

Information Security in Supplier Agreements Policy

(ISO 27001:2022 Organisational Controls – Clause 5.20)

Author	Greg Nott
Version	2.0
Date Created	14/05/2023
Last Update Date	22/05/2024
Document Control	Released
Document ID	230514-IMS-POL-InfoSecInSupplierAgreements-V2
Security Classification	Public

Table of Contents

Information Security in Supplier Agreements Policy	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Purpose.....	4
Exceptions.....	4
Confidentiality and Non-Disclosure	4
Data Protection and Privacy.....	4
Security Controls and Measures	5
Incident Response and Notification	5
Subcontractors and Third Parties.....	5
Compliance and Auditing.....	5
Termination and Transition	5
Indemnification and Liability.....	6
Governance and Review	6

Approval

Author	Issue	Approved By	Date
Paul Langan	1.0	Simon Naylor	03-Aug-23
Greg Nott	2.0	Paul Langan	21-May-24

Review

Reviewer	Review Criteria	Issue	Date
Greg Nott	ISO 27001:2022	1.0	02-Aug-23
Paul Langan	Review & Rebrand	2.0	21-May-24

Change History

Author	Change	Issue	Date
Paul Langan	Creation	1.0	14-May-23
Greg Nott	Review & Rebrand	2.0	21-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 Information Security in Supplier Agreements 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 staff within ARO who are involved in creating agreement with suppliers.

Purpose

The purpose of this policy is to outline how ARO should form an agreement with a supplier from the outset of a relationship with that client. In other words, what should be included in an agreement that would clearly state the obligations between ARO and the supplier.

Note that depending on the service and goods being supplied contents of each supplier agreement may differ.

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 (or a member of the IMS Team).
- All exceptions to this policy MUST be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

Confidentiality and Non-disclosure

The agreement should include clauses that clearly state the supplier's obligation to maintain the confidentiality of any information shared during the business relationship. This should cover at least:

- Customer data,
- Trade secrets,
- Intellectual property,
- and any other sensitive information.

Data Protection and Privacy

- The agreement should address data protection and privacy requirements by outlining the supplier's responsibility to comply with applicable laws and regulations, such as the General Data Protection Regulation (GDPR) or other relevant data protection frameworks.
- The agreement needs to specify how personal data (if any) should be handled, processed, stored, and protected.

Security Controls and Measures

The agreement should define the minimum-security controls and measures expected from the supplier to protect information. This may include requirements such as:

- encryption,
- access controls,
- intrusion detection systems,
- vulnerability assessments,
- incident response procedures,
- security audits.

Incident Response and Notification

- The agreement needs to establish clear procedures for reporting and managing security incidents. Specify the supplier's obligation to promptly notify the contracting party of any actual or suspected security breaches or incidents involving the shared information.
- The agreement needs to define the timeline and communication channels for reporting incidents and outline the steps for investigation, containment, and remediation.

Subcontractors and Third Parties

If the supplier engages subcontractors or third-party vendors in providing the contracted services, the agreement needs to outline the supplier's responsibility to ensure that these entities adhere to the same information security requirements. Include clauses that grant the contracting party the right to audit or assess the security practices of subcontractors.

Compliance and Auditing

- The agreement needs to specify the supplier's obligation to comply with relevant laws, regulations, and industry standards related to information security.
- The agreement needs to define the rights of the contracting party to conduct security audits or assessments to verify compliance. Include provisions for sharing audit reports and addressing any identified security gaps or non-compliance.

Termination and Transition

- The agreement needs to outline the information security requirements upon contract termination or expiration.
- The agreement needs to specify how the supplier should handle and transfer the shared information securely back to the contracting party or to another designated entity. Include provisions for data destruction or return, as applicable.

Indemnification and Liability

The Agreement needs to clearly define the supplier's liability for any security breaches or non-compliance with information security obligations. Include provisions for indemnification, damages, and financial remedies in case of breaches resulting in loss, damages, or regulatory penalties.

Governance and Review

The agreement needs to specify the governance and review mechanisms for monitoring and enforcing information security provisions. This may include regular security performance reviews, periodic assessments, or joint security committees to discuss security concerns, incidents, and improvements.