

Management of Storage Media Policy

(ISO 27001:2022 Physical Controls – Clause 7.10)

Author	Greg Nott
Version	2.0
Date Created	01/05/2023
Last Update Date	14/05/2024
Document Control	Released
Document ID	230501-IMS-POL-ManagementOfStorageMediaPolicy-V2
Security Classification	Public

Table of Contents

Management of Storage Media Policy	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Purpose	4
Exceptions.....	4
Roles and responsibilities.....	4
Senior Management	4
Head of Information Security.....	4
Employee's	4
Information Owner's.....	5
Physical Security.....	5
Media Handling.....	5
Media Disposal.....	5
Incident Reporting and Management.....	5
Compliance and Auditing.....	5
Training and awareness.....	6

Approval

Author	Issue	Approved By	Date
Paul Langan	1.0	Simon Naylor	15-Aug-23
Greg Nott	2.0	Paul Langan	15-May-24

Review

Reviewer	Review Criteria	Issue	Date
Paul Langan	ISO 27001:2022	1.0	14-Sep-23
Paul Langan	Review & Rebrand	2.0	15-May-24

Change History

Author	Change	Issue	Date
Paul Langan	Creation	1.0	01-May-23
Greg Nott	Review & Rebrand	2.0	15-May-24

Associated Documents

Document	Version
Secure Disposal and Reuse of Equipment Policy	1.0

Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and describes the Management of Storage Media Policy adopted by ARO.

- ISO 27001:2022 – Information Security Management Systems
 - ISO 27017:2015 – Code of Practice for Cloud Services
 - ISO 27018:2020 – Code of Practice of Personally Identifiable Information (PII)
- ISO 9001:2015 – Quality Management System
- DSPT (Data Security and Protection Toolkit) for the NHS.
- Cyber Essentials Plus

This policy applies to all storage media used within ARO, including but not limited to physical media (e.g., hard drives, DVDs, USB drives) and electronic media (e.g., cloud storage, network storage, databases).

Purpose

The purpose of this policy is to define the management, control, and protection of storage media to ensure the confidentiality, integrity, and availability of information assets.

Exceptions

- Any exceptions to the application of this policy or where controls cannot be adhered to MUST be presented to the Head of Information Security or a member of the management team.
- All exceptions to this policy MUST be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

Roles and responsibilities

Senior Management

- Senior management shall be responsible for providing clear direction and support for the implementation of this policy.
- Senior management shall ensure that sufficient resources are allocated for the implementation and maintenance of the storage media management system.

Head of Information Security

- The Head of Information Security shall be responsible for overseeing the implementation and enforcement of this policy.
- The Head of Information Security shall ensure that appropriate procedures and guidelines are developed and communicated to staff regarding the management of storage media.

Employee's

- All ARO employees shall comply with this policy and any associated procedures and guidelines.
- Employees shall be responsible for safeguarding storage media in their possession and reporting any incidents or breaches immediately.

Information Owner's

- The Information Owner must give permission for deletion of datasets owned by them.

Physical Security

- Storage media containing sensitive or confidential information shall be physically secured to prevent unauthorised access, loss, theft, or damage.
- Physical access controls (e.g., locks, access cards, CCTV) shall be implemented to restrict unauthorised access to storage areas.
- Storage media shall be stored in designated secure locations, such as locked cabinets or rooms, to prevent unauthorised access.

Media Handling

- Storage media shall be labelled with appropriate identification and classification markings to ensure proper handling and tracking.
- Only authorised personnel shall be allowed to handle storage media, and they shall follow the documented procedures for handling, transporting, and storing the media.
- Storage media shall be protected against environmental factors (e.g., temperature, humidity, magnetic fields) that could potentially damage the media.

Media Disposal

- Storage media that are no longer required or have reached the end of their life cycle shall be disposed of securely and in accordance with the organisation's media disposal procedures.
- Media disposal procedures shall include methods for physically destroying media (e.g., shredding, degaussing) or securely wiping electronic media to prevent data recovery.
- All media disposal activities shall be documented and kept for audit purposes.

Refer to the 'Secure Disposal and Reuse of Equipment Policy' for further details on the disposal of media.

Incident Reporting and Management

- Any incidents, breaches, or suspected compromises of storage media shall be reported immediately to the designated authorities and the incident management process shall be followed.
- An incident response plan shall be in place to address and mitigate the impact of storage media incidents.

Compliance and Auditing

- Regular audits and reviews shall be conducted to assess compliance with this policy and associated procedures.
- ARO shall comply with any legal, regulatory, or contractual requirements related to the management of storage media.

Training and awareness

- Training and awareness programs shall be implemented to ensure that employees are knowledgeable about their responsibilities and the requirements of this policy.
- Training programs shall be regularly reviewed and updated to address emerging threats and changes in technology.