

Review of Information Security Policy

(ISO 27001:2022 Technological Controls – Clause 8.8)

Author	Greg Nott
Version	2.0
Date Created	20/06/2023
Last Update Date	24/05/2024
Document Control	Released
Document ID	230620-IMS-POL-ReviewOfInformationSecurity-V2
Security Classification	Public

Table of Contents

Review of Information Security Policy.....1

Approval.....3

Review.....3

Change History.....3

Associated Documents.....3

Scope.....4

Policy.....4

Approval

Author	Issue	Approved By	Date
Greg Nott	1.0	Simon Naylor	20-Jun-23
Greg Nott	2.0	Paul Langan	24-May-24

Review

Reviewer	Review Criteria	Issue	Date
Paul Langan	ISO 27001:2022	1.0	20-Jun-23
Paul Langan	Review & Rebrand	2.0	24-May-24

Change History

Author	Change	Issue	Date
Greg Nott	Creation	1.0	19-Jun-23
Greg Nott	Review & Rebrand	2.0	23-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 Review of Information Security 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 have responsibilities regarding the maintenance of the IMS and informations security in general within ARO.

Policy

ARO recognises that the protection of information and the systems that manage information is vital to the continued success of our business.

The organisation defines effective information security management as providing measures that ensure the availability of information, its protection from corruption and unauthorised access, both from within and from external sources, and its removal when appropriate.

ARO has established an effective information security management system; the system complements other management systems within the company, which interact with the IMS. As such, the organisation responds appropriately to protect all information assets at all stages. All components, policies and procedures of the IMS are established using methods that are consistent with good commercial practice and appropriate risk assessments.

Integral to the IMS are procedures, which aim to achieve continual improvement in the effectiveness of the system. These are based upon the recording and analysing of incidents which impact on information security and the conducting of independent audits and reviews of the IMS.

The IMS Team will review the IMS to ensure where necessary compliance with any applicable legislation that directly affects the integrity of the system. ARO will maintain compliance with Intellectual Property Rights, the Data Protection Act, GDPR, The Computer Misuse Act and the Regulation of Investigatory Powers Act.

The organisation will ensure that all employees are aware of the need to protect information and their personal responsibilities in this respect, training will be provided both as part of their initial induction into ARO and on an ongoing basis.

The Head of Information Security has ultimate responsibility for the IMS, its effectiveness and applicability. The information asset users and owners are responsible for ensuring its ongoing suitability within their direct areas of interest and responsibility.

Every user is required to contribute to the operation of the IMS by complying with the guidelines relevant to their job role.

Failure to observe procedures defined by the IMS may constitute a disciplinary offence.

The ARO Information Security Policy is reviewed at least once a year by the IMS Team and the Senior Leadership team (or their nominees). The policy will be maintained to reflect current business circumstances and available technology.

The ARO IMS will be independently reviewed by an external body at least once a year.

The organisation may also initiate additional independent reviews relevant to the IMS including but not limited to:

- Penetration Tests
- Vulnerability Scanning
- Phishing Simulations
- Cyber Essentials Based Assessments
- Financial Regulatory Audits
- Insurance Provider Cyber Maturity Assessments