be sent unencrypted.

8.3. **Key management**

8.3.1. Software used for encryption will be provided by outsourced IT supplier with the necessary competencies and they shall be responsible for the management of keys.

8.4. **Encryption for information transferred outside the UK**

8.4.1. Regulatory controls for any country outside the UK to which data is exported should be checked to ensure that cryptographic legislation will not be contravened.

8.5. **Avoiding adverse impacts from encryption**

8.5.1. Encryption keys must be stored such that all information encrypted by the organisation can be decrypted if required.

8.5.2. Access to encryption keys must be controlled as per the **Access Control Policy**.

8.5.3. The persons with access to encryption keys must be recorded in the **Access Control Register**.

9.0. Information Classification, Labelling and Handling Policy

9.0. This sub-policy specifies the labelling, storage, copying and distribution controls that need to be applied to all information assets that are processed and stored by the organisation.

9.1. **Classification**

9.1.1. It is the responsibility of the Operations Director to maintain the Information Classification, Labelling and Handling Rules contained in the **Control of Documented Information Procedure** to ensure that:

- Information assets can be easily classified and that classification considers their value, criticality, legal requirements and sensitivity to unauthorised disclosure or modification;
- The rules can be applied practically by all information asset owners, employees and third parties with whom the organisation exchanges or provides access to information assets.

9.2. **Labelling**

9.2.1. Upon creation or receipt from a third party, all information assets must be labelled in accordance with the **Control of Documented Information Procedure (Appendix C)**.

9.2.2. Whenever an information asset is modified, consideration must be given as to whether the labelling applied to it should be changed.

9.3. **Copying**

9.3.1. The copying of all information assets should be avoided wherever possible. Where copying is necessary (i.e. to comply with the **Backup Policy**), copying must be done in accordance with **Control of Documented Information Procedure (Appendix C)**.

9.4. **Distribution**

9.4.1. Information assets should only be distributed:

- To comply with client requirements;
- To comply with legal requirements;
- On a need to know basis.

9.4.2. Where distribution is necessary, it must be done in accordance with **Control of Documented Information Procedure (Appendix C)**.

9.5. **Destruction**

9.5.1. Destruction of an information asset must be done in accordance with the **Disposals Procedure**.

9.5.2. Information must be destroyed when it is no longer required.

10.0. Mobile Devices Policy

10.0. This sub-policy specifies the controls that need to be applied to:

10.0.1. Control the use of any mobile devices owned by, or under the control of, the organisation; and

10.0.2. Minimise the risks to information security arising from the misuse or unauthorised use of mobile devices.

10.1. **Issuing of mobile devices**

10.1.1. The issue of any mobile device to a user must be authorised by the Operations Director and recorded the asset register.

10.2. **Use of mobile devices**

10.2.1. All users of mobile devices must comply with all relevant sections of this policy.

10.2.2. Mobile devices must only be used in connection with authorised business use.

10.2.3. A mobile device must only be used by the user to whom it was supplied. Users must not allow a mobile device issued to them to be used by any other individuals including other employees, suppliers, friends, associates or relatives.

10.2.4. In an emergency situation, a user may allow an individual to make a supervised call from a mobile or smart telephone.

10.2.5. Users must immediately notify the Operations Director if a mobile device is known or suspected to be lost or stolen.

10.2.6. Mobile devices must not be used or stored in environments or areas where there is a reasonable risk of them becoming damaged by impact, water ingress, extreme temperatures or electromagnetic fields.

10.2.7. When not in use, mobile devices must be retained in a secure environment. This may include a lockable store cupboard with controlled access, or lockable metal cabinets.

10.2.8. When mobile devices are taken away from buildings controlled by the organisation, users must ensure that they take adequate precautions at all times to protect the equipment against theft or accidental damage.

10.2.9. When transporting mobile devices, care should be taken not to draw attention to their existence to minimise the likelihood of street crime.

10.2.10. Mobile devices should only be transported in the bags or cases with which they were supplied. Replacement bags or cases must only be obtained from the IT Supplier.

10.2.11. Mobile devices must be carried as hand luggage when travelling.

10.2.12. Mobile devices must not be left unattended at any time in a vehicle or public place.

10.2.13. Mobile devices must always be protected from unauthorised use by an access password in accordance with the **Access Control Policy**.

10.2.14. Mobile devices must not be used to store passwords, safe/door combinations, or classified, sensitive or proprietary information.

10.2.15. Mobile devices must not be used to transfer information via wireless networks that have not been approved by the Operations Director.

10.3. **Return of mobile devices**

10.3.1. Upon request by the Human Resources Manager, termination of contract or change of role, a user must return any mobile devices they have been issued with to their Manager.

10.3.2. All mobile devices must be returned to the Operations Director and recorded in the asset register.

11.0. Physical and Environmental Security Policy

11.0. This sub-policy specifies the controls that need to be applied to all operating facilities and assets located at them to:

11.0.1. Protect the organisation's assets from physical and environmental threats; and

11.0.2. Reduce the risk of damage, loss and theft to the organisation's assets; and

11.0.3. Reduce the risk of unauthorised access to the organisation's operating facilities.

11.1. **Physical protection of operating facilities**

11.1.1. Using appropriate methods, all the organisation's operating facilities must be secured at all times to prevent unauthorised access.

11.1.2. All operating facilities must be protected by an intruder alarm system that is remotely monitored by IPS Fire and Security.

11.1.3. All external windows and doors must be kept shut and locked at all times unless authorised by the operations director.

11.1.4. Cables carrying power, data or supporting information services shall be protected from interception, interference or damage

11.2. **Environmental protection of operating facilities**

11.2.1. All the environmental vulnerabilities and controls associated with the organisation's operating facilities are identified in the **Asset and Risk Assessment Register**.

11.2.2. All relevant operating facilities are protected by suitable fire alarm systems and have a fire evacuation procedure in place.

11.2.3. All systems identified as being vulnerable to power outages should be protected by uninterruptable power supplies (UPS), such as a generator or battery backup, as follows:

- Generators must have the capability to meet the requirements of the **Business Continuity Plan**;
- Battery backup must be able to provide at least 30 minutes of uptime to the systems utilising their power.

11.2.4. All systems that need to be maintained in a temperature controlled environment must be suitably located where air conditioning facilities are available that are:

- Implemented with monitoring/backup to pro-actively alert/failsafe in the event of failure;
- Adequately maintained to ensure reliability.

11.3. **Protection of assets at operating facilities**

11.3.1. All network servers must be placed in locations designated as restricted access in the **Access Control Policy**.

11.3.2. All cable/wiring locations must be appropriately secured to prevent interception of data and damage to the network infrastructure.

11.3.3. All hard copy files must be stored in cabinets in accordance with the **Clear Desk and Clear Screen Policy** and the **Information Classification, Labelling and Classification Policy**.

11.3.4. All assets must be maintained in accordance with manufacturers' and suppliers' recommendations or as identified from an **Improvement Log**. Maintenance requirements and their status will be recorded in the **Equipment and Maintenance Register**.

11.3.5. All areas designated as restricted access in the **Access Control Policy** must be clearly signposted at all entrance points to them. Entrances to these areas must be physically controlled at all times to prevent access by non-authorised personnel.

12.0. Protection from Malware Policy

12.0. This sub-policy specifies the controls that need to be applied to all computer systems and the mobile devices that can connect to the organisation's information processing facilities to protect them against malware threats from sources such as viruses and spyware applications.

12.1. **Installation of anti-virus software on computer systems and mobile devices**

12.1.1. It is the responsibility of the Operations Director to ensure that effective anti-virus software is installed and appropriately updated on all computer systems and mobile devices that have access to the organisation's information processing facilities and store and transmit information assets, regardless of whether the organisation actively manages and maintains them.

12.1.2. All computer systems and mobile devices must not be used or handed over to a user unless they have up-to-date and operational anti-virus software installed.

12.1.3. All anti-virus software installed must have real-time scanning protection to files and applications running on the computer system or mobile device. The scanning must automatically assess the threat posed by any electronic files or software code downloaded onto a computer system or mobile device.

12.1.4. All anti-virus software must be configured to ensure it can detect, remove and protect against all known types of malware.

12.1.5. All anti-virus software must be configured to automatically start on device power-up and to continuously run for the duration that the computer system or mobile device is powered.

12.1.6. All anti-virus software must be configured to run automatic updates provided by the anti-virus software supplier.

12.1.7. All anti-virus software must be configured to conduct periodic scans of the computer system or mobile device on which it is installed.

12.1.8. All anti-virus software must be configured to generate log files, and to store these log files either locally on the computer system or mobile device or centrally on a organisation-wide anti-virus server (if applicable). All logs must be kept for a minimum of 3 months.

12.1.9. All anti-virus must scan external websites that the user visits and flag or block if they are of a restricted category or infected.

12.2. **Installation of anti-virus software on mail servers**

12.2.1. Mail servers must have either an external or an internal anti-virus scanning application that scans all mail destined to and from the server. Local anti-virus scanning may be disabled during any backup or system downtime periods if an external anti-virus application still scans inbound emails during this period.

12.3. **Other processes, systems and tools to deter malware**

12.3.1. All computer systems and mobile devices must run the organisation's approved operating system at its latest supported version with all relevant updates and patches installed.

12.3.2. Web filtering must be implemented to reduce the potential access to websites that may contain malicious code.

12.3.3. Web browsers must be configured to reduce the possibility of issues arising from mobile code.

12.4. **Requirements of users**

12.4.1. Any activity intended to create and/or distribute malware on an information processing facility, computer system or mobile device is strictly prohibited.

12.4.2. All users must not in any way interfere with the anti-virus software installed on any computer system or mobile device.

12.4.3. All users must immediately report any issues, or suspected issues relating to malware and any anti-virus warnings and alerts communicated to them from a computer system or mobile device.

12.4.4. All users must check the authenticity of attachments/software to be installed from internet sources.

12.4.5. Users must not install applications that arrive on unsolicited media.

12.4.6. Users must seek advice from the IT supplier if their computer system or mobile device requests them to install or update software such as Java and ActiveX.

13.0. Removable Media

17.1. The use of removable media is prohibited unless an expectation has been reviewed by the IT supplier and approved by top management.
17.2. Any exceptions grant to this policy shall be reviewed an annual basis.
17.3. Removable media used shall only be supplied by the IT provider.
17.4. Removable media shall never be the sole location of data.
17.5. Technical measures shall be put in place where feasible to protect the data contained.
17.6. Technical measures shall be in place where feasible to ensure that unauthorised removable media cannot be used in company devices.

14.0. Protection of Personal Information Policy

14.1. This sub-policy specifies the controls that need to be applied to the storage, processing and dissemination of Personal Information that is accessed, stored or processed by the organisation to ensure that One Resourcing complies with and can demonstrate compliance with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

14.2. **Data Protection Officer**

14.2.1. One Resourcing will not maintain and appointed Data Protection Officer as they are not legally required to have one appointed and there are currently no benefits that would offset the cost of an appointment. Instead a data protection co-ordinator will be appointed.

14.2.2. It is the responsibility of the Data Protection co-ordinator to:

- Inform and advise Top Management, employees and any suppliers who undertake processing of Personal Information on behalf of One Resourcing, of their obligations in regards to this policy and the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679);
- Monitor One Resourcing's compliance with this policy, the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679);
- Ensure all employees have appropriate training with regards to processing of Personal Information;
- Act as a contact point for the Information Commissioner's Office on issues relating to the processing of Personal Information.

14.3. **Application of the Personal Information protection principles**

14.3.1. The following principles must be applied and compliance with them demonstrated in relation to all Personal Information that is accessed, stored or processed by employees, and employees or suppliers, while they are accessing or processing the One Resourcing's information assets and any Personal Information that One Resourcing is the Controller of or processing on behalf of another Controller:

- Personal information shall be processed lawfully, fairly and in a transparent manner;
- Personal information shall be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
- Any Personal Information collected shall be adequate, relevant and and limited to what is necessary in relation to the purposes for which it is processed;
- Any Personal information processed shall be accurate, kept up-to-date (where necessary) and every reasonable step is taken to ensure that Personal Information that is inaccurate with regards to the purposes for which it is processed is erased or rectified without delay;
- Personal information shall not be kept in form that permits identification of Information Subjects for longer than is necessary for purposes for the which the personal information is processed (Personal Information may be put Beyond Use where deletion is not reasonably feasible);
- Appropriate technical and organisational measures shall be taken to ensure appropriate security of the Personal Information, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage;

14.3.2. All processes and operations that involve the processing of Personal Information must be designed to ensure that these principles can be achieved and are applied. Where any changes are required to One Resourcing's Assets that impact on the processing of Personal Information, the **Change Control Procedure** must be applied.

14.4. **Registration with the Information Commissioner**

14.4.1. It is the responsibility of the Operations Director to ensure that the appropriate registration is maintained with the Information Commissioner.

14.5. **Personal Information Processing Register**

14.5.1. It is the responsibility of Operations Director to ensure that a **Personal Information Processing Register** is maintained that contains information on

- All Personal Information that One Resourcing is the Controller of regardless of whether it is processed by One Resourcing or by a Processor engaged by One Resourcing;
- All Personal Information that One Resourcing is a Processor of on behalf a Controller or other Processor;

- The types of Information Subjects that the Personal Information relates to, the limit of the information collected and the source that it is obtained from;
- The reason the processing is undertaken and the legal grounds for doing so;
- The types of processing employed and the methods and technologies used;
- The details of any Processers used (where One Resourcing is the Controller) or direct Sub-Processors used (where One Resourcing is the Processor);
- The country or region where the Personal Information is processed and stored;
- All recipients of the Personal Information;
- The period for which the Personal Information is retained and the justification for doing so;
- Whether any Automated Processing is undertaken;
- Whether the Personal Information falls into a Special Category and if so the processing justification offered by Article 9 of the General Data Protection Regulation (EU 2016/679) that applies.
- Whether the Personal Information is transferred in any way outside of the EU and if so the countries/territories/organisations it is transferred to.

14.6. **Consent to Process Personal Information**

14.6.1. Where One Resourcing is a Controller of Personal Information and it undertakes processing of Personal Information requiring the consent of the Information Subject, a record of the consent must be obtained from the Information Subjects using a **Privacy Notice + Consent Opt-in Form**.

14.7. **Processing of Personal Information obtained from an Information Subject**

14.7.1. Where One Resourcing has collected personal data directly from an Information Subject, they must be provided with a **Privacy Notice** that contains at least the following information who consent to the processing of their Personal Information of the name and contact details of One Resourcing's Information Security Manager/Data Protection Officer;

- The scope and legal justification of processing that will be undertaken with the information they provide;
- Where the legal justification for processing the Personal Information is the Controller's legitimate interest, details of the legitimate interest;

- Where the legal justification for Processing the Personal Information is that the Information Subject has consented to the processing, the existence of a right to withdraw consent at any time, without affecting the lawfulness of the processing carried out prior to the withdrawal;
- The categories of recipients who will have access to their Personal Information;
- The time period for which their information will be stored or the criteria that will be applied to determine the time period;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- Any planned transfers of their information to a third country or international organisation and information on the safeguards being applied and the means by which the Information Subject can obtain a copy of them or where they are available;
- Whether any automated decision-making will be applied to their information and if so the logic that will be applied and the envisaged consequences for them;
- Whether One Resourcing is a joint Controller of the information and if so and overview of the agreement in place with other joint Controllers;
- Their rights to:
    - request access to their information
    - request corrections be made to their information
    - request their information be deleted
    - request that processing of their information is restricted
    - request their information be transferred to another Controller
    - lodge a complaint with the Information Commissioner
    - and the means by which they can notify One Resourcing to exercise one or more of these rights;

14.8. **Processing of Personal Information obtained from third parties**

14.8.1. Where One Resourcing is a Controller of Personal Information and it undertakes processing of Personal Information obtained from a third party (i.e. not directly from the Information Subjects it relates to) then unless:

- The Information Subject already has the information that One Resourcing has obtained; or
- The collection or disclosure of the information is authorised or required by EU or UK law; or
- The disclosure of the information is restricted by due to the obligation of a professional body that has provided it or a requirement of EU or UK law;
- It would require a disproportionate effort to provide the information.

One Resourcing will provide the following information to Information Subjects about whom the Personal Information relates to:

- The name and contact details of One Resourcing's Information Security Manager;
- The scope and legal justification of processing that will be undertaken with the information they provide;
- The categories of information that will be processed;
- The categories of recipients who will have access to their Personal Information;
- The source of the Personal Information and whether that source was publicly available;
- The time period for which their information will be stored or the criteria that will be applied to determine the time period;
- Where the legal justification for processing the Personal Information is the Controller's legitimate interest, details of the legitimate interest;
- Where the legal justification for Processing the Personal Information is that the Information Subject has consented to the processing, the existence of a right to withdraw consent at any time, without affecting the lawfulness of the processing carried out prior to the withdrawal;
- Any planned transfers of their information to a third country or international organisation and information on the safeguards being applied and the means by which the Information Subject can obtain a copy of them or where they are available;
- Whether any automated decision-making will the applied to their information and if so the logic that will be applied and the envisaged consequences for them;
- Whether One Resourcing is a joint Controller of the information and if so and overview of the agreement in place with other joint Controllers;

- Their rights to:
    - request access to their information
    - request corrections be made to their information
    - request their information be deleted
    - request that processing of their information is restricted
    - request their information be transferred to another Controller
    - request to not be subject to a decision based solely on Automated Processing.
    - lodge a complaint with the Information Commissioner

  and the means by which they can notify One Resourcing to exercise one or more of these rights;

This information will be provided to Information Subjects either within one month of One Resourcing obtaining the information or at the time of first communicating with the Information Subject (whichever is the soonest).

14.9. **Accessing, processing and storage of Personal Information**

14.9.1. The Operations Director must ensure that appropriate physical and technical controls are in place to:

- Protect the confidentiality, integrity and availability of all Personal Information;
- Prevent unlawful processing of Personal Information.

14.9.2. Personal Information should be accessed, processed and stored only to:

- Fulfil the needs of customers;
- Comply with legal requirements;
- Enable the effective implementation of the organisation's ISMS.

14.9.3. Personal Information should be accessed, processed and stored in accordance with this policy, the specifications detailed in the **Personal Information Processing Register** and the **Information Classification, Labelling and Handling Policy**.

14.9.4. Access to Personal Information must be provided in accordance with the **Access Control Policy**.

14.10. **Requests by Information Subjects to exercise their rights and freedoms**

For all Personal Information that One Resourcing is the Controller of:

14.10.1. All requests by Information Subjects whose Personal Information is processed by One Resourcing, to exercise their rights and freedoms under the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679) will be managed in accordance with the **Handling of Personal Information Requests Procedure**.

14.10.2. Any information that needs to be provided to Information Subjects who submit requests will be provided in a concise, transparent, intelligent and easily accessible form, using clear and plain language.

14.10.3. Any information requested by Information Subjects in the relation to any of their Personal Information processed by One Resourcing that One Resourcing is legally obliged to provide, will be provided free of charge unless the request if manifestly unfounded or excessive, in which case One Resourcing may change a reasonable fee for providing the information of refuse to act on the request.

14.10.4. Where the request covers the deletion of information that has been made public then One Resourcing will take all reasonable steps possible to inform other Controllers who are processing the information to delete any copy of the information that they hold or any links they have to the information.

14.11. **Transferring Personal Information**

14.11.1. Any transfer of Personal Information to a third party must be carried out under a written agreement, setting out the scope and limits of the sharing and in accordance with the **Information Classification, Labelling and Handling Policy**.

14.11.2. In the event that One Resourcing needs to transfer Personal Information to a non-EU country or an international organisation then:

- Relevant **Privacy Notices** needs to be updated to reflect this;
- The Information Subjects affected must be informed before the transfer takes place and provided with information regarding the safeguards that One Resourcing will ensure are in place.

14.12. **Compliance and Controls Assessments**

14.11.1 To ensure that:

- All controls employed to protect Personal Information is controlled or processed by One Resourcing are maintained and effective;
- One Resourcing complies with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679);

a schedule of audits will be completed as detailed in the **Internal Audit Schedule** and in accordance with the **Internal Audit Procedure**.

14.13. **Arrangements with Joint Controllers**

14.13.1. Where One Resourcing is a joint Controller of any Personal Information then a **Joint Controller Agreement** (or an equivalent agreement) will be implemented with any joint Controllers.

14.14. **Arrangements with Controllers**

Where One Resourcing undertakes processing on behalf of a Controller

14.14.1. A **Personal Data Processing Contract** will be (or an equivalent agreement) will be implemented with any Processors.

14.14.2. No processing of information provided by the Controller will be undertaken without an explicit instruction from them.

14.15. **Arrangements with Processors**

Where One Resourcing uses a supplier to undertake processing on its behalf:

14.15.1. A **Personal Data Processing Contract** will be (or an equivalent agreement) will be implemented with any Processors;

14.15.2. The **Change Management Procedure** shall be applied before changing supplier or taking on a new supplier and any applicable Controllers will be notified in writing of the change and provided with an opportunity to object to the change;

14.15.3. A **Personal Information Processor Assessment** will be completed to assess whether they can provide sufficient guarantees to implement appropriate control measures that will ensure the processing they undertake complies with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679) and protects the rights and freedoms on the Information Subjects whose information they process on behalf of One Resourcing.

14.15.4. An audit of a supplier's compliance with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679 will be undertaken where:

- The information obtained from a **Personal Information Processor Assessment** raises doubts as to the adequacy of the guarantees provided by a Processor; or
- The supplier is undertaking High Risk Processing; or
- An information security incident occurs that has a significant impact on the confidentiality or integrity or availability of any Personal Information and following an investigation of the root cause of the incident, the controls and processes employed by the supplier are identified as having been a contributing factor.

The audit will be completed using the **Activ Legal Compliance Manager.**

14.16. **High Risk Processing**

14.16.1. A data impact assessment must be completed for any High Risk Processing of Personal Information that One Resourcing is a Controller of before any such processing is started.

14.16.2. The results of the data impact assessment must be recorded in the **Personal Information Processing Register**.

14.16.3. If a data impact assessment indicates that the processing would result in a high risk to the rights and freedoms of the Information Subjects whose Personal Information is being processed, then Operations Director must consult with the Information Commissioner's office before any processing is started.

14.17. **Personal Information Breaches**

14.17.1. In the event of a Security Incident that compromises the confidentiality, integrity or availability of any Personal Information actions shall be taken and records maintained in accordance with the **Security Incident Management Procedure**.

15.0. Suppliers Policy

15.1. This sub-policy specifies the controls that need to be applied to all suppliers who can compromise the security of the organisation's information assets.

15.2. This sub-policy does not apply to services supplied by individuals under the terms of an **Employment Contract** issued by the organisation.

15.3. **Information security critical suppliers (ISCS)**

15.3.1. The use of all ISCS must be approved by the Operations Director.

15.3.2. This use of all ISCS who undertake processing of Personal Information on behalf of One Resourcing must done in accordance with the **Data protection Policy**

15.3.3. Up-to-date records relating to the status of information about ISCS security controls, certifications and key personnel must be maintained in the **Approved Suppliers Register**.

15.3.4. All information security risks identified that relate to the use of ISCS must be assessed and recorded in the **Risk Assessment Register** in accordance with the **Information Asset and Risk Management Procedure**.

15.3.5. ISCSs must not deliver goods or services that are not covered within the scope of a current **Supply of Goods and Services Agreement template**. The current **Supply of Goods and Services Agreement template** must include the following information:

- The scope of goods and services supplied by the ISCS covered by the agreement;
- The obligations of the ISCS to protect the organisation's information assets in respect of availability, integrity and confidentiality;
- The obligations of the ISCS to comply with the organisation's **Information Security Policy** and relevant processes, policies and procedures in its ISMS, including acknowledgement of documents supplied by the organisation;
- The minimum information security controls implemented and maintained by the ISCS to protect the organisation's information assets and the arrangements for monitoring their effectiveness;
- The arrangements for reporting and managing security incidents, as per the **Security Incident Management Procedure**;
- The arrangements for managing changes to any assets, as per the **Change Control Procedure**;
- The contact names of the persons employed by the organisation and ISCS with responsibility for information security;
- The defect resolution and conflict resolution processes.

15.3.6. The information security controls detailed above should include the following considerations:

- Subcontracting of the supply of goods and services by the ISCS to third parties;
- Access control to the organisation's assets by ISCS employees and subcontractors;
- Resilience, recovery and contingency arrangements to ensure the availability of any assets including any information processing facilities provided by the ISCS and/or the organisation;
- Accuracy and completeness controls to ensure the integrity of the assets, information or information processing equipment/facilities provided by the ISCS and/or the organisation;
- Processes and/or procedures for transferring information and/or information processing facilities between the ISCS, the organisation and other third parties;
- Screening checks undertaken on ISCS employees and subcontractors;
- Awareness training for ISCS employees and subcontractors;

- Any legal and regulatory requirements, including information protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;
    - ISCS obligation to periodically deliver an independent report on the effectiveness of controls.

15.3.7. It is the responsibility of the Operations Director to create and maintain an **Approved Suppliers Register**.

15.3.8. It is the responsibility of the Operations Director to ensure that all suppliers are provided with up-to-date copies of the organisation's policies and procedures that are relevant to them.

15.3.9. It is the responsibility of the Operations Director to ensure that the information security controls specified in the **Supply of Goods and Services Agreement** are audited at a frequency of not less that once every 12 months by a qualified auditor.

15.4. **Other suppliers**

15.4.1. Where suppliers will be handling personal data a due diligence survey with evidencing will be prior to any processing and refreshed every 18 months or if there is an information security incident.

15.4.2. Where suppliers will be handling personal data a data processing agreement place prior to any processing being under taken

15.4.3. Shall be checked to make sure that they comply with the relevant requirements of ISO9001, ISO27001 and ISO14001.

15.4.4. Shall be recorded in the supplier register.

16.0. Teleworking Policy

16.1. This sub-policy specifies the controls that need to be applied to teleworking to minimise the risks to information security arising from the access, processing and storage of information assets at locations that are not under the control of the organisation.

16.2. **Teleworking authorisation**

16.2.1. All teleworking must be approved by the Operation Director

16.2.2. The scope of a teleworker's teleworking must be defined to include:

- Authorised locations for teleworking, e.g. home, hotels, travelling etc.;
- Equipment and electronic communication facilities to be used;
- Access controls to the organisation's information processing facilities;
- Any specific controls to be applied, e.g. use of equipment by other individuals.

16.3. **Accessing the organisation's information processing facilities from teleworking locations**

16.3.1. Teleworkers must comply with the **Access Control Policy**, **Acceptable Use of Assets Policy**, **Mobile Devices Policy** and the **Protection from Malware Policy** when connecting to the organisation's information processing facilities whilst teleworking.

16.3.2. Remote access to the organisation's information processing facilities will be authorised by the Operation Director.

16.3.3. Remote access to the organisation's information processing facilities will be using openVPN.

16.4. **Organisation-provided equipment for teleworking**

16.4.1. Where equipment is provided to the teleworker for teleworking, the teleworker must comply with the **Acceptable Use of Assets Policy**, **Mobile Devices Policy** and **Use of Software Policy.**

16.5. **Use of teleworker-owned equipment for teleworking**

16.5.1. Teleworkers are permitted to use their own equipment in accordance with the **Access Control Policy** provided:

- The equipment is approved for use by the Operations Director;
- The equipment is only used in accordance with the approved scope of their teleworking and Section 16.2 of this sub-policy;
- The equipment is not set to automatically connect to wireless networks;

- All information assets are not saved locally on the equipment and are only accessed and saved on the organisation's information processing facilities;
- All equipment used has the current version of its operating system installed, defined as a version for which security updates continue to be produced and made available for the equipment;
- All equipment has anti-virus software installed that meets the requirements of the **Protection from Malware Policy**;
- All equipment has comprehensive password protection implemented for account access, application access and screensavers;
- All equipment is configured to "auto lock" after an inactivity period of 5 minutes**.**

16.5.2. The teleworker is responsible for ensuring the equipment is not accessed by any unauthorised person while the equipment is being used for work purposes.

16.5.3. Teleworkers must take extra care when using any equipment for teleworking to protect it from theft and damage.

16.5.4. When using teleworking equipment at home there must be physical control in place to, prevent unauthorised persons accessing the equipment and where possible seeing the display or output of the equipment.

16.5.5. Teleworking equipment should only be used by approved personnel.

16.5.6. Repairs of damaged equipment shall be approved the operations manager

16.5.7. The teleworker must report any loss or theft of any equipment that has been used for teleworking to the Operations Director.

16.5.8. The teleworker must notify the Operations Director of the disposal of any equipment and be willing to pass, by mutual agreement, the equipment to the IT supplier for the purpose of removing any of the organisation's information assets that may still reside on it.

17.0. Use of Software Policy

17.1. This sub-policy specifies the controls that need to be applied covering the use and installation of software on any assets owned by or under the control of the organisation to minimise risks to information security arising from the misuse of software or the use of unauthorised or illegally obtained software.

17.2. **Use of software**

17.2.1. Software must only be used in connection with authorised business use.

17.2.2. Users of software must be authorised to so in accordance with the **Access Control Policy**.

17.2.3. Users must not make copies of any software provided by the organisation without the express written consent of the software publisher and the organisation.

17.3. **Installation of software**

17.3.1. Installation of software onto an asset must be authorised by the Operations Director and must be done in accordance with the **Change Control Procedure** and **Backup Policy**.

17.3.2. Users must not install, or in any way make use of, software from sources other than those provided by the organisation unless authorised to do so by the Operations Director.

17.3.3. Any software installed must carry a valid license that covers the scope of use.

17.3.4. Where practicable, these requirements shall be supported with technical controls, for example only an administrator account is able to install software on the device.

18.0. Network Policy

18.1. Networks shall be managed and controlled to protect information in systems and applications.

18.2. Service level agreements shall document any require security mechanisms and service levels.

18.3.

19.0. Physical Media

19.1. Physical media show only be used when authorised by top management, all other uses of physical media are prohibited.

19.2. When transfer physical media outside of the company premises the contents show be backed up so that the media is not the only source of the data. Additionally all data one the media should be encrypted.

19.3. Physical media should be disposed of in with the disposals procedure, 07 Disposal Procedure.docx

20.0. Vulnerability Management

20.1. The Operations Director has overall responsibility for vulnerability Management.

20.2. The following tools have been authorised for conducting and managing vulnerability scans;

- WithSecure Vulnerability Management

- Bulletproof defence

20.3. Where suppliers are providing internet facing services these are to be subject to either a quarterly scan with an authorised scanning tool or an independently verified scan or test.

20.4. Where these activities may cause disruption or affected the security of the systems, additional steps shall be taken to minimise or mitigate these risks.

20.5. Detected vulnerabilities must evaluated, verified and actioned accordingly.

20.6. After being actioned, another scan shall be run to verify that the vulnerability has been mitigated.

21.0. Policy Review

21.1. This policy and its sub-policies should be reviewed at least 18 Months or if significant changes occur that might affect its continuing suitability, adequacy and effectiveness.

This policy has been approved & authorised by:

Name:	Kevin O'Reilly
Position:	Managing Director
Date:	24th February 2026