

Information Security in Supplier Relationships Policy

(ISO 27001:2022 Organisational Controls – Clause 5.19;
ISO 9001:2015 – Clause 8.4)

Author	Greg Nott
Version	2.0
Date Created	13/05/2023
Last Update Date	22/05/2024
Document Control	Released
Document ID	230513-IMS-POL-InformationSecurityInSupplierRelationships-V2
Security Classification	Public

Table of Contents

Information Security in Supplier Relationships Policy	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Purpose.....	4
Exceptions.....	4
Supplier Selection	4
Supplier Contracts.....	4
Information Exchange	5
Supplier Monitoring and Review	5
Incident Management.....	5
Continuous Improvement.....	5
Compliance	5
Roles and Responsibilities.....	5
Review.....	6

Approval

Author	Issue	Approved By	Date
Paul Langan	1.0	Simon Naylor	15-Aug-23
Greg Nott	2.0	Paul Langan	21-May-24

Review

Reviewer	Review Criteria	Issue	Date
Greg Nott	ISO 27001:2022	1.0	14-Aug-23
Paul Langan	Review & Rebrand	2.0	21-May-24

Change History

Author	Change	Issue	Date
Paul Langan	Creation	1.0	13-May-23
Greg Nott	Review & Rebrand	2.0	21-May-24

Associated Documents

Document	Version
230513-IMS-PRO-SupplierEvaluation-V1	1.0
230513-IMS-EVA-[SupplierName]Evalutation-V[n].dotx	1.0
230419-IMS-POL-InformationExchange-V2	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 Information Security in Supplier Relationships 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 suppliers who have access to the organisation's information assets or provide products or services that may impact the organisation's information security..

Purpose

ARO recognises the importance of maintaining a robust information security framework throughout its supply chain. This policy outlines the organisation's commitment to ensuring the confidentiality, integrity, and availability of information assets by establishing and maintaining secure supplier relationships in accordance with the above defined 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 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.

Supplier Selection

- ARO will establish a defined process for selecting suppliers (Supplier Evaluation) based on their ability to meet quality and information security requirements.
- Quality and Information security requirements shall be included in the supplier selection criteria, and potential suppliers shall be assessed for their adherence to these requirements.

Supplier Contracts

- ARO will ensure that supplier contracts address information security obligations.
- Supplier contracts will include provisions for the protection of the ARO's information assets, confidentiality, and compliance with applicable laws and regulations.
- ARO reserves the right to audit suppliers' information security practices periodically to verify compliance with contractual obligations.

Information Exchange

- ARO will establish secure methods for exchanging information with suppliers.
- When necessary, encryption and other appropriate security controls shall be used when transmitting information.

Supplier Monitoring and Review

- ARO will regularly monitor and review the performance of suppliers with respect to information security.
- Supplier compliance with information security requirements shall be assessed periodically through audits and evaluations.
- Any identified non-compliance or security incidents shall be promptly addressed, and appropriate actions taken.

Incident Management

- Suppliers will (where possible) promptly report any information security incidents or breaches to ARO.
- ARO shall have a defined process for managing and responding to supplier-related security incidents, including investigation, containment, and recovery.

Continuous Improvement

- ARO continuously improve the information security practices within its supplier relationships.
- Lessons learned from security incidents and audits shall be used to enhance the effectiveness of supplier-related information security controls.

Compliance

- Non-compliance with this policy may result in termination or suspension of the supplier relationship.
- Suppliers shall be made aware of their information security obligations and the consequences of non-compliance.

Roles and Responsibilities

- ARO shall designate individuals responsible for managing supplier relationships and ensuring compliance with this policy.
- All employees involved in supplier relationships shall be educated and trained on their information security responsibilities.

Review

This policy shall be reviewed and revised as necessary, but at least annually, to ensure its ongoing suitability and effectiveness.