r

Information Security Policy

INTERNAL USE ONLY

Version

2.3

DOCUMENT CONTROL

Document Information

Document Title	information Security Policy
Version	2.3
Publication Date	13 October 2017
Status	Approved
Review Date	15 January 2025

Revision History

Version	Date	Author/Reviewer	Details
1.0	15 November 2015	Q.Sheikh	Initial Release
1.0	01 December 2016	Q.Sheikh	Review
2.0	30 November 2017	Q.Sheikh	Updated for GDPR and ISO27001 inclusion
2.0	20 December 2018	Q.Sheikh	Review
2.1	29 December 2018	Q.Sheikh	Review /password policy updates as per NCSC/Cyber Essentials PLUS guidelines
2.1	06 January 2020	J.Holmes	Review
2.1	06 January 2021	Q Sheikh	Review
2.1	06 January 2022	Q Sheikh	Review
2.2	24 January 2023	Q Sheikh	Review
2.3	16 January 2023	Q Sheikh	Review /logo update

Classification

PROTECT - INTERNAL

Legal Notice

This document may contain valuable trade secrets and confidential information of Visav Ltd, and shall not be disclosed to any person, organisation, or entity unless such disclosure is subject to the provisions of a written non- disclosure and proprietary rights agreement or intellectual property license agreement approved by Visav Ltd

Content

1. POLICY OBJECTIVES

The objectives of this policy are to:

- Protect the information assets that VISAV LTD handles, stores, exchanges, processes and has access to and ensure the ongoing maintenance of their confidentiality, integrity and availability.
- Ensure controls are implemented that provide protection for information assets and are proportionate to their value and the threats that they are exposed to.
- Ensure VISAV Ltd complies with all relevant legal, customer and other third party requirements relating to information security.
- Continually improving VISAV Ltd.'s information security management system and its ability to withstand threats that could potentially compromise information security.

2. SCOPE

This policy and its sub-policies apply to the all people, processes, services, technology and assets detailed in the **ISMS Scope**. It also applies to all employees or subcontractors of Information Security Critical Suppliers who access or process any of VISAV Ltd.'s Information Assets.

3. CORE POLICY

VISAV LTD believes that despite the presence of threats to the security of such information, all security incidents are preventable.

VISAV Ltd is committed to achieving the objectives detailed in the policy through the following means:

- The implementation and maintenance of an Information Security Management System (ISMS) that is independently certified as compliant Cyber Essentials Plus.
- The systematic identification of security threats and the application of a risk assessment procedure that will identify and implement appropriate control measures.
- Regular monitoring of security threats and the testing/auditing of the effectiveness of control measures.
- The maintenance of a risk treatment plan that is focussed on eliminating or reducing security threats.

- The maintenance and regular testing of a **Business Continuity Plan**.
- The clear definition of responsibilities for implementing the ISMS.
- 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.
- The implementation and maintenance of the sub-policies detailed in this policy

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

The implementation of this **Information Security Policy** and the supporting policies and procedures is fundamental to the success of VISAV Ltd.'s business and must be supported by all employees as an integral part of their daily work and all suppliers who have an impact on.

All information security incidents must be reported to Security and Infrastructure Director who will report it to IT Director if required.

Violations of this policy may be subject to VISAV Ltd.'s **Disciplinary Procedure**.

4. SUB POLICY INDEX

5. DEFINITIONS

The following definitions are used in this policy and all sub policies.

5.1. Anti-Virus Software

Software used to prevent, detect and remove malware. For the purposes of this policy anti-virus can also mean anti-malware and/or anti-spyware.

5.2. Asset

Any physical entity that can affect the Confidentiality, Availability and Integrity of VISAV Ltd.'s Information Assets.

5.3. Availability

The accessibility and usability of an Information Asset upon demand by an authorised entity.

5.4. Computer Systems

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

5.5. Confidential Information

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

5.6. Confidentiality

The restrictions placed on the access or disclosure of an Information Asset.

5.7. Data Protection Principles

Principles that shall be applied in relation to all Personal Information as laid down in the Data Protection Act 2018 and any subsequent amendments.

5.8. Electronic Communication Facilities (ECF)

Any Asset that can be used to electronically transfer information.(Office365, Slack, Skype, Telephone and Fax)

5.9. Equipment

Any Asset that can be used to electronically store and/or process information.

5.10. Electronic Messages

The electronic transfer of information by means such as email, texts, blogs, message boards and instant messaging.

5.11. Information Asset

Any information that has value to VISAV Ltd.'s stakeholders and requires protection.

5.12. Information Processing Facility (IPF)

Any network of Assets that can be used to electronically store, process or transmit information.

5.13. 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 VISAV Ltd.'s premises or access to the one or more of VISAV Ltd.'s Information Assets or provides software or hardware used in VISAV Ltd.'s Information Processing Facilities or Electronic Communication Facilities.

5.14. Integrity

The accuracy and completeness of an Information Asset.

5.15. Mail Server

A system based on software and hardware that sends, receives and stores electronic mail.

5.16. 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.

5.17. Mobile Device

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

5.18. Operating Facility

Any physical location containing Assets owned by VISAV Ltd that VISAV Ltd controls, including buildings, offices, departments and locations affiliated with VISAV Ltd that are used to create, access, store or process any of VISAV Ltd.'s Information Assets.

5.19. 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 of, or is likely to come into the possession of VISAV Ltd.

5.20. Remote Users

Users accessing VISAV Ltd.'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 VISAV Ltd.'s Information Processing Facilities.

5.21. Restricted Access

Any physical location where access is restricted to named personnel only.

5.22. Security Incident

Any event that has a negative impact on the Confidentiality and/or Integrity and/or Availability of an Information Asset.

5.23. Software

All programs and operating information used by Equipment.

5.24. Supply of Goods and Services Agreement

A legally binding contract between VISAV Ltd and a supplier for the supply of a defined scope of goods and services

5.25. Teleworker

Any person that undertakes Teleworking on behalf of VISAV Ltd.

5.26. Teleworking

The access, processing and storage of Information Assets at locations that are not under the control of VISAV Ltd.

5.27. User

Any person that uses one or more of VISAV Ltd.'s Assets.

5.28. Visual Aids

Any Asset used to display information to the occupants of a room.

6. ASSOCIATED DOCUMENTS

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

7. RESPONSIBILITIES

- It is the responsibility of the Security and Infrastructure Director to ensure that this policy is implemented and any resources required are made available.
- It is the responsibility of the Security and Infrastructure Director to monitor the effectiveness of this policy and report the results at management review meetings.
- It is the responsibility of the Security and Infrastructure Director to create and maintain an **Risk Assessment Register** and ensure all Assets that need to be covered by this policy are identified.
- It is the responsibility of the Line Managers to ensure that their permanent and temporary staff and contractors are aware of:
    - The information security policies applicable in their work areas
    - Their personal responsibilities for information security
    - How to access advice on information security matters
- It is the responsibility of the Line managers to ensure the security of the physical environments where information is processed or stored.
- It is the responsibility of all employees and employees or subcontractors of Information Security Critical Suppliers, to adhere to this policy and report to the Security and Infrastructure Director any issues they may be aware of that breach any of its contents.

8. ACCEPTABLE USE OF ASSETS POLICY

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

- authorise the use of any Asset owned by or under the control of VISAV Ltd; and
- minimise the risks to information security arising from the misuse or unauthorised use of VISAV Ltd.'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 VISAV Ltd.'s **Access Control Policy**.

8.1.2. Users must only use Assets to access and transfer information that they have been authorised for 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 VISAV Ltd for advice.

8.1.4. Users must not:

- Disclose user IDs and personal passwords which give access to VISAV Ltd.'s Assets unless authorised by the Security and Infrastructure Director.
- Allow any third party to access VISAV Ltd.'s EFCs.
- Use any access method other than the method provided to them by VISAV Ltd.
- Deliberately cause damage to any of VISAV Ltd.'s ECF, including maliciously deleting, corrupting or restricting access to data contained therein.
- Deliberately introduce viruses or other harmful sources of Malware in to VISAV Ltd.'s ECFs.
- Deliberately access external sources that are not authorised and not related to VISAV Ltd.'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 VISAV Ltd
- Assist or create a potential security breach or disruption to VISAV Ltd.'s ECFs in any way.
- Post personal entries to social media websites which includes any reference to VISAV Ltd or which allows such a reference to be determined.
- Social media may be used for business purposes on condition that no sensitive or potentially sensitive material, IP or similar material is disclosed. Users must behave responsibly while using any social media for business use, bearing in mind that they directly represent VISAV Ltd.
- Use any ECFs for any personal reasons, other than those authorised by VISAV Ltd.

8.1.5. Any User supplied equipment must be approved by the Security and Infrastructure Director for connection to any of VISAV Ltd.'s electronic communications facilities.

8.1.6. VISAV Ltd reserves the right to monitor all use of ECFs.

8.2. Equipment

8.2.1. All Users must:

- Protect the equipment provided to them by VISAV Ltd while it is in their care.
- Ensure they are familiar with the operation of the equipment and how this policy applies to its use and seek advice if they are in any doubt.
- Ensure they take sensible precautions to prevent theft, damage and un-authorised use or access to the equipment in their care.
- Ensure equipment is not used or stored in physical locations that they were not designed to function in, such as environments with extremes of temperature or high levels of moisture
- Promptly report the theft of any equipment to the Managing Director
- Not interfere with any system configurations or software supplied by VISAV Ltd intended to aid the equipment's security.

8.2.2. All equipment that has the facility to be password protected must have one set and be configured to require the password to be entered on boot/power up.

8.2.3. For equipment that has a screen or facility to produce an image, users must ensure they adhere to the **Clear Desk and Clear Screen Policy**. As a minimum screen saver with password protection should be set to activate automatically after 15 minutes of inactivity.

8.2.4. All data shall be removed from hardware before disposal.

8.3. Removable Media

8.3.1. Official removable media **is** provided centrally, and its use **is** recorded (e.g. serial number, date, issued to, returned). Where indicated by a risk assessment, systems are prevented from using removable media. Use of personal removable media in business information systems (e.g. USB sticks, CD, DVD etc.) is forbidden unless approved by the Security and Infrastructure Director.

8.3.2. Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Security and Infrastructure Director before they may be used on business systems. Such media must also be fully virus checked before being used on the organisation's equipment.

8.4. Electronic Messages

8.4.1. Electronic Messages should not be used for the transfer of sensitive, personal and confidential information.

8.4.2. Users must ensure that the content of their Electronic Messages and not include any details or remarks that will breach clause 8.5 below.

8.5. Telephony

8.5.1. All calls made from and to a given telephone extension are logged and monitored users should presume no privacy at any time. Although

voicemail is password protected, an authorised administrator can reset the password and listen to voicemail messages in accordance with Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

8.5.2. Information must never be given out over the phone unless it is absolutely clear whom it is being given to and that they are entitled to the information and are ready and able to accept it.

8.5.3. Care must be taken to ensure that conversations involving confidential and/ or personal information cannot be overheard.

8.5.4. Voicemail messages containing personal information should only be left after due consideration has been given to any security and confidentiality risks involved.

8.5.5. All communications via telephone are VISAV Ltd.'s property.

8.6. Visual Aids

8.6.1. Users should only use visual aids for work purposes and should only display content that is relevant to their work.

8.6.2. Users must adhere to the **Clear Desk and Clear Screen Policy** when using visual aids.

8.7. Unacceptable Behaviour

8.7.1. Unacceptable behaviour in relation to the use of Electronic Communications Facilities, Equipment, Electronic Messages and other Information Assets will not be tolerated. Where unacceptable behaviour is identified VISAV Ltd will initiate the **Disciplinary Procedure**.

8.7.2. Unacceptable behaviour will be determined at the time of identification; however, some forms will always be deemed to fall below VISAV Ltd.'s standards of acceptable behaviour.

8.7.3. Examples of unacceptable behaviour include:

- The sending of inappropriate messages including those which are discriminatory, sexually harassing or offensive to others on the grounds of race, age, disability, gender, religion or sexual orientation.
- The sending of potentially defamatory messages which criticise other individuals or organisations (legally e-mail is classified as a form of publication).
- The creation, display, downloading, production, circulation, storage or transmission in any form or medium of inappropriate material. This includes pornographic, offensive or illegal material downloaded from any source such as the Internet.
- The downloading, circulation, storage, or transmission in any form or medium of copyright material for which you do not have the author's express permission.
- Forwarding confidential, sensitive or personal information on to third parties without appropriate authorisation.
- Sending messages which are rude, overbearing, aggressive or bullying.
- Using or forging, via unauthorised means, another email header or content.

8.7.4. Users must be aware of and comply with the legal and regulatory requirements identified by VISAV Ltd in its **Standards and Regulation Control**. If in doubt, please seek guidance from the ROLE.

8.8. Monitoring

8.8.1. VISAV Ltd monitors both the amount of time spent using on-line services and the sites visited by individual employees. VISAV Ltd reserves the right to limit such access by any means available to it, including revoking access altogether.

8.8.2. VISAV Ltd may also monitor its technology at any time in order to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

ACCESS CONTROL POLICY

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 Managing Director of VISAV Ltd.

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

9.1.3. All unsupervised accesses provided to Information Assets, Information Processing Facilities or Operating Facilities must be authorised by the person specified in the **Administrator Access Rights Policy** and recorded in the **Administrator Access Rights Policy**

9.1.4. Security and Infrastructure Director is responsible for:

- Ensuring no single person can access, modify or use VISAV Ltd.'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 Users access to Information Processing Facilities, Electronic Communication Facilities, Mobile Devices, Operating Facilities and Restricted Access areas using an Asset and Access Control and Review Form.
- Ensuring that individuals who enable and disable access to a VISAV Ltd 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 Systems

9.2.1. Security and Infrastructure Director is responsible for:

- Arranging access with the Security and Infrastructure Director as part of the induction of new starters and as part of any company changes within VISAV Ltd.

- Arranging the removal of access by notifying the Security and Infrastructure Director for leavers from VISAV Ltd 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 individuals' access privileges are reviewed upon a change of role or change in responsibilities.
- Recording the status of each Users access privileges in the **Administrator Access Rights Policy**
- 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. Security and Infrastructure Director is responsible for:

- Responding in a timely manner to requests for the activation and deactivation of user account access made to them by Security and Infrastructure Director.
- Configuring and reviewing User access to VISAV Ltd.'s Assets and Information Processing Facilities as specified in the **Administrator Access Rights Policy**
- Removing any expired or unused accounts.
- Testing that deactivated, deleted and removed accounts are no longer accessible.
- Implementing access control systems and mechanisms for VISAV Ltd.'s Assets and Information Processing Facilities as directed by the Security and Infrastructure Director.
- Logging and monitoring all access to VISAV Ltd.'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 16 digits in length.
- Passwords must be a combination of upper and lower case, numbers and special characters or be a phrase
- Passwords must not be guessable for example predictable words like 'password or consecutive number sequences such as '123345'
- Passwords must automatically expire every 60 days
- Historic passwords cannot be repeated.
- Users must ensure that passwords remain confidential.
- Users must be requested to change their passwords on initial access or if access needs to be re-established for any reason.
- Only 6 attempts can be made until the account is locked
- 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 in transfer.
- All displays must have a timeout of 10 minutes or less where the user is prompted to enter a password to access the system.
- Passwords must not be recorded unless a authorised password manager is used
- Personal passwords **MUST NOT** be used in the VISAV Corporate environment

9.2.4. The Security and Infrastructure Director is responsible for:

- Configuring and maintaining all of VISAV Ltd.'s Information Processing Facilities to ensure appropriate access controls are adhered to.
- Monitoring all Information Processing Facilities for attempted breaches of access controls and this policy.
- Recording all attempts to breach access controls and acting accordingly.
- Reporting all security incidents to the appropriate authority and technically assisting with any investigations as required.

9.2.5. The boundary between the business systems and the Internet or other non-trusted networks shall be protected by a firewall, which shall be configured to meet the threat and continuously monitored.

9.2.6. An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis

9.3. Control of Access to Physical Information Processing Facilities

9.3.1. The Security and Infrastructure Director will be responsible for:

- Granting permanent or temporary access to Restricted Access.
- Reviewing access to Restricted Areas every 6 months and authorising changes where required.
- Leading and providing support to incident investigations where required.

9.3.2. 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 for Remote Users

9.4.1. All users must adhere to the **Physical and Environmental Protection Policy**, **Mobile Devices Policy, Remote Access (IT) Policy** and **Acceptable Use of Assets Policy** when using VISAV Ltd.'s Assets in remote locations.

9.4.2. Remote access to VISAV Ltd.'s network and Information Processing Facilities must:

- Only be provided to authorised users only.

- Be used with approved Assets only in accordance with the **Acceptable Use of Assets Policy**, **Teleworking Policy, Remote Access (IT) Policy** and **Mobile Devices Policy**.
- Set to timeout after 5 minutes of inactivity.
- Insert other rules here as required.

9.5. Access to VISAV Ltd.'s Operating Facilities

9.5.1. Access to VISAV Ltd.'s Operating Facilities must be authorised by Security and Infrastructure Director.

9.5.2. Access to VISAV Ltd.'s Operating Facilities will be processed and granted by the Security and Infrastructure Director.

9.5.3. Access controls must be implemented at all of VISAV Ltd.'s Operating Facilities and must be:

- Appropriate and proportionate to the area under control.
- Updated at set intervals in order 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 control measures.
- Not deliberately holding open a controlled access door by wedging, latching on placing an item against it.
- Promptly reporting any problems relating to access controls to the Security and Infrastructure Director.
- Accompanying visitors at all times that are in their care and not allowing them to enter any unauthorised location.
- Immediately reporting to the Security and Infrastructure Director and challenging, if confident and safe to do so, any person who is suspected of being in an area that they are unauthorised to be.

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

9.6. Visitors and Suppliers

9.6.1. All visitors **must:**

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

9.6.2. All suppliers working in an Operating Facility must:

- Be managed and approved in accordance with the **Suppliers Policy**.
- Be appropriately inducted into VISAV Ltd 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.
- Immediately report any accidental breaches of this policy to Security and Infrastructure Director.
- 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. Covered by separate Remote Access Policy

10. BACKUP POLICY

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 on VISAV SAN and retained until unsupported. The backup copies made must ensure that all Information Assets that require the use of Software can be accessed, processes and distributed with minimal disruption.

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

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 on the appropriate SAN and retained for 7 days

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

10.2.3. All Users must ensure that all electronic files are stored on VISAV Ltd.'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 Schedule**.

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

Backups of Software and Electronic Files and media used to store them must be tested at least 6 monthly in accordance with the **Business Continuity Plan** and the **Electronic Data Backup Schedule**.

11. CLEAR DESK AND CLEAR SCREEN POLICY

This sub-policy specifies the controls that need to be applied to minimise the risks to information security arising from unauthorised access to VISAV Ltd.'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 storage media must stored in cabinets and/or draws (in accordance with the **Information Classification, Labelling and Handling Policy**) when not in immediate use and whenever the room they are being using in is vacated unless the room is vacated in accordance with a **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 where they are held.

11.2. Display Screens

11.2.1. Equipment that utilises display screens must have a screen saver 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 screen saver whenever they leave the equipment unattended.

11.3. Reproduction Devices (Printers, Photocopiers and Scanners)

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

12. COMMUNICATION POLICY

This sub-policy specifies the rules that must be applied with regards to internal and external communications relevant to the Information Security Management System.

12.1. Communication with Third Parties

12.1.1. Any enquiries received from Third Parties relating to Information Security or the firm's Information Security Management System must be immediately referred to the Security and Infrastructure Director or in their absence, IT Director

12.1.2. 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**.

12.1.3. Supply of information about VISAV Ltd.'s Information Security Management System including policies, procedures and specific Control Measures employed must be approved by Security and Infrastructure Director.

12.2. Employee Briefings

12.2.1. A member of the Top Management 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 the briefings.

13. CRYPTOGRAPHIC CONTROLS POLICY

This sub-policy specifies the cryptographic controls that must be applied to Confidential Information.

13.1. General Principles

13.1.1. VISAV Ltd.'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 business risk.

13.1.2. All Confidential Information transferred outside of VISAV Ltd must be encrypted prior to transfer.

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

13.1.4. Mobile Device hard drives must be encrypted.

13.1.5. Mobile Devices must be protected by passwords or PIN numbers.

13.1.6. E-mails (including attachments) must be encrypted whenever Confidential Information is contained or attached.

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. Software deployed to force-encrypt removable media. Where implemented, managed by the Security and Infrastructure Director

13.3.2. Software deployed to encrypt fixed hard drives. Where implemented, managed by the Security and Infrastructure Director

13.4. Encryption for Information Transferred Outside the UK

13.4.1. Regulatory controls for any country to which data is exported outside the UK 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 VISAV Ltd 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. INFORMATION CLASSIFICATION, LABELLING AND HANDLING POLICY

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 VISAV Ltd.

14.1. Classification

14.1.1. It is the responsibility of Security and Infrastructure Director to maintain the **Information Classification, Labelling and Handling Rules** to ensure that:

- Information Assets can be easily classified and the classification takes into account 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 VISAV Ltd 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 **Information Classification, Labelling and Handling Rules**.

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 Back-up Policy), copying must be done in accordance with **Information Classification, Labelling and Handling Rules**.

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 **Information Classification, Labelling and Handling Rules**.

14.5. Destruction

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

14.6 Information Classification, Labelling and Handling Rules.

Category	Description	Example	Labeling	Storage	Copying	External Distribution	Internal Distribution
Public	Information that can be made public without causing damage to the company, employees or stakeholders	Approved marketing materials Publicly available information	None	No Contols	In accordance with Copyright and IPR	In accordance with Copyright and IPR	In accordance with Copyright and IPR
Internal	Information where unauthorised disclosure outside the company could be damaging to the company, employees or stakeholders	Internal emails, memos, notes Procedures, policies, forms, work instructions Unapproved marketing material	Apply 'INTERNAL' To the coversheet, the classification box and the top right of each sheet of the document	Only designated Electronic copies should in accordance with the IM and Asset Owners instructions. No copies should be held anywhere else without express written approval from the <role>	No copies are permitted without express written approval from the <role> or Asset Owner	Encrypted email or Secure workspace, only with express permission from the , <ROLE> or Asset Owner. No verbal discussion outside of the organisation.	To persons approved by the , <ROLE> or Asset Owner. Verbal discussion permitted only with relevant staff.
Sensitive	Highly sensitive personal information which requires restricted access and or increased controls. Unauthorised disclosure would cause severe damage to staff or stakeholders	Date of Birth Address Religion Contact Details Bank Details Financial Details Medical Details		To be held on restricted areas of the company's servers ONLY. Not to be held on mobile devices or removable Media Hard Copies should be kept to a absolute minimum and kept in an approved lockable fire resistant cabinet. Backed up only by an approved 3rd Party provider	NONE without express written permissionn from the subject	NONE including verbal without express written permission from the subject	Only to be accessed by members of staff where the information is necessary for them to be able to fulfil their responsibilities. No verbal discussion outside of the organisation without express permission of the subject, <role>
Commercial	Information where unauthorised disclosure outside the Interested Parties could be damaging to the company, employees or stakeholders	Business Sensitive emails, memos, notes Service Contracts	Apply 'COMMERCIAL' To the coversheet, the classification box and the top right of each sheet of the document	Only designated Electronic copies should in accordance with the IM and Asset Owners instructions. No copies should be held anywhere else without express written approval from the <role>	No copies are permitted without express written approval from the <role> or Asset Owner	Normal methods of communication are permitted between the Interested Parties	Interested Parties. Persons approved by the , <ROLE> or Asset Owner. Verbal discussion permitted only with relevant staff.
Commercial in	Highly sensitive client information which requires restricted access and or	Assessment reviews	Commercial in confidence is to be applied to the cover sheet	Electronic Copies should be stored in accordance with IM and Asset Owners	Limited only to the appropriate assessor for	NONE including verbal.	Limited persons involved in the assessment and only for the

Confidence	increased controls. Unauthorised disclosure would cause severe damage to the organisation. In most cases will be covered by an NDA	Gap Analysis Assessment Reports Network Diagrams	and to the top right of each sheet of the document.	Instructions. Hard Copies are to be stored in the designated lockable cabinet	the purposes of the assessment. All copies should be recorded in the document Control register		purposes of the assessment. All copies should be recorded in the Document Control Register. No verbal discussion outside of relevant parties.
Confidential	Highly sensitive company information which requires restricted access and or increased controls. Unauthorised disclosure would cause severe damage to the organisation	Any usernames or Passwords Encryption Keys, PIN or access control identifiers Physical Security Details		To be held on restricted areas of the company's servers ONLY. Not to be held on mobile devices or removable Media Hard Copies should be kept to a absolute minimum and kept in an approved lockable fire resistant cabinet. Backed up only by an approved 3rd Party provider	No copies are permitted without express written approval from the <role>	Encrypted email or Secure workspace, only with express permission from the , <ROLE>. No verbal discussion outside of the organisation.	To persons approved by the <role>. Verbal discussion permitted only with relevant staff.

15. MOBILE DEVICES POLICY

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

- control the use of any Mobile Devices owned by or under the control of VISAV Ltd; and
- 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 Managing Director and recorded on the Asset Register

15.1.2. All Users must sign and return a **Mobile Device User's Agreement**.

15.2. Use of Mobile Devices

15.2.1. All Users of Mobile Devices must comply with the **Acceptable Use of Assets Policy**, **Clear Desk and Clear Screen Policy**, **Backup Policy**, **Teleworking Policy** and the **Use of Software Policy**.

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 it was supplied to. 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 telephone or smart telephone.

15.2.5. Users must immediately notify Managing Director 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 VISAV Ltd, Users must ensure that they take adequate precautions to protect the equipment against theft or accidental damage at all times.

15.2.9. When transporting Mobile Devices, care should be taken not to draw attention to their existence, so as 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 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 **Access Control Policy**.

15.2.14. Mobile Devices must always be trackable and have a remote wiping feature installed.

15.2.15. The mobile threat prevention solution must always be active on any mobile phone.

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

15.2.17. Mobile Devices must not be used to transfer information via wireless networks that have not been approved by Security and Infrastructure Director.

15.3. Return of Mobile Devices

15.3.1. Upon request by Managing Director, termination of contract or change of role a User must return any Mobile Devices they have been issued with to Managing Director.

15.3.2. All Mobile Devices returned to Managing Director and recorded on Asset Register

15.3.3. All Users must complete their **Mobile Device User's Agreement** upon return.

16. PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY

This sub-policy specifies the controls that need to be applied to all Operating Facilities and Assets located at them to:

- protect VISAV Ltd.'s Assets from physical and environmental threats;
- reduce the risk of damage, loss and theft to VISAV Ltd.'s Assets; and
- reduce the risk of unauthorised access to VISAV Ltd.'s Operating Facilities.

16.1. Physical Protection of Operating Facilities

16.1.1. All of VISAV Ltd.'s Operating Facilities must be secured at all times using appropriate methods to prevent unauthorised access.

16.1.2. All Operating Facilities must be protected by an intruder alarm system

16.1.3. All external windows and doors must always be kept shut and locked unless authorised by Security and Infrastructure Director.

16.1.4. All doors to be always kept closed

16.2. Environmental Protection of Operating Facilities

16.2.1. All of the environmental vulnerabilities and controls associated with VISAV Ltd.'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 back-up as follows:

- Generators must have the capability to meet the requirements of the **Business Continuity Plan**.
- Battery back-up must have the ability to provide at least 30 minutes of uptime to the systems utilising their power.

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.

16.2.5. Insert other rules here as required.

16.3. Protection of Assets at Operating Facilities

16.3.1. All network servers and must be located 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 Handling, Labelling and Classification Policy**.

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

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. PROTECTION FROM MALWARE POLICY

This sub-policy specifies the controls that need to be applied to all Computer Systems and the Mobile Devices that can connect to VISAV Ltd.'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 Security and Infrastructure Director to ensure that effective Anti-Virus Software is installed and appropriately updated on all Computer Systems and Mobile Devices that have access to VISAV Ltd.'s Information Processing Facilities and store and transmit Information Assets, regardless of whether VISAV Ltd actively manages and maintains them or not.

17.1.2. All Computer System and Mobile Devices must not be used or handed over to a User unless they have up to date Anti-Virus Software installed and operational on them.

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 on to a Computer System or Mobile Device.

17.1.4. All Anti-Virus Software must be configured to ensure it is able to detect, remove and protect against all known types of Malware.

17.1.5. All Anti-Virus Software must be configured to automatically start up on device power up and to continuously run for the duration 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 VISAV Ltd-wide anti-virus server (if applicable). All logs must be kept for a minimum of 30 days

17.2. Installations of Anti-Virus Software on Mail Servers

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

17.3. Other Processes, Systems and Tools to Deter Malware

17.3.1. All Computer Systems and Mobile Devices must run VISAV Ltd.'s approved operating system at its latest supported version with all relevant updates and patches installed.

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

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

17.4. Requirements of Users

17.4.1. Any activity intended to create and / or distribute malware on an Information Processing Facility, Computer System or Mobile Device is strictly prohibited.

17.4.2. All Users must not in any way interfere with the Anti-Virus Software installed on any Computer System or Mobile Device.

17.4.3. All Users must immediately report any issues, or suspected issues relating to Malware and any anti-virus warnings and alerts communicated to them from a Computer System or Mobile Device.

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

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

17.4.6. Users must seek advice from the Security and Infrastructure Director if their Computer System or Mobile Device requests them to install or update software such as Java and ActiveX.

18. DATA PROTECTION POLICY

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 processes by VISAV Ltd to ensure that VISAV Ltd and its employees comply with the Data Protection Act 2018.

18.1. Application of the Data Protection Principles

18.1.1. The following principles must be applied in relation to all Personal Information that is accessed, store or processed by employees and employees or subcontractors of Information Security Critical Suppliers while they are accessing or processing VISAV Ltd.'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.

18.2. Registration with the Information Commissioner

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

18.3. Accessing, Processing and Storage of Personal Information

18.3.1. The Security and Infrastructure Director must ensure that appropriate physical and technical controls are in place to prevent unauthorised access to Personal Information.

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

- fulfil the needs of customers
- comply with legal requirements
- enable the effective implementation of VISAV Ltd.'s Information Security Management System

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

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

18.4. Transferring Personal Information

18.4.1. 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**.

18.4.2. 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. SUPPLIERS POLICY

This sub-policy specifies the controls that need to be applied to all suppliers who can compromise the security of VISAV Ltd.'s Information Assets.

This sub-policy does not apply to services supplied by individuals under the terms of a **Contract of Employment** issued by VISAV Ltd.

19.1. Information Security Critical Suppliers (ISCS)

19.1.1. The use of all ISCS must be approved by the Security and Infrastructure Director. This approval must be completed and recorded in accordance with the **Change Control Procedure**.

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

19.1.3. All Information Security risks identified relating to the use of ISCS must be assessed and recorded in the **Asset Identification and Risk Assessment Register** in accordance with the **Asset Identification and Risk Assessment Procedure**.

19.1.4. ISCS 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 VISAV Ltd.'s Information Assets in respect of Availability, Integrity and Confidentiality.
- The obligations of the ISCS to comply with VISAV Ltd.'s **Information Security Policy** and relevant processes, policies and procedures in its Information Security Management System including acknowledgement of documents supplied by VISAV Ltd.
- The minimum information security controls implemented and maintained by the ISCS to protect VISAV Ltd.'s Information Assets and the arrangements for monitoring their effectiveness.
- The arrangements for reporting and managing Security Incidents (as per the **Security Incident Reporting Procedure**).
- The arrangements for managing changes to any Assets (as per the **Change Control Procedure**).
- The contact names of the persons employed by VISAV Ltd and ISCS with responsibility for information security.
- The defect resolution and conflict resolution processes.

19.1.5. 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 VISAV Ltd.'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 VISAV Ltd.
- Accuracy and completeness controls to ensure the Integrity of the Assets, information or information processing equipment/facilities provided by the ISCS and/or VISAV Ltd.
- Processes and/or procedures for transferring information and/or information processing facilities between the ISCS, VISAV Ltd 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.

19.1.6. It is the responsibility of the Security and Infrastructure Director to create and maintain an **Approved Information Security Critical Suppliers Register**.

19.1.7. It is the responsibility of the Security and Infrastructure Director to ensure that all Suppliers are provided with up to date copies of VISAV Ltd.'s policies and procedures that are relevant to them.

19.1.8. It is the responsibility of the Security and Infrastructure Director to ensure that the information security controls specified in the Supply of Goods and Services Agreement are audited at a frequency of not less that once every 12 months by a qualified auditor in accordance with the **Supplier Audit Procedure**.

20. TELEWORKING POLICY

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 VISAV Ltd.

20.1. Teleworking Authorisation

20.1.1. All Teleworking must be approved by Security and Infrastructure Director.

20.1.2. The scope of a Teleworker's teleworking must be defined to include:

- Authorised locations for Teleworking (e.g. home, hotels, travelling etc)
- Equipment and ECF to be used
- Access controls to VISAV Ltd.'s Information Processing Facilities
- Any specific controls to be applied (e.g. use of Equipment by other individuals).

20.2. Accessing VISAV Ltd.'s Information Processing Facilities from Teleworking Locations

20.2.1. Teleworkers must comply with the **Access Control Policy**, **Acceptable Use of Assets Policy**, **Mobile Devices Policy** and the **Protection from Malware Policy** when connecting to VISAV Ltd.'s Information Processing Facilities whilst Teleworking.

20.2.2. Remote access to VISAV Ltd.'s Information Processing Facilities will be authorised by the Security and Infrastructure Director.

20.2.3. Remote access to VISAV Ltd.'s Information Processing Facilities will be SSL VPN

20.3. VISAV Ltd-Provided Equipment for Teleworking

20.3.1. Where Equipment is provided to the Teleworker for Teleworking the Teleworker must comply with the **Acceptable Use of Assets Policy**, **Mobile Devices Policy** and **Use of Software Policy**.

20.4. Use of Teleworker-Owned Equipment for Teleworking

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

- The Equipment is approved for use by the Security and Infrastructure Director.
- The Equipment is only used in accordance with the approved scope of their Teleworking and 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 VISAV Ltd.'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 screen savers.
- All Equipment is configured to “auto lock” after an inactivity period of 5 minutes.

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

20.4.3. Teleworkers must take extra care when using any Equipment for Teleworking to protect it from theft and damage. All equipment should be hidden from view from windows with access by 5 lever mortice operated doors.

20.4.4. Only authorised people can use the equipment

20.4.5. All repairs reported to Security and Infrastructure Director and approved before progression.

20.4.6. The Teleworker must report any loss or theft of any Equipment that has been used for Teleworking to the Security and Infrastructure Director.

20.4.7. The Teleworker must notify the Security and Infrastructure Director of the disposal of any Equipment and be willing to pass, by mutual agreement, the Equipment to the Security and Infrastructure Director for the purpose of removing any of VISAV Ltd.’s Information Assets that may still reside on it.

21. USE OF SOFTWARE POLICY

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 VISAV Ltd 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 VISAV Ltd without the express written consent of the software publisher and VISAV Ltd.

21.2. Installation of Software

21.2.1. Installation of software onto an Asset must be authorised by Security and Infrastructure Director and must be done in accordance with the **Change Management 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 VISAV Ltd unless authorised to do so by the Security and Infrastructure Director.

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

22. POLICY REVIEW

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