INFORMATION SECURITY POLICY

1. Policy Objective

1.0. To protect the information assets that SDM Holdings Limited handles, stores, exchanges, processes and has access to, and to ensure the ongoing maintenance of their confidentiality, integrity and availability.

1.1. To ensure controls are implemented that provide protection for information assets and are proportionate to their value and the threats to which they are exposed.

1.2. To ensure the organisation complies with all relevant legal, customer and other third-party requirements relating to information security.

1.3. To continually improve the organisation's Information Security Management System (ISMS) and its ability to withstand threats that could potentially compromise information security.

2. Scope

2.0. This policy and its sub-policies apply to all people, processes, services, technology and assets detailed in the **Scope**. It also applies to all employees or subcontractors of information security critical suppliers who access or process any of the organisation's information assets.

3. Core Policy

3.0. The organisation believes that despite the presence of threats to the security of such information, all security incidents are preventable.

3.1. The Managing Director (Marc Chauveau) of SDM Holdings Limited is committed to achieving the objectives detailed in the policy through the following means:

3.1.1. The implementation and maintenance of an ISMS that is independently certified as compliant with ISO 27001:2017;

3.1.2. The systematic identification of security threats and the application of a risk assessment procedure that will identify and implement appropriate control measures;

3.1.3. Regular monitoring of security threats and the testing/auditing of the effectiveness of control measures;

3.1.4. The maintenance of a risk treatment plan that is focused on eliminating or reducing security threats;

3.1.5. The maintenance and regular testing of a **Business Continuity Plan**;

3.1.6. The clear definition of responsibilities for implementing the ISMS;

3.1.7. The provision of appropriate information, instruction and training so that all employees are aware of their responsibilities and legal duties, and can support the implementation of the ISMS;

3.1.8. The implementation and maintenance of the sub-policies detailed in this policy.

3.2. The appropriateness and effectiveness of this policy, and the means identified within it, for delivering the organisation's commitments will be regularly reviewed by Top Management.

3.3. The implementation of this policy and the supporting sub-policies and procedures is fundamental to the success of the organisation's business and must be supported by all employees and contractors who have an impact on information security as an integral part of their daily work.

3.4. All information security incidents must be reported to the Quality & Compliance Manager. Violations of this policy may be subject to the organisation's **Disciplinary Procedure (as contained in the employee handbook)**.

Signature/Release Confirmation

26.07.23

Marc Chauveau

Managing Director

26.07.23

Nicola Peters

Quality & Compliance Manager

4. Sub-policy index

5. Responsibilities

5.0. It is the responsibility of the Managing Director (Marc Chauveau) to ensure that this policy is implemented and that any resources required are made available.

5.1. It is the responsibility of the Quality & Compliance Manager to monitor the effectiveness of this policy and report the results at management reviews.

5.2. It is the responsibility of the Quality & Compliance Manager to create and maintain an **Asset List Access Control & Risk Register** and to ensure all assets that need to be covered by this policy are identified.

5.3. 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 Quality & Compliance Manager any issues they may be aware of that breach any of its contents.

6. Definitions

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

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

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

6.3. **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.

6.4. **Beyond use**: Controls placed on Personal Information that it is no longer necessary for SDM Holdings Limited to keep where it is not reasonably feasible to delete the information. These controls must comply with guidance from the Information Commissioner's Office.

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

6.6. **Confidential information**: Any type of information that has been specified by the organisation's **Data Protection Policy** as requiring protection through the application of cryptographic controls when it is stored or transferred electronically.

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

6.8. **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.

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

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

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

6.12. **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.

6.13. **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.

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

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

6.16. **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.

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

6.18. **Information subject**: An Identifiable Natural Person who has Personal Information that SDM Holdings Limited is the Controller of or is a Processor of on behalf of a Controller.

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

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

6.21. **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.

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

6.23. **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.

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

6.25. **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.

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

6.27. **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.

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

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

6.30. **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.

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

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

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

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

7. Associated Documents

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

8. Acceptable Use of Assets Policy

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

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

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

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

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

8.1.2. 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 **Data Protection Policy**.

8.1.3. Users must apply extreme caution when opening email attachments received from unknown senders. If in doubt, please ask the Quality & Compliance Manager for advice.

8.1.4. Users must not:

- Disclose user IDs and personal passwords which give access to the organisation's assets unless authorised by the Quality & Compliance Manager;
- 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 Quality & Compliance Manager;
- 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.

8.1.5. Any user supplied equipment must be approved by the Quality & Compliance for connection to any of the organisation's ECFs.

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

9. Access Control Policy

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

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

9.1.1. 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 the Managing Director of the organisation.

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

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

9.1.4. The Quality & Compliance Manager 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 by using and maintaining the **Asset List, Access Control and Risk Register**;
- 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.

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

9.2.1. The HR Advisor is responsible for:

- Arranging access with the Quality & Compliance Manager or/and the Archive & Web Support Manager 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 Quality & Compliance Manager or/and the Archive & Web Support Manager 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 **Asset List, Access Control and Risk 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.

9.2.2. The Quality & Compliance Manager or/and the Archive & Web Support Manager is responsible for:

- Responding in a timely manner to requests for the activation and deactivation of user account access made to them by the HR Advisor;
- Configuring and reviewing user access to the organisation's assets and information processing facilities as specified in the **Asset List, Access Control and Risk 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 Quality & Compliance Manager;
- 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.

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

- Passwords must be at least 7 characters in length;
- Passwords must be a combination of:
  - English uppercase characters (A...Z)
  - English lowercase characters (a…z)
  - Base 10 digits (0…9)
  - Non-alphanumeric characters selected from the following:
  - ! " $ % ^ & * ( ) - _ = + [ ] { } ; : ' @ # ~ , < . > / ? \ |
  - (Do not use £, € or a SPACE).
- 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.

9.2.4. The Quality & Compliance Manager is responsible for:

- Granting permanent or temporary access to restricted areas;
- Reviewing access to restricted areas every 6 months and authorising changes where required;
- Leading and providing support to incident investigations where required.

9.2.5. 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.

9.3. **Access to remote users**

9.3.1. 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.

9.3.2. 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 3 minutes of inactivity;
- Access to the Organisation's hosted network is controlled by means of individual user logins and passwords. Login names are allocated by the IT supplier, who also issues the initial password for each user.
- Only SDM Holdings Provided Mobile devices are to be used to access SDM Holdings information or that of its subsidiaries.

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

9.4.1. Access to the organisation's operating facilities must be authorised by the Managing Director.

9.4.2. Access to the organisation's operating facilities will be processed and granted by the Quality & Compliance Manager

9.4.3. 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.

9.4.4. 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 the Quality & Compliance Manager;
- Accompanying visitors that are in their care at all times, and not allowing them to enter any unauthorised location;
- Immediately reporting to the Quality & Compliance 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.

9.4.5. Authorisation must be granted by the Quality & Compliance Manager to hold open a controlled access door for longer than the time required for an individual to enter or exit the area.

9.5. **Visitors and suppliers**

9.5.1. All visitors must:

- Sign in visitor reception within the administration building;
- 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;
- Display the visitor's pass provided to them by a member of staff at visitor reception within the administration building;
- Return passes to the visitor reception when they leave the organisation's premises, even if for a limited period such as lunchtime;
- 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.

9.5.2. All suppliers working in an operating facility must:

- Sign in visitor reception within the administration building

- 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;
- Display a visitor's pass at all times;
- Return passes to Site Manager or visitor reception within the administration building when they leave the organisation's premises, even if for a limited period such as lunchtime;
- Immediately report any accidental breaches of this policy to the Quality & Compliance Manager;
- Not access or view any information that has not been provided as part of the contracted task.

9.6. **Remote access to customer networks**

9.6.1. Any access to, logging onto any customer networks for the purposes of depositing information will only be done with the expressed permission of the customer and by prearrangement – this will be restricted to the depositing of data that has been scanned in accordance with SDM's Internal Scanning Service Procedure.

10. Backup Policy

10.0. 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.

10.1. **Software**

10.1.1. Backup copies of all software, including previous versions, must be made prior to their first use, stored in the location mentioned below in the **Electronic Data Backup Requirements Table** and retained for the period of time mentioned below. 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.

Electronic Data Backup Requirements Table

Server	Backup Media	Type of Backup	Frequency	Copies Kept
Hosted Desktop	**Cloud Back up**	**Full**	**Daily**	**In a secure offsite location 365 days.**
365 Email	**Cloud Back Up**	**Incremental**	**Daily**	**2 years**
O'Neil Cloud based system	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
Xero	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
Zendesk	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
Activ	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
Recurly	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**

Stripe	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
Hotjar	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
Calendar Hero	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
Visitor Que	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
Mail Chimp	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
Devsoft on SDMSCAN server	**Cloud Back up**	**Full**	**Every 2 hours**	**In a secure offsite location 365 days.**
Allied Images on SDMSCAN server	**Cloud Back up**	**Full**	**Every 2 hours**	**In a secure offsite location 365 days.**
Google Analytics	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
Zopmin Chat	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
Go Cardless	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**	**As cloud service provider contract**
WP Engine	**Cloud Back up**	**Full**	**Daily**	**Cloud Back Up**

Backups must be made in accordance with the **Electronic Data Backup Requirements Table**.

10.2. **Electronic files**

10.2.1. Backup copies of all electronic files that contain information assets, including previous versions, must be made daily, stored in Hosted Desktop > Cloud Back up and retained for 365 days.

10.2.2. All backup copies of electronic files must be encrypted in accordance with the **Use of Cryptographic Controls Policy** and as specified in the **Electronic Data Backup Requirements Table**.

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

10.2.4. Backups must be made in accordance with the **Data Protection Policy** and the **Electronic Data Backup Requirements Table**.

10.3. **Storage of backups**

10.3.1. 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.

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

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

10.4. **Testing of backups**

10.4.1. Backups of software and electronic files, and media used to store them, must be tested at intervals as determined by the ISMS Committee in accordance with the **Electronic Data Backup Requirements Table**.

11. Clear Desk and Clear Screen Policy

11.0. 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.

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

11.1.1. Information assets held on paper or portable storage media must be stored in cabinets and/or drawers, in accordance with the **Data Protection 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 site **Fire Evacuation Procedure**.

11.1.2. 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.

11.2. **Display screens**

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

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

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

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

12. Communication Policy

12.0. This sub-policy specifies the rules that must be applied with regards to internal and external communications relevant to the ISMS.

12.1. **Communication with third parties**

12.1.1. Any enquiries received from third parties relating to information security or the organisation's ISMS must be immediately referred to the Managing Director or, in their absence, the Quality & Compliance Manager.

12.1.2. Any information exchanged with third parties must be done in accordance with the **Data Protection Policy** and the **Control of Documented Information Procedure**.

12.1.3. Supply of information about the organisation's ISMS, including policies, procedures and specific control measures employed must be approved by the Quality & Compliance Manager.

12.2. **Employee briefings**

12.2.1. The Quality & Compliance Manager will deliver a briefing to all employees on information security matters at least once a year, or if any significant issues arise or decisions are made that have consequences for employees.

12.2.2. Employees will be encouraged to raise any concerns they have relating to information security matters at employee briefings.

13. Cryptographic Controls Policy

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

13.1. **General principles**

13.1.1. 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.

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

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

13.1.4. Mobile device hard drives must be encrypted.

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

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

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

13.2. **Encryption of data in transit**

13.2.1. 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.

13.3. **Key management**

1. All critical or sensitive data transferred outside Secure Data Management Limited is encrypted
2. All removable media, including memory sticks is precluded.
3. Laptop hard drives are whole-disk encrypted utilising a 2048-bit encryption key for any laptops which leave Secure Data Management Limited premises.
4. All remote access is to take place via encrypted VPN or an equally secure alternative. (2048 bit encryption on hosted system)
5. WPA (preferably WPA2) encryption is mandatory for all wireless networks carrying Secure Data Management Limited data
6. E-mails are all encrypted via use of the Hosted system and office 365.
7. Client access to web-based applications (O'Neil) is encrypted using at least a 128-bit SSL certificate.

7.0. The internal SDMSCAN server has a secure username and password to grant access to the server. The machine is on the standard Production VLANto enable scanning from site to site. The server is not accessible from the Guest Wifi but only from the Private network or plugged in PC.
Bit defender Antivirus is on this Server and runs continuously and automatically updates its definitions from the cloud.

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.

7.1. **Avoiding adverse impacts from encryption**

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

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

7.1.3. The persons with access to encryption keys must be recorded in the **Asset List Access Control & Risk Register**.

8. Information Classification, Labelling and Handling Policy

8.0. 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.

8.1. **Classification**

8.1.1. It is the responsibility of the Quality & Compliance manager to maintain the **I**nformation 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.

8.2. **Labelling**

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

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

8.3. **Copying**

8.3.1. 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.**

8.4. **Distribution**

8.4.1. Information assets should only be distributed:

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

8.4.2. Where distribution is necessary, it must be done in accordance with **Control of Documented Information Procedure.**

8.5. **Destruction**

8.5.1. Destruction of an information asset must be done in accordance with the **Control of Documented Information Procedure**.

9. Mobile Devices Policy

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

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

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

9.1. **Issuing of mobile devices**

9.1.1. The issue of any mobile device to a user must be authorised by the MD and recorded **Asset List, Access Control and Risk Register**

9.2. **Use of mobile devices**

9.2.1. All users of mobile devices must comply with the **Acceptable Use of Assets Policy**, **Clear Desk and Clear Screen Policy**, **Backup Policy**, **Teleworking Policy** and the **Use of Software Policy**.

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

9.2.3. 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.

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

9.2.5. Users must immediately notify the Quality & Compliance Manager if a mobile device is known or suspected to be lost or stolen.

9.2.6. 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.

9.2.7. 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.

9.2.8. 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.

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

9.2.10. 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 Quality & Compliance Manager.

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

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

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

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

9.2.15. Mobile devices must not be used to transfer information via wireless networks that have not been approved by the Quality & Compliance Manager.

9.3. **Return of mobile devices**

9.3.1. Upon request by the HR Advisor termination of contract or change of role, a user must return any mobile devices they have been issued with to the Quality & Compliance Manager.

9.3.2. All mobile devices must be returned to the Quality & Compliance and recorded **Asset List, Access Control and Risk Register.**

10. Physical and Environmental Security Policy

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

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

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

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

10.1. **Physical protection of operating facilities**

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

10.1.2. All operating facilities must be protected by an intruder alarm system that is remotely monitored by an approved service provider and includes red care with police and management call out. This is maintained under an existing maintenance contract.

10.1.3. All external windows and doors must be kept shut and locked at all times unless authorised by the Site Manager.

10.1.4. The main storage access doors are kept closed other than when unloading deliveries and loading outgoing vehicles.

10.2. **Environmental protection of operating facilities**

10.2.1. All the environmental vulnerabilities and controls associated with the organisation's operating facilities are identified in the **Asset List, Access Control and Risk Register**.

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

10.2.3. 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.

10.2.4. SDM Holdings have a spill control Procedure and a COSHH statement to protect the working environment of the sites in its control.

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

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

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

10.3.3. All hard copy files must be stored in cabinets in accordance with the **Clear Desk and Clear Screen Policy** and the **Data Protection Policy**.

10.3.4. All assets must be maintained in accordance with manufacturers' and suppliers' recommendations or as identified in the Activ based **Improvement Log**. Maintenance requirements and their status will be recorded in the **Asset List, Access Control and Risk Register**.

10.3.5. 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.

11. Protection from Malware Policy

11.0. 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.

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

11.1.1. It is the responsibility of the Quality & Compliance Manager 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.

11.1.2. 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.

11.1.3. 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.

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

11.1.5. 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.

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

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

11.1.8. 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 an organisation-wide anti-virus server (if applicable). All logs must be kept for a minimum of 365 days.

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

11.2.1. 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.

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

11.3.1. 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.

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

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

11.4. **Requirements of users**

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

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

11.4.3. 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.

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

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

11.4.6. Users must seek advice from the Quality & Compliance Manager if their computer system or mobile device requests them to install or update software such as Java and ActiveX.

11.4.7. All logs generated by the system and related processes are checked on a regular basis by the established IT supplier and/or the hosted / cloud services providers. Particular attention is paid to remote access logins, virus protection and firewall logs.
Any substantial issues may be escalated to the ISMS Manager and/or the ISMS Committee and may be addressed using Business Continuity or non-conformance mechanisms as appropriate.

12. Protection of Personal Information Policy

12.0. 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 SDM Holdings Limited complies with and can demonstrate compliance with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

12.1. **Data Protection Officer**

12.1.1. SDM Holdings Limited will maintain and appointed Data Protection Officer whose contact details are published on the company's website and communicated to the Information Commissioner's Office.

12.1.2. The appointed Data Protection Office will:

- Report directly to Top Management;
- Be involved properly and in a timely manner, in all issues which relate to the protection of Personal Information;
- Have the full support of Top Management in performing their tasks;
- Be provided with all resources necessary to carry out the tasks required by the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679);
- Be provided with all the resources necessary to maintain their expert knowledge;
- Have unlimited access to Personal Information processing operations;
- Not receive any instructions from Top Management regarding the exercise of the tasks required by the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679);
- Not be dismissed or penalised by the Top Management for performing tasks and duties required of them by the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679);
- Not undertake any other tasks and duties that result in a conflict of interest.

12.1.3. It is the responsibility of the Data Protection Officer to:

- Inform and advise Top Management, employees and any suppliers who undertake processing of Personal Information on behalf of SDM Holdings Limited, 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 SDM Holdings Limited 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.

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

12.2.1. 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 SDM Holdings Limited information assets and any Personal Information that SDM Holdings Limited 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 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;

12.2.2. 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 SDM Holdings Limited Assets that impact on the processing of Personal Information, the **Change Control Procedure** must be applied.

12.3. **Registration with the Information Commissioner**

12.3.1. It is the responsibility of the Quality & Compliance Manager to ensure that the appropriate registration is maintained with the Information Commissioner.

12.4. **Personal Information Processing Register**

12.4.1. It is the responsibility of Quality & Compliance Manager to ensure that a **Personal Information Processing Register** is maintained that contains information on

- All Personal Information that SDM Holdings Limited is the Controller of regardless of whether it is processed by SDM Holdings Limited or by a Processor engaged by SDM Holdings Limited;
- All Personal Information that SDM Holdings Limited 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 SDM Holdings Limited is the Controller) or direct Sub-Processors used (where SDM Holdings Limited 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.

12.5. **Consent to Process Personal Information**

12.5.1. Where SDM Holdings Limited 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 + Opt-in agreement via the Data Processing Agreement for the business and employee / commercial contracts as appropriate**.

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

12.6.1. Where SDM Holdings Limited 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 SDM Holdings Limited'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 SDM Holdings Limited 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 SDM Holdings Limited to exercise one or more of these rights;

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

12.7.1. Where SDM Holdings Limited 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 SDM Holdings Limited 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.

SDM Holdings Limited will provide the following information to Information Subjects about whom the Personal Information relates to:

- The name and contact details of SDM Holdings Limited's Information Security Manager/Data Protection Officer;
- 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 SDM Holdings Limited 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 SDM Holdings Limited to exercise one or more of these rights;

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

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

12.8.1. The Quality & Compliance Manager/HR Advisor 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.

12.8.2. 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.

12.8.3. 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**.

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

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

For all Personal Information that SDM Holdings Limited is the Controller of:

12.9.1. All requests by Information Subjects whose Personal Information is processed by SDM Holdings Limited, 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 **Data Protection Policy.**

12.9.2. 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.

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

12.9.4. Where the request covers the deletion of information that has been made public then SDM Holdings Limited 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.

12.10. **Transferring Personal Information**

12.10.1. 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 **Data Protection Policy.**

12.10.2. In the event that SDM Holdings Limited 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 SDM Holdings Limited will ensure are in place.

18.11 **Compliance and Controls Assessments**

18.11.1 To ensure that:

- All controls employed to protect Personal Information is controlled or processed by SDM Holdings Limited are maintained and effective;

- SDM Holdings Limited 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**.

18.12 **Arrangements with Joint Controllers**

18.12.1 Where SDM Holdings Limited is a joint Controller of any Personal Information then a **Data Processing Agreement** (DPA) (or an equivalent agreement) will be implemented with any joint Controllers.

18.13 **Arrangements with Controllers**

Where SDM Holdings Limited undertakes processing on behalf of a Controller

18.13.1 A **Data Processing Agreement** (DPA) will be (or an equivalent agreement) will be implemented with any Processors.

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

18.14 **Arrangements with Processors**

Where SDM Holdings Limited uses a supplier to undertake processing on its behalf:

18.14.1 A **Data Processing Agreement** (DPA) will be (or an equivalent agreement) will be implemented with any Processors;

18.14.2 Where deemed necessary by the SDM Holdings Data Protection Officer, an assessment of personal data processing requirements will be completed to assess whether the business 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 SDM Holdings Limited.

18.14.3 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 an assessment of personal data processing requirements 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.

18.15 **High Risk Processing**

18.15.1 A data impact assessment and an assessment of personal data processing requirements must be completed for any High-Risk Processing of Personal Information that SDM Holdings Limited is a Controller of before any such processing is started.

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

18.15.3 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 Managing Director must consult with the Information Commissioner's office before any processing is started.

18.16 **Personal Information Breaches**

18.16.1 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**.

19.0. Suppliers Policy

19.1. 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.

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

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

19.1.1 The use of all ISCS must be approved by the Quality & Compliance Manager.

19.1.2 This use of all ISCS who undertake processing of Personal Information on behalf of SDM Holdings Limited must done in accordance with the **Data Protection Policy**;

19.1.3 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**.

19.1.4 All information security risks identified that relate to the use of ISCS must be assessed and recorded in the **Asset List Access Control & Risk Register** in accordance with the **Data Protection Policy and the Information Asset and Risk Management Procedure**.

19.1.5 ISCSs must not deliver goods or services that are not covered within the scope of a current Supply of Goods and Services Agreement. The current Supply of Goods and Services Agreement 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.

19.1.2 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.

19.1.3 It is the responsibility of the Quality & Compliance Manager to create and maintain an **Approved Suppliers Register**.

19.1.4 It is the responsibility of the Quality & Compliance Manager> to ensure that all suppliers are provided with up-to-date copies of the organisation's policies and procedures that are relevant to them.

19.1.5 It is the responsibility of the Quality & Compliance Manager 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.

19.2 **Other suppliers**

19.2.2 At least annually, senior management will meet to discuss and review the proposed selection of new suppliers and to review the current Approved Suppliers Register.

All approved suppliers are registered on the Approved Suppliers Register. The Approved Suppliers Register is maintained by the Quality & Compliance Manager and the Financial Director.

In addition to the above, all operationally essential suppliers are reviewed in Activ annually via Supplier Assessments. These assessments are scheduled

and reviewed by the Quality Manager to coincide with the internal audit schedule.

20.0 Teleworking Policy

20.1. 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.

20.1 Teleworking authorisation

20.1.1 All teleworking must be approved by Managing Director/Quality & Compliance Manager.

20.1.2 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.

20.2 Accessing the organisation's information processing facilities from teleworking locations

20.2.1 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.

20.2.2 Remote access to the organisation's information processing facilities will be authorised by the Quality & Compliance Manager

20.2.3 Remote access to the organisation's information processing facilities will take place via encrypted VPN or an equally secure alternative. (2048 bit encryption on hosted system)

20.3 Organisation-provided equipment for teleworking

20.3.1 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.**

20.4 Use of teleworker-owned equipment for teleworking

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

- The equipment is approved for use by the Quality & Compliance Manager;
- 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**.**

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

20.4.3 Teleworkers must take extra care when using any equipment for teleworking.

20.4.4 The teleworker must report any loss or theft of any equipment that has been used for teleworking to the Quality & Compliance manager.

20.4.5 The teleworker must notify the Quality & Compliance Manager of the disposal of any equipment and be willing to pass, by mutual agreement, the equipment to the approved IT provider for the purpose of removing any of the organisation's information assets that may still reside on it.

21.0 Use of Software Policy

21.1 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.

21.2 Use of software

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

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

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

21.3 Installation of software

21.3.1 Installation of software onto an asset must be authorised by the Quality & Compliance Manager and IT Provider and must be done in accordance with the **Change Control Procedure** and **Backup Policy**.

21.3.2 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 Quality & Compliance Manager and IT Provider.

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

22.0 Policy Review

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