

Information Security Policy

(ISO 27001:2022: Leadership - clause 5.1; ISO 9001:2015 Clause 5.2)

Author	Paul Langan
Version	4.0
Date Created	02/05/2023
Last Update Date	18/06/2026
Document Control	Released
Document ID	230501-IMS-POL-InformationSecurityPolicy-V4
Security Classification	Public

Table of Contents

Approval.....3

Author 3

Review.....3

Change History.....3

Associated Documents.....3

Scope.....4

Purpose 4

 Exceptions.....4

 Information Security Policy Statement 4

 Information Security Planning 5

 Client Copies 5

 GDPR Principles.....5

 Compliance with PII (Personal Identifiable Information) Protection Legislation 6

 Senior Management Team Approval.....6

Approval

Signature of Approver	Ciaran Rafferty		
			
Approver's Role Within ARO		CEO	
Issue	4.0	Date	18/06/2026

Author

Author	Issue	Date
Paul Langan	1.0	23-May-23
Greg Nott	2.0	13-May-24
Paul Langan	3.0	18-Jun-25
Greg Nott	4.0	18-Jun-26

Review

Reviewer	Review Criteria	Issue	Date
Greg Nott	ISO 27001:2022, ISO 9001:2015	1.0	06-Aug-23
Paul Langan	Review & Rebrand	2.0	13-May-24
Paul Langan	General Review	3.0	18-Jun-25
Greg Nott	Annual Review	4.0	18-Jun-26

Change History

Author	Change	Issue	Date
Paul Langan	Initial	1.0	23-May-23
Greg Nott	Review & Rebrand	2.0	13-May-24
Paul Langan	New CEO and Review	3.0	18-Jun-25
Greg Nott	Annual Review	4.0	18-Jun-26

Associated Documents

Document	Version
Information Security Planning Procedure	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 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

Purpose

This information security policy specifies management's intent to protect all information assets within ARO from all threats, whether internal or external, deliberate, or accidental. Information (both health and non-health) within ARO exists in many forms and this policy applies to and includes the protection of data stored electronically, transmitted across networks, and printed or written on paper. The prime purpose of this Information Security Policy is to protect and safeguard the information of the company, its' clients, and customers.

ARO, as a 'Data Processor' (GDPR¹) takes its custodianship of health data seriously and as such this policy supports the seven Caldicott principles and the associated ten data security standards.

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 & IT 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 Security Policy Statement

At ARO, we recognise the critical importance of protecting our information assets, maintaining the confidentiality, integrity, and availability of sensitive data entrusted to us by our customers, partners, and stakeholders. Our commitment to information security is unwavering, and we are dedicated to complying with ISO 27001:2022 and other relevant regulations to safeguard against security breaches, data loss, and unauthorised access.

Key Principles of our Information Security Policy:

- **Information Protection:** We prioritise the protection of all information assets, including customer data, intellectual property, and sensitive business information. Our employees are entrusted with the responsibility to handle this information with the utmost care and confidentiality.
- **Risk Management:** We adopt a risk-based approach to assess, identify, and address potential security threats and vulnerabilities. By conducting regular risk assessments, we implement appropriate controls to mitigate risks effectively.
- **Access Control:** We enforce strict access controls to ensure that information is accessible only to authorised personnel on a need-to-know basis. User access privileges are granted, reviewed, and revoked promptly as per their roles and responsibilities.

¹ Within the UK the GDPR has been incorporated into Data Protection Act 2018. The 2021 updated is known as the UK GDPR.

- **Employee Awareness:** We recognise that our employees are the first line of defence against information security threats. We provide comprehensive training and awareness programs to educate our staff about their roles in safeguarding information assets.
- **Incident Response:** In the event of a security incident, we have established procedures to respond promptly, investigate thoroughly, and implement corrective actions to prevent recurrence.
- **Compliance and Legal Requirements:** We commit to complying with all applicable information security laws, regulations, and contractual obligations. Our policies and practices align with ISO 27001:2022 and other relevant standards.
- **Supplier Security:** We hold our suppliers and business partners to the same high standards of information security. We collaborate closely with them to ensure the secure handling of information throughout the supply chain.
- **Continual Improvement:** We believe that information security is an ongoing journey. We regularly review and enhance our security measures, policies, and procedures to adapt to evolving threats and technologies.
- **Cloud Services:** Where multi-tenancy services are provided (i.e., Data Centre Cloud Services) ARO will ensure that each service is security isolated from other services.

Standards, policies, and security operating procedures will be produced to support this policy and will include virus control, access control, personnel security, the use of e-mail and the Internet. A formal disciplinary process will be documented and implemented for those employees who choose not to comply with these company standards, policies, and procedures.

The Head of Information Security & IT has overall responsibility for maintaining this Policy and providing guidance on its implementation.

All managers are personally responsible for implementing the policies and procedures within their business areas. It is the responsibility of each employee to adhere to the policies and procedures in their areas. Employees who do not adhere to the policies and procedures in their areas may be subject to the disciplinary process.

This policy will be reviewed regularly to ensure it remains appropriate for the business and ARO's ability to serve its customers.

Information Security Planning

When new objectives are identified (from risk arising from addition of new information assets, modification of existing information assets, internal and/or external audits, etc.) a plan of how to achieve these objectives must be done. Refer to the Information Security Planning Procedure document for further information.

Customer Copies

All customers may be provided with a copy of any policy (or policies) within the IMS upon request.

GDPR Principles

ARO has adopted the following GDPR principles:

- ARO will process all personal data fairly and lawfully.
- ARO will only process personal data for specified and lawful purposes.
- ARO will endeavour to hold relevant and accurate personal data, and where practical, we will keep it up to date.
- ARO will not keep personal data for longer than is necessary.

- ARO will keep all personal data secure.
- ARO will endeavour to ensure that personal data is not transferred to countries outside of the European Economic Area (EEA) without adequate protection.

Compliance with PII (Personal Identifiable Information) Protection Legislation

ARO confirms its support for and commitment to achieving compliance with applicable PII protection legislation, e.g., DPA Act 2018 (GDPR), ISO 27018:2020, etc.

ARO is primarily a data processor rather than a data controller.

Senior Management Team Approval

We, the senior management team at ARO, pledge to support this Information Security Policy and provide the necessary resources and guidance to achieve its objectives. Our collective commitment to information security supports our success and strengthens the trust our customers place in us.

Approved By		Ciaran Rafferty	
Signature of Approver			
Approver's Role Within ARO		CEO	
Issue	4.0	Date	18/06/2026