INFORMATION SECURITY POLICY

1.0. *Policy Objective*

1.1. To protect the information assets that Standing on Giants handles, stores, exchanges, processes and has access to, and to ensure the ongoing maintenance of their confidentiality, integrity and availability.

1.2. To ensure controls are implemented that protect information assets and are proportionate to their value and the threats to which they are exposed.

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

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

2.0. *Scope*

2.1. 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.

3.0. *Core Policy*

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

3.2. The Directors of Standing on Giants are committed to achieving the objectives detailed in the policy through the following means:

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

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

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

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

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

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

3.2.7. 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;

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

3.3. 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.

3.4. 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.

3.5. All information security incidents must be reported to the Head of Solutions. Violations of this policy may be subject to the organisation's **Disciplinary Policy and Procedure.**

Signed on behalf of Standing on Giants: Zsuzsanna Recsey

Position: CEO Date: 01/22

4.0. *xSub-policy index*

5.0. *Responsibilities*

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

5.2. It is the responsibility of the **Head of Solutions** to monitor the effectiveness of this policy and report the results at management reviews.

5.3. It is the responsibility of the **Operations Manager** 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.

5.4. 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 Manager** any issues they may be aware of that breach any of its contents.

6.0. *Definitions*

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

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

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

6.4. **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.

6.5. **Beyond use:** Controls placed on Personal Information that it is no longer necessary for Standing on Giants 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).

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

6.7. **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.

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

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

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

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

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

6.13. **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).

6.14. **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.

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

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

6.17. **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 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.

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

6.19. **Information subject:** An Identifiable Natural Person who has Personal Information that Standing on Giants is the Controller of or is a Processor of on behalf of a Controller.

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

6.21. **Mail server:** A system based on software and hardware that sends, receives and stores electronic mail.

6.22. **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.

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

6.24. **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.

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

6.26. **Personal Information protection principles:** Principles that shall be applied 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.

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

6.28. **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.

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

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

6.31. **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.

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

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

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

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

7.0. Associated Documents

7.1. All associated documents referred to in this policy are either hyperlinked or in bold and underlined.

8.0. Acceptable Use of Assets Policy

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

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

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

8.2. Use of electronic communication facilities (ECFs)

8.2.1. All users of ECFs must be authorised to do so by the organisation's **Access Control Policy**.

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

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

8.2.4. Users must not:

- Disclose user IDs and personal passwords which give access to the organisation's assets unless authorised by the **Head of Solutions**;
- 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**;
- 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.

8.2.5. Any user-supplied equipment must be approved by the **Head of Solutions** for connection to any of the organisation's ECFs.

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

9.0. Access Control Policy

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

9.2. Access to the information assets, operating facilities and information processing facilities

9.2.1. 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 member of the Leadership Team of the organisation.

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

9.2.3. 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.

9.2.4. The **Head of Solutions** 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's 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 review the logs of system administrator access and actions.

9.3. Control of access to information processing facilities

9.3.1. **The Operations Manager** is responsible for:

- Arranging access with the **Head of Solutions** 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 **Head of Solutions** 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.

9.3.2. The **Operations Manager** is responsible for:

- Responding promptly to requests for the activation and deactivation of user account access made to them by the **Head of Solutions**;
- 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 **Head of Solutions**;
- 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.

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

- Passwords must be at least 8 characters in length;
- Use a mix of alphanumeric characters (letters and numbers) and symbols: Uppercase (capital) letters. Examples: A, E, R, Lowercase (small) letters. Examples: a, e, r, Numbers. Examples: 2, 6, 7, Symbols and special characters. Examples: ! @ & *
- Users must have 2-factor authentication enabled;
- Passwords must automatically expire every 3 Months;
- 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.

9.3.4. The **Operations Manager** is responsible for:

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

9.3.5. 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.

9.4. Access to remote users

9.4.1. 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.

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

- Only be provided to authorised users;
- Only be used with approved assets, following the **Acceptable Use of Assets Policy**, **Teleworking Policy** and **Mobile Devices Policy**;
- Be set to timeout after **5 mins** of inactivity;

9.5. Remote access to customer networks

9.5.1. Employees are permitted to work from places other than their home address, including abroad at the discretion of their line manager and or the leadership team. Working from a public space or abroad is permitted when:

- A VPN has been set up for their account
- Employees ensure that they are complying with the **teleworking policy**

9.5.2. Any requests to work abroad must be approved in advance by the employee's line manager, allowing sufficient time to set up a VPN for the employee.

10.0. Backup Policy

10.1.1. 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.

10.2. Software

10.2.1. Backup copies of all software, including previous versions, must be made before their first use, stored in Google workspace, Google cloud platform and Bitbucket and retained without an expiry date. 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.

10.2.2. Backups must be made following the Electronic Data Backup Register.

10.3. Electronic files

10.3.1. Backup copies of all electronic files that contain information assets, including previous versions, must be made daily, stored on Google Drive and retained forever.

10.3.2. All backup copies of electronic files must be encrypted following the Use of **Cryptographic Controls Policy** and as specified in the **Electronic Data Backup Register**.

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

10.3.4. Backups must be made following the Information **Classification, Labelling and Handling Policy** and the **Electronic Data Backup Register.**

10.4. Storage of backups

10.4.1. 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.

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

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

10.5. Testing of backups

10.5.1. Backups of software and electronic files, and media used to store them, must be tested at least annually following the **Business Continuity Plan** and the **Electronic Data Backup Register**.

11.0. Clear Desk and Clear Screen Policy

11.1. 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.

11.2. Paper assets, visual aids and portable storage media

11.2.1. Information assets held on paper or portable storage media must be stored in cabinets and/or drawers, following 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 following the **Fire Evacuation Procedure**.

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

11.3. Display screens

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

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

11.4. Reproduction devices (printers, photocopiers and scanners)

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

12.0. Communication Policy

12.1. This sub-policy specifies the rules that must be applied to internal and external communications relevant to the ISMS and following the **Communications Register**.

12.2. Communication with third parties

12.2.1. Any enquiries received from third parties relating to information security or the organisation's ISMS must be immediately referred to the **Head of Solutions** or, in their absence, the **Operations Manager**.

12.2.2. Any information exchanged with third parties must be done following the **Information Classification, Labelling and Handling Policy** and the **Control of Documented Information Procedure**.

12.2.3. The supply of information about the organisation's ISMS, including policies, procedures and specific control measures employed must be approved by the **Head of Solutions**.

12.3. Employee briefings

12.3.1. The **Head of Solutions** 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.

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

13.0. *Cryptographic Controls Policy*

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

13.2. General principles

13.2.1. 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.

13.2.2. All confidential information transferred outside of the organisation must be encrypted before transfer.

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

13.2.4. Mobile device hard drives must be encrypted.

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

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

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

13.3. Encryption of data in transit

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

13.4. Encryption for information transferred outside the UK

13.4.1. 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.

13.5. Avoiding adverse impacts from encryption

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

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

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

14.0. Information Classification, Labelling and Handling Policy

14.1. 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.

14.2. Classification

14.2.1. It is the responsibility of the **Operations Manager** 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.

14.3. Labelling

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

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

14.4. Copying

14.4.1. 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 following the **Control of Documented Information Procedure (Appendix C)**.

14.5. Distribution

14.5.1. Information assets should only be distributed:

- To comply with client requirements;
- To comply with legal requirements;

- On a need to know basis.

14.5.2. Where distribution is necessary, it must be done following the **Control of Documented Information Procedure (Appendix C)**.

14.6. Destruction

14.6.1. Destruction of an information asset must be done following the **Control of Documented Information Procedure**.

15.0. Mobile Devices Policy

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

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

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

15.2. Issuing of mobile devices

15.2.1. The issue of any mobile device to a user must be authorised by the **Operations Manager** and recorded in the **Asset Register**

15.3. Use of mobile devices

15.3.1. 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**.

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

15.3.3. 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.

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

15.3.5. Users must immediately notify the **Operations Manager** if a mobile device is known or suspected to be lost or stolen.

15.3.6. 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.

15.3.7. 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.

15.3.8. 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.

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

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

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

15.3.12. Mobile devices must always be protected from unauthorised use by an access password following the **Access Control Policy**.

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

15.3.14. Mobile devices must not be used to transfer information via wireless networks that have not been approved by the **Head of Solutions**.

15.4. Return of mobile devices

15.4.1. Upon request by the **Head of Solutions**, termination of contract or change of role, a user must return any mobile devices they have been issued with to the **Operations Manager**.

15.4.2. All mobile devices must be returned to the **Operations Manager** and recorded in the **Asset Register**.

16.0. *Protection from Malware Policy*

16.1. 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.

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

16.2.1. It is the responsibility of the **Operations 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.

16.2.2. 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.

16.2.3. 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.

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

16.2.5. 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.

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

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

16.2.8. 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 60 days.

16.3. Installation of anti-virus software on mail servers

16.3.1. 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.

16.4. Other processes, systems and tools to deter malware

16.4.1. 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.

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

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

16.5. Requirements of users

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

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

16.5.3. 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.

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

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

16.5.6. Users must seek advice from the **Head of Solutions** if their computer system or mobile device requests them to install or update software such as Java and ActiveX.

17.0. Protection of Personal Information Policy

17.1. 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 Standing on Giants complies with and can demonstrate compliance with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

17.2. Application of the Personal Information protection principles

17.2.1. 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 Standing on Giants' information assets and any Personal Information that Standing on Giants 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 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 a form that permits identification of Information Subjects for longer than is necessary for purposes for 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;

17.2.2. 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 Standing on Giants's Assets that impact the processing of Personal Information, the Change Control Procedure must be applied.

17.3. Registration with the Information Commissioner

17.3.1. Standing on Giants is not required to register with the ICO. It is the responsibility of the **Head of Solutions** to review this annually.

17.4. Personal Information Processing Register

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

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

17.5. Consent to Process Personal Information

17.5.1. Where Standing on Giants 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**.

17.6. Processing of Personal Information obtained from an Information Subject

17.6.1. Where Standing on Giants 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 Standing on Giants Information Security Manager - the **Head of Solutions**;

- 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 before the withdrawal;
- The categories of recipients who will have access to their Personal Information;
- The period for which their information will be stored or the criteria that will be applied to determine the 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 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 how 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 Standing on Giants is a joint Controller of the information and if so an overview of the agreement in place with other joint Controllers;
- Their rights to:
  - request access to their information
  - request corrections are 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
  - complain with the Information Commissioner
  - and how they can notify Standing on Giants to exercise one or more of these rights;

17.7. Processing of Personal Information obtained from third parties

17.7.1. Where Standing on Giants 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 Standing on Giants 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 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.

Standing on Giants will provide the following information to Information Subjects about whom the Personal Information relates:

- The name and contact details of Standing on Giants 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 before the withdrawal;
- Any planned transfers of their information to a third country or international organisation and information on the safeguards being applied and how 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 Standing on Giants is a joint Controller of the information and if so an 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 how they can notify Standing on Giants to exercise one or more of these rights;

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

17.8. Accessing, processing and storage of Personal Information

17.8.1. **The Head of Solutions** 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.

17.8.2. 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.

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

17.8.4. Access to Personal Information must be provided per the **Access Control Policy**.

17.9. Requests by Information Subjects to exercise their rights and freedoms

For all Personal Information that Standing on Giants is the Controller of:

17.9.1. All requests by Information Subjects whose Personal Information is processed by Standing on Giants, to exercise their rights and freedoms under the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679) will be managed following the Handling of **Personal Information Requests Procedure**.

17.9.2. 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.

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

17.9.4. Where the request covers the deletion of information that has been made public then Standing on Giants 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.

17.10. Transferring Personal Information

17.10.1. 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 following the **Information Classification, Labelling and Handling Policy**.

17.10.2. If Standing on Giants needs to transfer Personal Information to a non-EU country or an international organisation then:

- Relevant Privacy Notices need 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 Standing on Giants will ensure are in place.

17.11. Compliance and Controls Assessments

17.11.1. To ensure that:

- All controls employed to protect Personal Information is controlled or processed by Standing on Giants are maintained and effective;
- Standing on Giants 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 accordance with the **Internal Audit Procedure**.

17.12. Arrangements with Joint Controllers

17.12.1. Standing on Giants is not a joint Controller of any Personal Information at the time of writing this document, this will be reviewed annually.

17.13. Arrangements with Controllers

Where Standing on Giants undertakes processing on behalf of a Controller

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

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

17.14. Arrangements with Processors

Where Standing on Giants uses a supplier to undertake processing on its behalf:

- A Personal Data Processing Contract (or an equivalent agreement) will be implemented with any Processors;
- 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;
- 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 Standing on Giants.
- 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.

17.15. High-Risk Processing

17.15.1. A data impact assessment must be completed for any High-Risk Processing of Personal Information that Standing on Giants is a Controller of before any such processing is started.

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

17.15.3. 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 the **Head of Solutions** must consult with the Information Commissioner's office before any processing is started.

17.16. Personal Information Breaches

17.16.1. 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 following the **Security Incident Management Procedure.**

18.0. Suppliers Policy

18.1. 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.

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

18.3. Information security-critical suppliers (ISCS)

18.3.1. The use of all ISCS must be approved by the **Head of Solutions**.

18.3.2. This use of all ISCS who undertake processing of Personal Information on behalf of Standing on Giants must be done following the **Protection of Personal Information Policy**;

18.3.3. 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**.

18.3.4. All information security risks identified that relate to the use of ISCS must be assessed and recorded in the **Asset and Risk Assessment Registe**r following the **Information Asset and Risk Management Procedure.**

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

- The scope of goods and services supplied by the ISCS is 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.

18.3.6. 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 are 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.
- It is the responsibility of the **Operations Manager** to create and maintain an **Approved Suppliers Register**.
- It is the responsibility of the **Operations 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.
- It is the responsibility of the **Operations 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 than once every 12 months by a qualified auditor.

19.0. Teleworking Policy

19.1. 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.

19.2. Teleworking authorisation

19.2.1. All teleworking must be approved by Each employee's line manager

19.2.2. 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.

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

19.3.1. 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.

19.3.2. Remote access to the organisation's information processing facilities will be authorised by the **Operations Manager**.

19.3.3. Remote access to the organisation's information processing facilities will be only accessible through a VPN.

19.4. Organisation-provided equipment for teleworking

19.4.1. 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**.

19.5. Use of teleworker-owned equipment for teleworking

19.5.1. Teleworkers are permitted to use their own equipment following the **Access Control Policy** provided:

- The equipment is approved for use by the **Operations Manager**;
- The equipment is only used following 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.

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

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

19.5.4. Teleworkers must not allow individuals other than themselves to use the equipment

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

19.5.6. The teleworker must notify the **Operations Manager** of the disposal of any equipment and be willing to pass, by mutual agreement, the equipment to the **Operations Manager** to remove any of the organisation’s information assets that may still reside on it.

20.0. Use of Software Policy

20.1. 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.

20.2. Use of software

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

20.2.2. Users of software must be authorised to do so following the **Access Control Policy**.

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

20.3. Installation of software

20.3.1. Installation of software onto an asset must be authorised by the **Head of Solutions** and must be done following the **Change Control Procedure** and **Backup Policy**.

20.3.2. 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 **Head of Solutions**.

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

Policy Review

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.