Talk Think Do

Information Security Policy

Document Title	Information Security Policy
Owner	Matthew Hammond
Master copy Location	https://matttalkthinkdoco.sharepoint.com/:w:/s/TalkThinkDo/EQIlA194OUpKrIPR2hPcTqoBJU eAJudPYf4ObLKE7ydxbQ?e=QNvkpv talkthinkdo.sharepoint.com/documents/2022
Change control	This is a version-controlled document, printed copies or those stored anywhere other than the file location stated above, are considered uncontrolled and the document in that file should be referenced in the first instance
Review and Approval Authorisation	Matthew Hammond Louise Clayton Daniel Meineck
Circulation	All Employees

Signed by Founder, Matthew Hammond:	

Document History

Issue Date	Version	Details of Change	Author
15/01/2022	0.1	First Draft	Matthew Hammond
09/03/2022	1.0	Amendments & sign off	Matthew Hammond
27/04/2022	1.1	Adding CEO signature	Matthew Hammond
04/05/2022	1.2	Added 16.1.4 & updating 9.2.5 (minor change therefore no update to public version required)	Amy St Louis
05/01/2023	1.3	Job title, responsibility, and format changes	Louise Clayton
18/01/2023	1.4	Minor changes to made throughout	Amy St Louis
20/02/2023	1.5	Changes to names of documents, removing out of date information, etc.	Amy St Louis
23/03/2023	1.6	Include use of MS Intune	Amy St Louis

Document Distribution

Name	Version	Title	Issue date
All employees	1.0	Information Security Policy	22/03/2022
All employees & public version	1.3	Information Security Policy	05/01/2023
Hodder Education	1.3	Information Security Policy	13/01/2023
TTD Website	1.6	Information Security Policy	23/03/2023

1.0. Policy Objective

1.0. To protect the information assets that Talk Think Do 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.

2.0. 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.

3.0. 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 Directors of Talk Think Do Limited are 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.

3.2. The maintenance and regular testing of a Business Continuity Plan.

3.2.1. The clear definition of responsibilities for implementing the ISMS.

3.2.2. 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.

3.2.3. The implementation and maintenance of the sub-policies 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 Senior 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 Engineering. Violations of this policy may be subject to the organisation's Disciplinary and Appeals Policy and Procedure.

4.0.   Sub-policy index

5.0.   Responsibilities

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

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

5.2.   It is the responsibility of the Head of Architecture 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.

5.3.   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 Head of Engineering any issues they may be aware of that breach any of its contents.

6.0.   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 Talk Think Do 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 (see Information Commissioner's Office Guidance on GDPR Compliance).

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 Information Classification, Labelling and Handling 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 (see Information Commissioner's Office Guidance on GDPR Compliance).

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 Talk Think Do 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 server: 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.   Remote worker: Any person that undertakes remote working on behalf of the organisation.

6.32.   Remote working: 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.

7.0.   Associated Documents

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

8.0.   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 Information Classification, Labelling and Handling Policy.

8.1.3.   Users must apply extreme caution when opening email attachments received from unknown senders. If in doubt, please ask the Head of Engineering 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 Head of Engineering.

- 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 Head of Engineering.

- 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 Head of Architecture for connection to any of the organisation's ECFs.

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

9.0.   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 a 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 Access Control Register.

9.1.4.   The Head of Engineering is responsible for:

- Ensuring no single person can access, modify or use the organisation's assets without authorisation or detection.

- Authorising and recording the use of any software that might be capable of overriding this sub-policy.

- Authorising and recording access to any software source codes.

- Authorising and recording individual user access to information processing facilities, electronic communication facilities, mobile devices, operating facilities and restricted access areas using an Asset and Access Control Review Form.

- Ensuring that individuals who enable and disable access to an organisation asset do not have access to any software that monitors the use of the asset.

- Ensuring that the access control for specific assets and information processing facilities meets the security requirements of each information asset owner.

- Regularly reviewing the logs of system administrator access and actions.

9.2.   Control of access to information processing facilities

9.2.1.   The Office & Finance Assistant is responsible for:

- Arranging access with the relevant Access Authorities & Access Providers 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 Access Providers 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.

9.2.2.   The relevant Access Provider is responsible for:

- Responding in a timely manner to requests for the activation and deactivation of user account access made to them by the Office & Finance Manager.

- Configuring and reviewing user access to the organisation's assets and information processing facilities as specified in the Access Control Register.

- Removing any expired or unused accounts.

- Testing that deactivated, deleted and removed accounts are no longer accessible.

- Implementing access control systems and mechanisms for the organisation's assets and information processing facilities as directed by the Managing Director.

- Logging and monitoring all access to the organisation's assets and information processing facilities and providing access logs where requested to do so.

- Ensuring that access log files cannot be edited or deleted.

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

- Passwords must be at least 12 characters in length.

- Passwords must be a combination of upper-case, lower-case, numeric and symbol characters.

- Passwords must automatically expire every 90 days.

- 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 15 minutes or less where the user is prompted to enter a password to access the system.

9.2.4.   The Head of Engineering is responsible for:

- Granting permanent or temporary access to restricted areas.

- Reviewing access to restricted areas every 30 days 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 via the appropriate Microsoft Form 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, Remote working Policy and Mobile Devices Policy.

- Be set to timeout after 5 minutes of inactivity.

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 Managing Director.

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 Office & Finance Assistant.
- Accompanying visitors that are in their care at all times, and not allowing them to enter any unauthorised location.
- Immediately reporting to the Office & Finance Assistant 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 Office & Finance Assistant 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:

- Be accompanied by a member of the organisation's staff at all times.
- 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:

- Be managed and approved in accordance with the Suppliers Policy;
- Be appropriately inducted into the organisation by the relevant authority;
- Not access areas other than those identified as appropriate to perform the contracted tasks;
- Immediately report any accidental breaches of this policy to the Managing Director.
- 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.   Access to customer networks should only be made using credentials supplied by the customer.

9.6.2.   Requests for credentials to access customer networks must be authorised by the Head of Engineering.

10.0. 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 SharePoint and retained for 3 years (where appropriate). 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.

10.1.2.   Backups must be made in accordance with the Electronic Data Backup Register.

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 SharePoint and retained for 5 years.

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 Register.

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 Information Classification, Labelling and Handling Policy and the Electronic Data Backup Register.

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 least annually in accordance with the Business Continuity Plan and the Electronic Data Backup Register.

11.0.   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 Information Classification, Labelling and Handling Policy, when not in immediate use and whenever the room they are being used in is vacated unless the room is vacated in accordance with the Fire Evacuation Procedure.

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.

12.0. 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 and in accordance with the Communications Register.

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 Project Management Office (PMO).

12.1.2.   *Any information exchanged with third parties must be done in accordance with the Information Classification, Labelling and Handling 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 Manging Director.

12.2. Employee briefings

12.2.1.   The PMO 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.

13.0. 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.   Removable media is prohibited at Talk Think Do.

13.1.4.   Data on a mobile device 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

13.3.1.   Fixed hard drives are encrypted using BitLocker, which is enforced using Microsoft Intune and is managed by the Head of Engineering.

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

14.0.   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.

14.1.   Classification

14.1.1.   It is the responsibility of the PMO 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.

14.2.   Labelling

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

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

14.3.   Copying

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

14.4.   Distribution

14.4.1.   Information assets should only be distributed:

- To comply with client requirements.

- To comply with legal requirements.

- On a need-to-know basis.

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

14.5.   Destruction

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

15.0. Mobile Devices Policy

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

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

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

15.1.   Issuing of mobile devices

15.1.1.   The issue of any mobile device to a user must be authorised by the Managing Director and recorded in the Equipment and Maintenance Register.

15.2.   Use of company mobile devices

15.2.1.   All users of mobile devices must comply with the <u>Acceptable Use of Assets Policy</u>, <u>Clear Desk and Clear Screen Policy</u>, <u>Backup Policy</u>, <u>Remote working Policy</u> and the <u>Use of Software Policy</u>.

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

15.2.3.   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.

15.2.4.   In an emergency situation, a user may allow an individual to make a supervised call from a mobile.

15.2.5.   Users must immediately notify the Office & Finance Assistant if a mobile device is known or suspected to be lost or stolen.

15.2.6.   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.

15.2.7.   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.

15.2.8.   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.

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

15.2.10.   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 Managing Director.

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

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

15.2.13.   Mobile devices must always be protected from unauthorised use by an access password in accordance with the <u>Access Control Policy</u>.

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

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

15.3.   Return of mobile devices

15.3.1.   Upon request by the Line Manager, termination of contract or change of role, a user must return any mobile devices they have been issued with to the Office & Finance Assistant.

15.3.2.   All mobile devices must be returned to the Office & Finance Assistant and recorded <u>Equipment and Maintenance Register</u>.

16.0.   Physical and Environmental Security Policy

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

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

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

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

16.1.   Physical protection of operating facilities

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

16.1.2.   All operating facilities must be protected by a security camera that is remotely monitored by the Head of Architecture or office security.

16.1.3.   All external doors must be kept shut and locked at all times unless authorised by the Office & Finance Assistant.

16.1.4.   Anyone who does not have access to the operating facilities will need to ring the doorbell or check in with security in order to gain access.

16.2.   Environmental protection of operating facilities

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

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

16.2.3.   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.

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

- Implemented with monitoring/backup to pro-actively alert/failsafe in the event of failure.

- Adequately maintained to ensure reliability.

16.3.   Protection of assets at operating facilities

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

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

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

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

16.3.5.   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.

17.0. Protection from Malware Policy

17.0.   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.

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

17.1.1.   It is the responsibility of the Head of Engineering 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.

17.1.2.   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.

17.1.3.   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.

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

17.1.5. 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.

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

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

17.1.8. All anti-virus software must be configured to generate log files, and to store these log files either locally on the computer system or mobile device or centrally on a organisation-wide anti-virus server (if applicable). All logs must be kept for a minimum of 90 days.

17.2. Other processes, systems and tools to deter malware

17.2.1. 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.

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

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

17.3. Requirements of users

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

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

17.3.3. 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.

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

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

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

18.0. Protection of Personal Information Policy

18.0. 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 Talk Think Do Limited complies with and can demonstrate compliance with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

18.1. Application of the Personal Information protection principles

18.1.1. 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 Talk Think Do Limited's information assets and any Personal Information that Talk Think Do 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.

18.1.2. 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 Talk Think Do Limited's Assets that impact on the processing of Personal Information, the Change Control Procedure must be applied.

18.2. Registration with the Information Commissioner

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

18.3. Record of Processing Activity

18.3.1. It is the responsibility of Data Protection Officer to ensure that a Record of Processing Activity is maintained that contains information on:

- All Personal Information that Talk Think Do Limited is the Controller of regardless of whether it is processed by Talk Think Do Limited or by a Processor engaged by Talk Think Do Limited;

- All Personal Information that Talk Think Do 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 Talk Think Do Limited is the Controller) or direct Sub-Processors used (where Talk Think Do 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.

18.4. Consent to Process Personal Information

18.4.1. Where Talk Think Do 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 + Consent Opt-in Form.

18.5. Processing of Personal Information obtained from an Information Subject

18.5.1. Where Talk Think Do 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:

- 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 Talk Think Do 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 Talk Think Do Limited to exercise one or more of these rights.

18.6.   Processing of Personal Information obtained from third parties

18.6.1.   Where Talk Think Do 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 Talk Think Do 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.

18.6.2.   Talk Think Do Limited will provide the following information to Information Subjects about whom the Personal Information relates to:

- The name and contact details of Talk Think Do Limited's 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 Talk Think Do 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 Talk Think Do Limited to exercise one or more of these rights.

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

18.7. Accessing, processing and storage of Personal Information

18.7.1. The Head of Engineering 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.

18.7.2. 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.

18.7.3. Personal Information should be accessed, processed and stored in accordance with this policy, the specifications detailed in the Record of Processing Activity and the Information Classification, Labelling and Handling Policy.

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

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

For all Personal Information that Talk Think Do Limited is the Controller of:

18.8.1. All requests by Information Subjects whose Personal Information are processed by Talk Think Do 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 Handling of Personal Information Requests Procedure.

18.8.2. 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.

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

18.8.4. Where the request covers the deletion of information that has been made public then Talk Think Do 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.

18.9. Transferring Personal Information

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

18.9.2. In the event that Talk Think Do 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 Talk Think Do Limited will ensure are in place.

18.10. Compliance and Controls Assessments

18.10.1. To ensure that:

- All controls employed to protect Personal Information is controlled or processed by Talk Think Do Limited are maintained and effective;

- Talk Think Do 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 and in accordance with the Internal Audit Procedure.

18.11. Arrangements with Joint Controllers

18.11.1. Where Talk Think Do Limited is a joint Controller of any Personal Information then a Joint Controller Agreement (or an equivalent agreement) will be implemented with any joint Controllers.

18.12. Arrangements with Controllers

Where Talk Think Do Limited undertakes processing on behalf of a Controller

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

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

18.13. Arrangements with Processors

Where Talk Think Do Limited uses a supplier to undertake processing on its behalf:

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

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

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

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

- The information obtained from a Personal Information Processor Assessment raises doubts as to the adequacy of the guarantees provided by a Processor; or

- The supplier is undertaking High Risk Processing; or

- An information security incident occurs that has a significant impact on the confidentiality or integrity or availability of any Personal Information and following an investigation of the root cause of the incident, the controls and processes employed by the supplier are identified as having been a contributing factor.

18.14. High Risk Processing

18.14.1. A data impact assessment must be completed for any High-Risk Processing of Personal Information that Talk Think Do Limited is a Controller of before any such processing is started.

18.14.2. The results of the data impact assessment must be recorded in the Record of Processing Activity.

18.14.3. 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 Head of Engineering must consult with the Information Commissioner's office before any processing is started.

18.15. Personal Information Breaches

18.15.1. 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

19.0. 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.

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

19.2. Information security critical suppliers (ISCS)

19.2.1. The use of all ISCS must be approved by the Managing Director.

19.2.2. This use of all ISCS who undertake processing of Personal Information on behalf of Talk Think Do Limited must done in accordance with the Protection of Personal Information Policy.

19.2.3. 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.

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

19.2.5. 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.

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

- Subcontracting of the supply of goods and services by the ISCS to third parties;

- Access control to the organisation's assets by ISCS employees and subcontractors;

- Resilience, recovery and contingency arrangements to ensure the availability of any assets including any information processing facilities provided by the ISCS and/or the organisation;

- Accuracy and completeness controls to ensure the integrity of the assets, information or information processing equipment/facilities provided by the ISCS and/or the organisation;

- Processes and/or procedures for transferring information and/or information processing facilities between the ISCS, the organisation and other third parties;

- Screening checks undertaken on ISCS employees and subcontractors;

- Awareness training for ISCS employees and subcontractors;

- Any legal and regulatory requirements, including information protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;

- ISCS obligation to periodically deliver an independent report on the effectiveness of controls.

19.2.7.	It is the responsibility of the PMO to create and maintain an Approved Suppliers Register.

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

19.2.9.	It is the responsibility of the PMO 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.

20.0. Remote working Policy

20.0.	This sub-policy specifies the controls that need to be applied to remote working 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.	Remote working authorisation

20.1.1.	All remote working must be approved by the Line Manager.

20.1.2.	The scope of a remote worker's remote working must be defined to include:

- 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.	Organisation-provided equipment for remote working

20.2.1. Where equipment is provided to the remote worker for remote working, the remote worker must comply with the Acceptable Use of Assets Policy, Mobile Devices Policy and Use of Software Policy.

20.2.2. Microsoft Intune must be in use across all organisation-provided equipment and must be set-up prior to new starters leaving with equipment

20.3. Use of remote worker-owned equipment for remote working

20.3.1. Remote workers are permitted to use their own equipment in accordance with the Access Control Policy provided:

- The equipment is approved for use by the Head of Engineering.

- The equipment is only used in accordance with the approved scope of their remote working 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.

- All equipment Is enrolled with MS Intune.

20.3.2. The remote worker is responsible for ensuring the equipment is not accessed by any unauthorised person while the equipment is being used for work purposes.

20.3.3. Remote workers must take extra care when using any equipment for remote working to protect it from theft and damage.

20.3.4. Remote workers must ensure all equipment is kept secure, in locked premises when left unattended.

20.3.5. Remote workers must ensure equipment is not used by any other individuals.

20.3.6. Remote workers must escalate any issues with equipment to their line manager who will arrange for repair or replacement.

20.3.7. The remote worker must report any loss or theft of any equipment that has been used for remote working to their line manager.

20.3.8. The remote worker must notify their line manager of the disposal of any equipment and be willing to pass, by mutual agreement, the equipment to their line manager for the purpose of removing any of the organisation's information assets that may still reside on it.

21.0. Use of Software Policy

21.0. 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.

21.1. Use of software

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

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

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

21.2. Installation of software

21.2.1. Installation of software onto an asset must be authorised by the Head of Engineering and must be done in accordance with the Change Control Procedure and Backup Policy.

21.2.2. 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 Engineering.

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

21.3. Policy Review

21.3.1. 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.