

Data Destruction 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-DataDestruction-V2
Security Classification	Public

Table of Contents

Data Destruction Policy	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Purpose	4
Exceptions	4
Classification of Data.....	4
Data Destruction Methods.....	4
Physical Data Destruction	4
Electronic Data Destruction	5
Responsibilities	5
Documentation and Record Keeping	5
Internal to ARO	5
Client Specific.....	5
Training and Awareness	5
Policy Non-Compliance	5

Approval

Author	Issue	Approved By	Date
Paul Langan	1.0	Simon Naylor	19-Sep-23
Greg Nott	2.0	Paul Langan	14-May-24

Review

Reviewer	Review Criteria	Issue	Date
Greg Nott	ISO 27001:2022	1.0	17-Sep-23
Paul Langan	Review & Rebrand	2.0	14-May-24

Change History

Author	Change	Issue	Date
Paul Langan	Creation	1.0	01-May-23
Greg Nott	Review & Rebrand	2.0	14-May-24

Associated Documents

Document	Version
Secure Disposal and Reuse of Equipment Policy	2.0

Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and describes the Data Destruction 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 employees, contractors, and third-party vendors who access, utilise, or manage information on behalf of ARO.

Purpose

The purpose of this data destruction policy is to ensure the secure and proper disposal of data within our organisation, in compliance with legal and regulatory requirements. This policy outlines the procedures and guidelines for the destruction of both physical and electronic data to protect sensitive information and maintain the privacy of individuals.

This policy covers all types of data including temporary files and documents.

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.

Classification of Data

ARO classifies data based on its sensitivity and the potential impact of unauthorised disclosure. The classification levels include, but are not limited to:

- **Confidential** - Company confidential, issued only to parties authorised by Senior Management and/or the IMS Team. Information will be made available and distributed strictly on a need-to-know basis.
- **Commercial In Confidence** - Documents that are Shared/Co-authored with partners that contain proprietary information.
- **Public** - General Release
- **Internal** - Internal Company information not deemed to be confidential or public. Open to all staff.

Data Destruction Methods

Physical Data Destruction

- **Shredding** - Paper documents and physical media should be shredded using cross-cut shredders or contracted shredding services that adhere to industry standards.

Electronic Data Destruction

- **Clearing** - Public/Private Clouds. On shared drives and media data destruction will involve deletion of data from the file system and where possible an overwrite process to ensure the data is not recoverable.
- **Purging** - Private Clouds only. Degauss the media.
- **Destruction** - Private Clouds only. Media is shredded.

Responsibilities

- **Employees** - All employees should be aware of their responsibilities in handling sensitive data and following the data destruction procedures outlined in this policy.
- **IT Department** - The IT department is responsible for implementing and maintaining appropriate data destruction processes and technologies. They should also provide guidance and training to employees on secure data disposal.
- **Internal Audit Team** – The Internal Audit Team should oversee the implementation and compliance of this policy and periodically review the data destruction procedures to ensure they are up to date and effective.
- **Information Owner** – The Information Owner must give permission for deletion of datasets owned by them.

Documentation and Record Keeping

Internal to ARO

- Records of data destruction activities, including date, time, method used, and individuals involved, should be maintained for auditing and compliance purposes. These records should be securely stored for a specified period in accordance with legal and regulatory requirements.

Client Specific

- ARO will destroy all client data and will supply the client with a Certificate of Data Destruction, this document will detail the volume of data held by ARO and the media on which it was stored as well as the date, method and name of the technician responsible for the destruction of the data and confirmed by a member of the management team.
- The method applied will be client specific (one of the previously mentioned methods) and will be specifically addressed and agreed with clients in the Service Level Agreement (SLA) section of the contract with the client.

Training and Awareness

- Regular training and awareness programs should be conducted to educate employees about the importance of data destruction and to ensure that they are familiar with the procedures outlined in this policy.

Policy Non-Compliance

- Any violations of this data destruction policy should be reported to the appropriate management or the designated authority for investigation and appropriate action. Non-compliance may result in disciplinary measures as per ARO's policies.