CORE TO CLOUD™

INFORMATION SECURITY POLICY

1.0. Policy objective

1.1. To protect the information assets that Core to Cloud 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 provide protection for 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 organisation is 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 27001:2013.

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 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 Board of Directors. Violations of this policy may be subject to disciplinary action.

Signed on behalf of Board of Directors

Position: COO Date: 15/6/23

4.0.Sub-policy index

5.0.Responsibilities

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

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

5.3. It is the responsibility of the COO 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 Management Team any issues they may be aware of that breach any of its contents.

5.5. All Employees should be familiar with the sub policies within this document.

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

6.5. **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.

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

6.7. **Data protection principles**: Principles that shall be applied in relation to all personal information as laid down in the Data Protection Act 1998 and any subsequent amendments.

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

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

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

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

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

6.13. **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.

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

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

6.16. **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.

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

6.18. **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.

6.19. **Personal information**: Information that relates to a living individual who can be identified from the information, or from other information, which is in the possession, or is likely to come into the possession, of the organisation.

6.20. **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.

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

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

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

6.24. **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.

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

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

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

6.28. **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 highlighted 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 in accordance with 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 in accordance with 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 CTO for advice.

8.2.4. Comply with the Email Internet and Social Media Use Policy within the **Employee Handbook**

8.2.5. Users must not:

- Disclose user IDs and personal password.
- s which gives access to the organisation's assets unless authorised by the CTO.
- 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 **Employee Handbook**

- 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.

8.2.6. Any user supplied equipment must be approved by the CTO for connection to any of the organisation's ECFs.

8.2.7. 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 director of the organisation.

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

9.2.3. Users are not permitted to operate their PC (such as using email or web browsing) via the provided service account. This account is only to allow software update and required configuration changes. These software changes and installs have to be authorised by the CTO.

9.2.4. 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**.

9.2.5. Access to Internet based firewalls and routers is permitted for management. This is due to the equipment we utilise being an SD-WAN and Cloud Managed Routers which are all internet based.

9.2.6. The CTO 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.

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

9.3.1. The COO is responsible for:

- Arranging access with the CTO 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 CTO 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 CTO is responsible for:

- Responding in a timely manner to requests for the activation and deactivation of user account access made to them by the COO.
- Providing staff with a standard PC account as well as a service account to allow required changes when the user is offsite.
- 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 COO.
- Logging and monitoring all access to the organisation's assets and information processing facilities and providing access logs were 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:

- Office 365 Passwords must be at least 8 characters in length and with 2FA Enabled.
- The PC login passwords must be at least 8 Characters and be a non-guessable password.

- An example of a non-guessable password that is difficult to guess will be unique and not be made up of common or predictable words such as 'password' or 'admin', or include predictable number sequences such as '12345'.

- Passwords must be a combination of Upper Case, Lower Case and Complex characters;
- Office 365 Passwords are set to automatically expire every 365 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 20 minutes or less where the user is prompted to enter a password to access the system.
- Passwords if stored must be stored securely such as in a password vault or encrypted medium.
    - As per email sent to Staff 14/6/21 Core to Cloud recognises https://bitwarden.com or https://keepass.info/ as suitable stores and recommends but doesn't enforce this. Alternatively, they can be stored within the encrypted work device within the browser.

9.3.4. The COO is responsible for:

- Granting permanent or temporary access to restricted areas;
- Reviewing access to restricted areas every quarter 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 Protection 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 online systems must:

- Only be provided to authorised users;
- Only be used with approved assets, in accordance with the **Acceptable Use of Assets Policy**, **Teleworking Policy** and **Mobile Devices Policy**;
- Be utilised only through our secure Software defined WAN.

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

9.5.1. Access to the organisation's operating facilities must be authorised by COO.

9.5.2. Access to the organisation's operating facilities will be processed and granted by the COO.

9.5.3. 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.

9.5.4. 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 COO.
- Accompanying visitors that are in their care at all times, and not allowing them to enter any unauthorised location;
- Immediately reporting to the COO 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.

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

9.6. **Visitors and suppliers**

9.6.1. All visitors must:

- Sign in at reception;
- Be accompanied by a member of the organisation's staff at all times;
- Not be allowed access to any restricted areas without the relevant authorisation to do so;
- Display the visitor's pass provided to them at reception;
- Return passes to reception when they leave the organisation's premises, even if for a limited period such as lunchtime;
- Not attempt to access any of the organisation's assets and information processing facilities or view any of the organisation's information without authorisation to do so.

9.6.2. All suppliers working in an operating facility must:

- Sign in at reception;
- Be managed and approved in accordance with the **Suppliers Policy**;
- Be appropriately inducted into the organisation by the relevant authority;
- Not access areas other than those identified as appropriate to perform the contracted tasks;
- Display a visitor's pass at all times;
- Return passes to reception when they leave the organisation's premises, even if for a limited period such as lunchtime;
- Immediately report any accidental breaches of this policy to the COO.
- Not access or view any information that has not been provided as part of the contracted task.

9.7. **Remote access to customer networks**

9.7.1. Core to Cloud operate a guest WIFI which is a separate SSID and VLAN and which will not allow routing to the internal network. This is to be utilised by all non-core to cloud employees visiting the building.

10.0. Backup Policy

10.1. 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. As Core to Cloud operate cloud hosted software no software beyond the logins to these systems needs to be stored.

10.3. **Electronic files**

10.3.1. As Core to Cloud operate cloud hosted storage no corporate data is permitted to be stored on laptops in non redirected folders and therefore should be placed within My Documents and Desktop which will place it all within The Corporate One Drive. Backups of One Drive, Office 365 email and SharePoint are made to the companies backup solution – at minimum daily.

10.3.2. Backup copies of all electronic files stored in the cloud that contain information assets, including previous versions, must be made daily, stored with a separate storage area to the source and retained for 365 days.

10.3.3. 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**.

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

10.3.5. Backups must be made in accordance with 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 within a separate cloud area to the live system.

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 Twice a year in accordance with the **Business Continuity Plan, Restore Test Procedure** 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, 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 Procedures** displayed within the Castle.

11.2.2. 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.

11.3. **Display screens**

11.3.1. Equipment that utilises display screens must have a screensaver or screen lock enabled with password protection that activates automatically after 20 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 with regards to internal and external communications relevant to the ISMS and in accordance with the **Communication Procedure**.

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 COO or, in their absence, the CTO.

12.2.2. Any information exchanged with third parties must be done in accordance with the **Information Classification, Labelling and Handling Policy** and the **Information Classification, Labelling and Handling Rules**.

12.2.3. Supply of information about the organisation's ISMS, including policies, procedures and specific control measures employed must be approved by the COO

12.3. **Employee briefings**

12.3.1. The Senior Management Team 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. This will also be delivered to new starters as part of their initial technical briefing.

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 prior to transfer.

13.2.3. All removable media, including memory sticks, must be encrypted and the use of this medium is blocked unless requested and signed off. Employees should make use of the provided corporate One Drive.

13.2.4. Retired removable media must be passed to the CTO for Disposal.

13.2.5. Mobile device hard drives must be encrypted.

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

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

13.2.8. 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 which is already in the public domain, or would be of no adverse significance if it were to be so, may be sent unencrypted.

13.4. **Key management**

13.4.1. Encryption Keys for Laptops are stored within the Sophos UTM Console. This is controlled from this console as well.

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

13.5.1. 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.

13.6. **Avoiding adverse impacts from encryption**

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

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

13.6.3. 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 CTO to maintain the **Information Classification, Labelling and Handling Rules** 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 in accordance with the **Information Classification, Labelling and Handling Rules**.

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 in accordance with **Information Classification, Labelling and Handling Rules**.

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 in accordance with **Information Classification, Labelling and Handling Rules**.

14.6. **Destruction**

14.6.1. Destruction of an information asset must be done in accordance with 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 COO and recorded within the Asset Register.

15.2.2. All users must sign and return a **Device User Agreement**.

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. Only Apple Mobile Phones are supported and authorised applications are listed within this document under **Appendix 1**

15.3.3. Corporate mobile phones should be protected with Lookout Mobile Security.

15.3.4. 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.

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

15.3.6. Users must immediately notify the CTO if a mobile device is known or suspected to be lost or stolen.

15.3.7. 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.

15.3.8. 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.

15.3.9. 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.

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

15.3.11. Mobile devices should only be transported in the bags or cases with which they were supplied.

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

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

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

15.3.15. Mobile devices must not be used to store passwords, safe/door combinations, or classified, sensitive or proprietary information unless they are encrypted.

15.4. **Return of mobile devices**

15.4.1. Upon request by the COO termination of contract or change of role, a user must return any mobile devices they have been issued with to their line manager.

15.4.2. All mobile devices must be returned to the Line Manager and recorded within the corporate asset register.

15.4.3. All users must complete their **Device User Agreement** upon return.

16.0. Physical and Environmental Security Policy

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

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

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

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

16.2. **Physical protection of operating facilities**

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

16.2.2. All operating facilities must be protected by an intruder alarm system

16.2.3. All external windows and doors must be kept shut and locked at all times unless authorised by the COO.

16.3. **Environmental protection of operating facilities**

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

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

16.3.3. Any systems identified as being vulnerable to power outages should be protected by uninterruptable power supplies (UPS), such a battery backup.

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

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

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

16.4.3. 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**.

16.4.4. 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**.

16.4.5. 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

17.1. 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.

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

17.2.1. It is the responsibility of the CTO 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.

17.2.2. 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.

17.2.3. 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.

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

17.2.5. 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.

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

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

17.2.8. All anti-virus software must be configured to store status information within the host cloud environment.

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

17.3.1. Installed AV software will scan attachments and we have the native protection provided within the Microsoft Office 365 environment.

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

17.4.1. 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.

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

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

17.5. **Requirements of users**

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

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

17.5.3. 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.

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

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

17.5.6. Users must seek advice from the CTO if their computer system or mobile device requests them to install or update software they have not seen before – such as beyond standard windows and application updates.

18.0. Protection of Personal Information Policy

18.1. 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 the organisation and its employees comply with the Data Protection Act 2018.

18.2. **Application of the data protection principles**

18.2.1. The following principles must be applied in relation to all personal information that is accessed, stored or processed by employees, and employees or subcontractors of information security critical suppliers, while they are accessing or processing the organisation's information assets:

- Personal information shall be processed fairly and lawfully;
- Personal information shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Personal information shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
- Personal information shall be accurate and, where necessary, kept up-to-date;
- Personal information shall not be kept for longer than is necessary for that purpose or those purposes;
- Personal information shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018;
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information;
- Personal information shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

18.3. **Registration with the Information Commissioner**

18.3.1. It is the responsibility of the COO to ensure that the appropriate registration is maintained with the Information Commissioner.

18.4. **Accessing, processing and storage of personal information**

18.4.1. The Senior Management Team must ensure that appropriate physical and technical controls are in place to prevent unauthorised access to personal information.

18.4.2. 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.

18.4.3. Personal information should be accessed, processed and stored in accordance with the **Information Classification, Labelling and Handling Policy**.

18.4.4. Access to personal information must be provided in accordance with the **Access Control Policy**.

18.5. **Transferring personal information**

18.5.1. 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**.

18.5.2. Personal information must never be transferred to any country or territory outside the European Economic Area unless that country or territory ensures an adequate level of data protection.

19.0. Suppliers Policy

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

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

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

19.3.1. The use of all ISCS must be approved by the Senior Management Team. This approval must be completed and recorded in accordance with the **Improvement Procedure**.

19.3.2. 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**.

19.3.3. 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**.

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

19.3.5. 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 data 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 data 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.

19.3.6. It is the responsibility of the COO to create and maintain an **Approved Suppliers Register**.

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

19.3.8. It is the responsibility of the COO to ensure that the information security controls specified in the **Supply of Goods and Services Agreement** or equivalent, are audited at a frequency of not less that once every 12 months in accordance with the **Supplier Audit Procedure**.

20.0. Teleworking Policy

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

20.2. **Teleworking authorisation**

20.2.1. Teleworking is approved for all employees provided they have a device utilising Core to Cloud core security products which includes Anti-Virus and the SD-WAN Connection)

20.2.2. 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.

20.3. **Accessing the organisation's system from teleworking locations**

20.3.1. 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.

20.3.2. Remote access to the organisation's systems will be over and approved SD-WAN VPN.

20.4. **organisation-provided equipment for teleworking**

20.4.1. 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**

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

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

- The equipment is approved for use by the COO/CTO.
- The equipment is only used in accordance with the approved scope of their teleworking and Section 16.2 of this sub-policy;
- The equipment is not set to automatically connect to non-trusted 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 20 minutes**.**
- Users should lock their device when leaving their desk.

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

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

20.5.4. Users working from home should secure any sensitive company information.

20.5.5. The teleworker must report any loss or theft of any equipment that has been used for teleworking to the organisations systems.

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

21.0. Use of Software Policy

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

21.2. **Use of software**

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

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

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

21.3. **Installation of software**

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

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

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

22.0. Policy Review

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

Appendix 1 – Supported IOS Applications

The following Applications are supported by Core to Cloud for use on their Phones.

Abby BCR
360
8 Ball Hero
Acast
accor hotels
Airbnb
Alexa
All 4
Amazon
Amazon Alexa
Among US
App Store
Apple Store
Apple TV
Arhos
Arsenal
ASOS
ASUS Routers
Audible
Authenticator
Auto Trader
Avatarify
BabyName
Bandcamp
Barclays
BBC Iplayer
BBC News
BBC Sounds
BBC Sport
Beathe HR
Bet365
Betway

Blinkist
Booking.com
Books
Boomerang
Brighttalk
British Gas
BT email
BT Sport
Calculator
Calendar
Camera
Capital One
Cato Client
Centr
Chrome
Cineworld
Clips
Clock
Color Bump 3D
Compass
Contacts
Costa
Cozi
Crossy Road
Daddy Up
David Lloyd
Deezer
Deliveroo
Dentist Bling
Discord
Disney+
Ebay
Emma
END.
Evernote
Excel
Experian
FaceBook
Facetime
Files
Fill
Find My
Firefox
Fonts
Fruit Ninja
Gacha Life
GarageBand

Garmin Connect
Geometry Lite
Glofoxx
GO 4 Schools
Go to Webinar
Golfnow
Good Food
Google
Google Authenticator
Google Maps
Groceries (Tesco)
Habitica
Handelsbanken
HappyCow
Headphones
Heads Up!
Headspace
Health
High Heels!
HMRC
Hoburne
Home
Hotels.com
Houseparty
HSBC
IDU Mobile
IMDb
iMovie
inflow
Instagram
Instasize
iTunes
iTunes Store
ITV 7
ITV Hub
Jabra Sound+
Jane Video
John Lewis
Just Eat
Kahoot!
Keynote
KyPass
Linkedin
Lloyds bank
Lookout Work
Magic Tiles 3
Mail

Maps
Maps (Apple)
Measure
Messages
Messenger (facebook)
Met office
Microsoft 365 admin
Microsoft Authenticator
Music
MyFitnessPal
MySky
Myzone
National Trust
Nattional Lottery
Nectar
Netflix
News
NHS COVID 19
Nike Run Club
NordVPN
Notes
NOW
Numbers
Oculus
Office
One Drive
OneNote
OpenTable
Outlook
Pags
Pardot
Paypal
Phone
Photo
Photo-Editor
Photos
Pinterest
Planner
Pleo
pleo
Plex
Podbean
Podcasts
Pokemon GO
Power automate
Powerpoint
Premier League

Prime Video
Rec Room
Reddit
Reminders
Renpho
Rightmove
Roblox
Safari
Sales Navigator
Salesforce
Salesforce Authenticator
Santander
Score! Hero 2
Scribzee
Seconds
Settings
Sharepoint
Shazam
Shop
Shortcuts
Signal
Six!
Sky Go
Sky news
Sky Sports
Skyscanner
Slack
Sleep Cycle
Smartthings
SmartView_Frame
Snake VS Block
Snapchat
Sonos
Soundcloud
Speedtest
Splash
Spotify
Starling
Stocks
Strava
Surfshark
Teams
The Athletic
The Calculator
The National Lottery
The Times
TikTok
Tile

Tiles Hop
Timehop
Times Radio
Tips
TOFU GIRL
Training
Trainline
Translate
Trello
Trip Advisor
TUI
Tupe Map
TV
Twitter
Uber Eats
Vanquis
Virgin Media Connect
Visio Viewer
Vivino
Voice Memos
Wallet
Watch
Waze
Weather
Webex Meet
WhatsApp
Wiltshire Walks
Word
Words 2
XE
Xero
Yahoo Mail
You Tube
Youtube
Zara
Zoom
Zoopla