

Acceptable Use of Information and Associated Assets

(ISO 27001:2022 Organisational Controls - Clause 5.10)

Author	Greg Nott
Version	2.0
Date Created	12/05/2023
Last Update Date	14/05/2024
Document Control	Released
Document ID	230512-IMS-POL-AcceptableUseOfAssets-V2
Security Classification	Public

Table of Contents

Acceptable Use of Information and Associated Assets	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Purpose.....	4
Exceptions.....	4
Policy.....	4
General Principles.....	4
User Responsibilities.....	4
Protection of Information and Associated Assets.....	5
Acceptable Use Guidelines.....	5
Return of Information Assets.....	5
Mobile and Remote Assets.....	5
Compliance.....	6
Review.....	6

Approval

Author	Issue	Approved By	Date
Paul Langan	1.0	Simon Naylor	15-Aug-23
Greg Nott	2.0	Paul Langan	14-May-24

Review

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

Change History

Author	Change	Issue	Date
Paul Langan	Creation	1.0	12-May-23
Greg Nott	Review & Rebrand	2.0	14-May-24

Associated Documents

Document	Version

Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and describes the Acceptable Use of Assets 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

This document establishes the acceptable use of information and associated assets within ARO.

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.

Policy

General Principles

- Information and associated assets shall be used in a lawful, ethical, and responsible manner.
- Users shall protect the confidentiality, integrity, and availability of information and associated assets.
- Users shall comply with applicable laws, regulations, and contractual obligations.
- ARO reserves the right to monitor and audit the use of information and associated assets to ensure compliance with this policy.

User Responsibilities

- Users shall access and use information and associated assets solely for authorised business purposes.
- Users shall not disclose sensitive or confidential information to unauthorised individuals or organisations.
- Users shall not misuse or abuse information and associated assets for personal gain or malicious

purposes.

- Users shall report any suspected or actual unauthorised use, loss, or disclosure of information and associated assets to the appropriate authority within the organisation.

Protection of Information and Associated Assets

- Users shall apply appropriate security controls, such as passwords, encryption, and access controls, to safeguard information and associated assets.
- Users shall not install or use unauthorised software or hardware that may compromise the security of information and associated assets.
- Users shall promptly update and patch software and systems to mitigate known security vulnerabilities.
- Users shall not intentionally introduce viruses, malware, or other malicious code to information and associated assets.

Acceptable Use Guidelines

- Users shall use email, internet, and other communication tools in accordance with ARO's policies and guidelines.
- Users shall not engage in activities that may harm ARO's reputation, such as spreading false or misleading information.
- Users shall not download, upload, or distribute copyrighted materials without proper authorisation or licensing.
- Users shall not engage in activities that may disrupt or degrade the performance of information and associated assets.
- Where assets need to be removed off-site, management approval for the removal of such assets must be obtained by raising a ticket on the relevant ITSM platform (i.e. BOLT, Autotask).

Return of Information Assets

When an information asset is returned the following needs to be done:

- The associated entry on the Asset allocation form should be updated.
- Any data held on the asset that is relevant to ARO (or its clients) needs to be transferred to suitable media within ARO. This must be recorded by creating a change request on the relevant ITSM platform (i.e. BOLT, Autotask).
- Any data on the asset should be cleaned (removed) before re-use in line with the Secure Disposal and Reuse of Equipment Policy.

Mobile and Remote Assets

- Users shall adhere to ARO's mobile and remote access policies and guidelines.
- Users shall use secure connections and encryption when accessing information and associated

assets remotely.

- Users shall not store sensitive or confidential information on personal devices without proper authorisation or encryption.

Compliance

Non-compliance with this policy may result in disciplinary actions, including but not limited to reprimands, suspension, termination of employment or contract, and legal proceedings if applicable.

Review

This policy shall be reviewed at least once year and updated as necessary to ensure its ongoing relevance and effectiveness. Any proposed changes to this policy shall be subject to appropriate approval processes.