Storage Media Policy

Objective and Scope

The objective of this policy is to document the management of removable storage media to prevent unauthorised access, disclosure, modification, removal or destruction of information stored on media (including removable media devices). This is intended to ensure only authorised disclosure, modification, removal or destruction of information on storage media.

Data handling and storage is the recording (storing) of information (data) in a storage medium. Handwriting, phonographic recording, magnetic tape and optical discs are all examples of media handling and storage.

The scope of this policy covers media content lifecycle of classified information security risk nature and includes the:

- acceptable media tools approved for holding high risk classified data and information
- acceptable classification of information that can be stored on a removable media tool information
- registration of devices used for business purposes whether company or privately owned
- physical protection of such devices
- secure transfer of data and information when required
- secure destruction of data and information on reusable devices
- media devices used as backups

Roles, Responsibilities and Authorities

The Operations Director or competent IT Team delegate determines policy and standards for the management of high risk classified media.

The Operations Director takes ownership for monitoring high risk classified media handling in relation to ensuring individuals are following due process by monitoring the registration of media devices, secure transfer and destruction.

Individuals are accountable for general use of media device use and compliance to this policy.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

Storage Media Policy

Legal and Regulatory

Title	Reference
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
Computer Misuse Act1990	www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction
National Assistance Act 1948	https://www.legislation.gov.uk/ukpga/Geo6/11-12/29/enacted
The Copyright, Designs and Patents Act 1988	https://copyrightservice.co.uk/
The Freedom of Information Act 2000	https://www.legislation.gov.uk/ukpga/2018/12/contents

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
Media Handling	8.3	8.3.1		7.10
Disposal of media		8.3.2		7.10
Physical media transfer		8.3.3		
Removal of assets		11.2.5		

Related Information

- Information Security Policy
- Privacy Policy
- Information Classification Policy

Policy

Prevision Research removable media is managed through the following core principles:

- Authorisation from Operations Director is required for the use or removal of stored media of high risk classified information
- Devices must be secured in a safe environment to prevent loss from theft or damage due to environmental factors
- Devices holding secure business data including personal identifiable information must be registered, content encryptable and then only used as approved by the Operations Director.

All roles and or individuals using removable media devices for high risk information classification cannot use these devices for any other purpose than that described by the Operations Director. This device shall be

Storage Media Policy

registered to a specific user, only contain encrypted data and shall be subject to secure destruction when no longer required.

Regardless of ownership, each removable media device must meet the minimum company standards in terms of security and use.

Management of removable media - high risk or above information classification

The following steps must be followed when using removable media for information classified as high risk (or above):

1. Removable media devices such as USB or other removable ports should only be allowed if there is a business case to do so. This shall be included in the Register of removable media devices containing high risk classified information.
2. The content of any reusable media device (information classified as high risk) should be removed so that it is not recoverable once removed.
3. Maintain an audit trail of the handling of information classified as high risk subject to removable media device use.
4. Cryptography controls are mandated for removable media devices containing high risk classified information, including for storage or transfer.

Removal of media

Removal of assets to other locations is permitted for work related activities as long as this is managed in a secure manner to protect from loss, damage, misuse or unauthorised access.

Password protection, locked or protected storage locations and other security protocols according to asset management protocols apply.

All assets and their home location shall be recorded in the asset register.

Disposal or reuse of media

When not required for specific reasons, media devices holding high risk classified information shall be disposed of securely after the content has been securely wiped.

Methodologies for disposal can include shredding or data erasure via use by another application within an organisation. Credible data collection and disposal organisations may be used at the discretion of the Operations Director. Refer to the preferred supplier register for approved suppliers.

In order to maintain an audit trail, the disposal of confidential items must be logged and the register updated accordingly.

Physical media transfer

High risk classified Information media devices shall be protected from unauthorised access, misuse or corruption during transportation or other means of transfer.

Information and/or devices may be vulnerable to unauthorised access, misuse or corruption when sending the media by mail or courier. The media includes both paper and electronic documents in this process.

Storage Media Policy

Should a physical media device be damaged or require repair, risk assess the content of the device against data confidentiality integrity and availability to determine whether the device content poses a security risk. It may be preferable to destroy rather than repair a device.

Paper based media

Paper based documents that contain CIA sensitive information shall be treated with the same level of security as does electronic CIA information. Such documents shall be subject to secure disposal through shredding or use of a credible disposal organisation. Also refer to the Information Transfer Policy for transfer of secure paper based documents.

Policy review

This policy shall be reviewed by the policy owner no less than annually or immediately after a process change or a policy breach is known to have occurred.

Periodic reviews shall take into account feedback from management reviews, regulatory changes and audits. Changes to the policy must be approved by a senior executive then communicated to all previous persons or organisations with access to the policy.

Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N