

Information Labelling Policy

(ISO 27001:2022 Organisational Controls – Clauses 5.13)

Author	Greg Nott
Version	3.0
Date Created	23/05/2023
Last Update Date	06/12/2024
Document Control	Released
Document ID	230523-IMS-POL-InformationLabelling-V3
Security Classification	Public

Table of Contents

Information Labelling Policy	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Purpose	4
Exceptions	4
Information Classification	4
Information Labelling.....	4
Note on Public Documents	5
Responsibilities	5
Specialist Data Centre Services (SDCS) Customers	5
Compliance and Auditing.....	5
Training and Awareness	5
Review.....	5

Approval

Author	Issue	Approved By	Date
Paul Langan	1.0	Simon Naylor	23-Aug-23
Greg Nott	2.0	Paul Langan	16-May-24
Greg Nott	3.0	Greg Nott	06-Dec-24

Review

Reviewer	Review Criteria	Issue	Date
Greg Nott	ISO 27001:2022	1.0	04-Aug-23
Paul Langan	Review & Rebrand	2.0	16-May-24
Greg Nott	Information Classification Register	3.0	06-Dec-24

Change History

Author	Change	Issue	Date
Paul Langan	Creation	1.0	12-May-23
Greg Nott	Review & Rebrand	2.0	16-May-24
Greg Nott	Information Classification Register	3.0	06-Dec-24

Associated Documents

Document	Version
230506-IMS-POL-InformationHandling-V2.docx	2.0
241031-IMS-REG-InformationClassification-V1	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 Information Labelling 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 stakeholders who handle or have access to organisational information, regardless of its format (physical or digital). It encompasses all information assets, including but not limited to documents, records, electronic data, and intellectual property.

Purpose

This Information Labelling Policy outlines the principles and guidelines for labelling information in ARO. The policy ensures the accurate identification and appropriate handling of information to enhance its accessibility, confidentiality, integrity, and availability.

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.

Information Classification

Information is classified based on its sensitivity, criticality, and legal/regulatory requirements. The following classification levels are in use throughout ARO:

- **Confidential** - Company confidential, 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.

How Data Types and Key Systems / Sources used in ARO are Classified can be found in the Information Classification Register.

Information Labelling

Where possible information assets shall be appropriately labelled to reflect their classification level. The following labelling requirements shall be adhered to:

- **Physical Documents:** Documents shall be labelled visibly and prominently with the appropriate classification level, using standardised labels or markings.
- **Electronic Documents:** Electronic documents shall be labelled with appropriate metadata or tags indicating their classification level. Electronic file properties or document headers/footers may also be used for this purpose.
- **Email Communications:** Email messages containing sensitive information shall be appropriately marked with an email classification label or tag in the subject line or body of the email.
- **Data Systems:** Data systems (where possible) shall be configured to automatically apply classification labels to information based on predefined rules and policies.

Note on Public Documents

Documents that are classified as Public do not always need to be labelled.

Where the inherent purpose of a document is to be shared broadly, such as marketing materials, there is no need to label the document.

Where a document is not inherently shared by its purpose, but has been made Public by an appropriate authority – i.e. certain Policy documents – the document should be explicitly labelled as Public so as to avoid uncertainty and confusion.

Responsibilities

- **Management:** Management shall ensure the implementation, maintenance, and periodic review of this policy. They shall also allocate necessary resources for training, awareness, and compliance activities related to information labelling.
- **Employees:** All employees are responsible for adhering to this policy and appropriately labelling information assets they handle or create. They shall report any violations, incidents, or breaches to the designated authority.

Specialist Data Centre Services (SDCS) Customers

This policy should be made available to ARO's SDCS customers upon request.

Compliance and Auditing

Compliance with this policy shall be regularly monitored through internal audits, assessments, and reviews. Non-compliance shall be addressed through corrective actions, training, or disciplinary measures as per ARO's policies and procedures.

Training and Awareness

All employees shall receive training on this policy and its associated procedures during onboarding and periodically thereafter. Awareness programs shall be conducted to promote a culture of information security and compliance throughout the organisation.

Review

This policy shall be reviewed at least once per year to ensure its relevance and effectiveness. Amendments or revisions shall be made as necessary and communicated to all relevant stakeholders.