

Information Security FAQ

Author	Paul Langan
Version	1.0
Date Created	04/06/2024
Last Update Date	04/06/2024
Document Control	Released
Document ID	240604-IMS-RPT-InformationSecurityFAQ-V1
Security Classification	Public

Table of Contents

Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Purpose	4
Questions and Answers.....	4
General.....	4
Organisational Security	5
Information/Data Asset Classification.....	6
Personnel Security	7
Physical and Environmental Security	7
Communications and Operations	9
Access Control.....	10
Information Security Incident/Data Breach Management.....	11
Business Continuity Management	11
Compliance	12

Approval

Author	Issue	Approved By	Date
Paul Langan	1.0	Greg Nott	04-Jun-2024

Review

Reviewer	Review Criteria	Issue	Date
Greg Nott	Security Compliance	1.0	04-Jun-24

Change History

Author	Change	Issue	Date
Paul Langan	Initial	1.0	04-Jun-2024

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.

- ISO 27001:2022 – Information Security Management Systems
 - ISO 27017:2015 – Code of Practice for Cloud Services
 - ISO27018:2020 – Code of Practice for PII Data
- ISO 9001:2015 – Quality Management System
- DSPT (Data Security and Protection Toolkit) for the NHS.
- Cyber Essentials Plus

Purpose

The purpose of this document is to provide ARO customers and partners information on how we protect the information entrusted to us. The below FAQ can be read in conjunction with the policies and summary published on our website at aro.tech/policies. Further information may be provided upon request subject to appropriate confidentiality.

Questions and Answers

General

#	Question	ARO Answer
1.1	Does ARO hold or comply with any information security or information technology relevant certifications?	ARO is independently certified for the following standards: (1) ISO27001:2022 - Information Security Management Systems (2) ISO27017:2015 Code of Practice for information security controls based on ISO27002 for Cloud Services (3) ISO27018:2022 Code of Practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. (4) ISO 9001:2015 – Quality Management Systems (5) Cyber Essentials (6) Cyber Essentials Plus (7) NHS DSPT – ODS #: 8J121
1.2	What is ARO's ICO Data Protection Registration Number?	Z9552844
1.3	Does ARO have a documented Information Security Policy?	ARO has an externally audited Information Security Management System based around the above standards, which includes our Information Security Policy. This and other key policies are available on our website at aro.tech/policies .
1.4	How often are the ARO security policies reviewed and updated?	All ARO policies are reviewed and updated at least annually, or in response to relevant changes to the business or its operations.
1.5	Who in ARO is responsible for the security policy development, maintenance, and issuance?	Overall responsibility sits with our Head of Information Security supported by our Security Advisory Board, Internal Audit team and Management Review Board.

1.6	Are all ARO security policies and standards readily available to all users?	Yes, all policies and related information and training collateral is freely available to all users. Key policies and related information are also available publicly on our website.
1.7	What security areas are addressed in the ARO information security policies?	Constructed to ISO 27001:2022 standards our Information Security Management System includes polices covering areas of Organisational Controls, People Controls, Physical Controls, Technological Controls, Cloud Service Controls and Protection of PII Controls. Key topics include Acceptable Use of Assets, Access Controls, Data Protection, Incident Response, Business Continuity, Infrastructure Security, Supplier Management and Legal Compliance.
1.8	Are ARO's security policies available for review?	Yes, our key policies are available on our website at aro.tech/policies . Further information not available on the website may be available upon request subject to appropriate confidentiality agreement.

Organisational Security

#	Question	ARO Answer
2.1	Have ARO security have roles and responsibilities been clearly defined and documented?	Yes, Roles & Responsibilities are clearly documented within our contract of employment, staff handbook, management system policies and our IMS Roles and Responsibilities Register.
2.2	Have ARO security policies, standards, and procedures been reviewed and certified by a qualified third party such as an accredited audit body?	Yes, the ARO Integrated Management System is independently certified to the above listed ISO standards by DNV – Business Assurance. (DNV - Business Assurance, 4 th Floor, Vivo Building, 30 Stamford Street, London, SE1 9LQ) The Management system is reviewed by DNV annually.
2.3	Has the ARO security perimeter infrastructure been assessed and reviewed by a qualified third party?	Yes, this is included in our annual audit with DNV – Business Assurance.
2.4	Do ARO contracts with third parties contain language describing responsibilities regarding information protection requirements?	Yes, all contracts with third parties contain provisions to ensure proper protection and security of our information and assets, appropriate to the risk of each relationship.
2.5	Does ARO have a process for granting privileged access to data?	Yes, strict controls are adopted by ARO to restrict privileged access to information assets, over and above our standard access control policies. Wherever possible privileged access is only granted on a time-limited basis to avoid 'persistent privilege' and 'privilege creep' risks. For customer privileged access to their assets hosted within our data centre facilities, requests can be raised through our ITSM platform specifying time, date, individuals and reasons for

		access. Access must be authorised by members of the ARO SDCS technical staff. If physical access to customer assets is requested, first time visitors must provide photo ID upon arrival. Customers may request that only specific personnel can authorise entry for their employees. Requests for access MUST be made 24 hours in advance. Requests for access made less than 24 hours in advance may be declined at the discretion of ARO.
--	--	--

Information/Data Asset Classification

#	Question	ARO Answer
3.1	Does ARO maintain an inventory of all important information assets and asset owners clearly identified?	Yes, a full register of all information assets is maintained including asset owners, location(s), PII status and applicable controls.
3.2	Describe the information classification methods and labelling practices adopted by ARO.	All ARO information is classified into four bands: • Confidential → Information issued only to parties authorised by the information owner / data controller. Information will be made available and distributed strictly on an approved, need-to-know basis. • Commercial-In-Confidence → Information that is Shared/Co-authored with partners that contains proprietary information or one of more parties. • Internal → ARO information not deemed to be strictly confidential nor public. Open to all staff only. • Public → General Release
3.3	Does ARO have formal procedures for handling and storage of information assets?	Yes, our Information Handling, Information Labelling and Data Destruction policies are all available for review on our website at [URL]. In respect of Personal Identifiable Information (PII, also known as Personal Identifiable Data (PID)) ARO maintains a robust set of policies and procedures to ensure compliance with UK GDPR and the Caldicott Principles, for keeping individuals' personal data safe and private. Our Transparency & Privacy policy and GDPR Compliance Statement are both available on our website.
3.4	What encryption standards does ARO use?	ARO enforces that all sensitive information is encrypted both at rest and in transit. All algorithms, key lengths and protocols are up-to-date and approved by the National Cyber Security Council (NCSC) and NHS England, including Triple DES, AES and RSA. The exact encryption methods used will be dependent upon the type, location(s) and communication channel(s) of the information in question.
3.5	What country will ARO data be stored and processed in?	All information processed by ARO is done so in the UK. All information is held in EEA-based data centres.

Personnel Security

#	Question	ARO Answer
4.1	Do ARO terms and conditions of employment clearly define information security requirements?	Yes, ARO employment contracts include provisions for data protection, confidentiality / non-disclosure and post-termination obligations, for both employees and contractors.
4.2	Does ARO screen all users (employees, contractors, vendors, and other third parties)?	Yes, all employees and contractors are screened including right to work, reference check, and DBS checks where required. All vendors are subject to a rigorous assessment process before approval to partner with them is granted.
4.3	Does ARO conduct formal information security awareness and governance training for all users, including upper management?	Yes, all ARO users are subject to appropriate training upon induction to the business and on an ongoing basis.
4.4	Does ARO require additional training for system administrators, developers, researchers and other users with privileged usage?	Yes, further training is provided to users as appropriate to their role and duties.
4.5	Is there a formal procedure dictating actions that must be taken when a user has violated any of the ARO security policies?	Yes, ARO operates robust procedures to investigate, remediate and educate users including, if necessary, a formal disciplinary process.
4.6	Are all ARO employees required to sign a confidentiality agreement?	Yes, all users are subject to confidentiality clauses within their contract of employment.

Physical and Environmental Security

#	Question	ARO Answer
5.1	Are all critical ARO information assets located in a physically secure area?	Yes, all such assets are in secure spaces, primarily secure data centres including our own facility in Liverpool, and industry leading public cloud platforms.
5.2	Are ARO information assets protected by fire suppression systems?	All ARO locations are protected by a minimum of fire alarms, fire extinguishers and fire blankets. The ARO SDCS Liverpool Data Centre has the following fire suppression systems installed: • Independent VESDA detection. • 'Double knock' co-incidence system-controlled suppressant discharge. • FM 200 (HFC-227ea) environmentally friendly gas suppression. • Fully integrated with BMS.
5.3	What physical access control restrictions have ARO put in place?	Access to ARO facilities is protected by various account control systems including ID badges, smart NFC devices and biometric scanners.

		Access to ARO Data Centre facilities requires multiple such form factors (minimum 2) for access. Access is granted on a strictly need-to-know basis with individuals restricted to only those areas needed to carry out their duties. This is especially enforced in our Liverpool Data Centre where only a very small number of people are allowed access to the data halls and supporting utilities. Access is maintained on a separate platform from the rest of the Liverpool facility.
5.4	How is contractor access granted to ARO secure locations?	When required, third party access to our secure areas is strictly limited. Access must be planned, reviewed and approved by the appropriate information asset owner(s). All third parties being allowed access to secure areas must be ID checked and escorted or always monitored. Customer requests for third party access to their physical assets within our data centre facilities must be formally requested via our ITSM platform, specifying time, date, attendees and purpose of works to be conducted. Access must be authorised by members of the ARO Technical staff and/or Operations Director. Visitors must provide photo ID upon arrival. Customers may request that only specific personnel can authorise entry for their third parties. Requests for access MUST be made 24 hours in advance. Requests for access may be declined for any reason at the discretion of ARO to ensure the security of our facilities and information assets.
5.5	What exterior security is provided for at ARO facilities (i.e. gates, secure vehicle access, security cameras, etc.)?	As a minimum all ARO facilities are protected by physical locking mechanisms, access control systems, security cameras and monitored security alarms. Certain facilities may also benefit from perimeter fencing, gates, secure vehicle access and security personnel dependent upon their location. The ARO SDCS Liverpool Data Centre is located in a secure technology park, protected by secure fencing with a single point of entry and manned security lodge (24-hour, 365 days per year). The perimeter and all vehicle / pedestrian access points are monitored by CCTV and protected by infrared detection.
5.6	Are ARO systems configured to record system faults?	Yes, all systems are configured to record and alert faults to our technical teams for immediate investigation.
5.7	Do ARO have a formal media destruction policy?	Yes, see our Data Destruction and Management of Storage Media policies for more information.
5.8	Does ARO employ automatic locking screen savers when users' workstations remain idle after a set period?	Yes, all workstations will automatically lock after a set period, but all users are advised to manually lock their workstation when leaving it unattended.
5.9	How is the removal of information assets from ARO premises authorised and controlled?	The removal of any information assets must be formally approved by the appropriate information asset owner(s) after being logged as a formal change request. Removal will then be conducted by only competent, authorised personnel and

		handled per the appropriate hand policies for transfer, reuse and/or disposal.
5.10	Are logs maintained that record all changes to ARO information systems?	Yes, all changes to ARO systems are recorded per our formal Change Management policy & procedures.

Communications and Operations

#	Question	ARO Answer
6.1	Do ARO segregate duties to ensure a secure environment?	Where practicable operational responsibilities are allocated in a way which avoids overlapping areas of interest between any individual's duties. Where this is not possible ARO use supervision and shared controls to minimise threats, which may arise from such an overlap. Reviews of user access rights are conducted regularly to ensure that these objectives are met. As necessary access rights will be removed from users who no longer need such access to conduct their duties.
6.3	How does ARO protect its systems against newly discovered vulnerabilities and threats?	ARO employs a systematic approach including continuous monitoring, automated patch management, regular vulnerability scans, and threat intelligence integration. Additionally, we maintain secure configurations, conduct employee training, and collaborate with industry partners and other special interest groups to enhance our security measures.
6.4	How does ARO prevent end users from installing potentially malicious software?	We prevent end users from installing potentially malicious software by implementing strict access controls and application whitelisting. Only approved applications can be installed, and we use endpoint protection software to detect and block malicious software. Additionally, we provide regular training to employees on the risks of unauthorised software and continuously monitor and enforce compliance with our security policies.
6.4	Does ARO scan traffic coming into your network for malware?	Yes, traffic into ARO network(s) is scanned for malware at various points including firewall appliances, email gateways, software firewalls and EDR platforms.
6.5	How does ARO dispose of storage media when they are no longer of use?	Disposal will be undertaken in a sensitive way, which ensures that no sensitive information becomes available in the public domain in line with our Data Destruction and Secure Disposal & Reuse of Equipment policies. For customer data hosted in an ARO Data Centre they can request that data is removed per device. If requested, destruction will be carried out in accordance with the Data Destruction Policy, with sanitisation methods including: • Clearing → Public/Private Clouds. On shared drives and media data destruction will involve deletion of data from the file system and where possible an overwrite process to ensure the data is not recoverable.

		• Purging → Private Clouds only. Degauss of the media. • Destruction → Private Clouds only. Media is shredded. ARO will supply the customer with a 'Certificate of Data Destruction' recording the date, method and name of the technician responsible for the destruction of the data.
6.6	Does ARO keep logs of media disposal activity?	Yes, all disposal activities are formally recorded including identifiers, dates / times, methods used and certificates or other proof of destruction.
6.7	Are ARO backup procedures documented and monitored to ensure they are properly followed?	Yes, critical information assets are backed up as appropriate to ensure the confidentiality, integrity and accessibility of information in the event of a security or business continuity incident. ARO maintains an internal schedule to ensure compliance with our IMS policies and procedures.
6.8	What processes and standards does ARO follow for incident management, problem management, change management, and configuration management?	ARO maintains a robust set of operational management procedures constructed in line with the ITIL framework, as well as documented Information Security Incident Response and Data Breach procedures, all of which are available on our website at aro.tech/policies .

Access Control

#	Question	ARO Answer
7.1	Does ARO have an Access Control policy?	Yes, ARO takes all reasonable steps to prevent unauthorised access to its systems, information and facilities. Access rights are always granted on a 'least privilege' basis and must follow formal procedures for approval. Access credentials and other tokens are unique to the individual, and all activity is logged and monitored. Access rights are regularly reviewed to ensure they are appropriate and revoked when no longer needed. For more information our Access Control Policy is available on our website at aro.tech/policies along with a summary of other related policies.
7.2	Does ARO conduct periodic checks on users' accesses to ensure their access matches their responsibilities?	Yes, access rights are checked regularly to ensure they are still up-to-date and appropriate, the schedule for which is determined by the criticality and risk of the system or information being accessed.
7.3	Do ARO utilise any type of Host Intrusion Prevention or Detection software?	ARO employ several leading Endpoint Detection & Response (EDR) and Managed Detection & Response (MDR) tools to protect our endpoints.
7.4	Are failed login attempts to ARO systems recorded and reviewed on a regular basis?	Yes, all systems are configured to retain logs of activity including failed sign-ins. Where possible systems are configured to alert in real-time based on appropriate baseline criteria.

Information Security Incident/Data Breach Management

#	Question	ARO Answer
8.1	Does ARO have a dedicated Information Security Response Team(s)?	Yes, ARO maintain several Critical Security Incident Response plans, relevant to distinct functions and units within the organisation. Each plan details the roles & responsibilities of the related team.
8.2	Are the ARO Incident Response Team(s) trained in evidence gathering and handling?	Yes, all response teams are led by trained, experienced incident responders and comply with the ARO Collection of Evidence policy as required.
8.3	Are incident reports issued to appropriate ARO management / other stakeholders?	Yes, ARO ensure appropriate reporting and awareness is conducted to relevant stakeholders during and after an incident.
8.4	After an incident, does ARO review its policies and procedures to determine if modifications need to be implemented?	Yes, all ARO Critical Security Incident Response plans include post-incident tasks which may include modifying policy or procedure if required.

Business Continuity Management

#	Question	ARO Answer
9.1	Has an ARO Business Continuity plan been built and a mission statement identifying scope and responsibilities been published?	Yes, ARO maintains a top-level Business Continuity plan and Crisis Management Strategy Communication structure, as well as localised Disaster Recovery plans for each business unit. Roles & responsibilities are detailed within each plan.
9.2	Has a "worst-case" scenario to recover within a prescribed timeframe been implemented and tested within ARO?	Yes, all Business Continuity / Disaster Recovery plans are test on a regular basis.
9.3	Is a list of current emergency telephone numbers for police, fire department, medical aid and company officials available to all ARO employees?	Yes, relevant contact details for stakeholders are made available to all personnel.
9.4	Have lead times for communication lines and equipment, specialised devices, or other specialised requirements been considered into the ARO Disaster Recovery Plans?	Yes, all plans include considerations for specialist / long lead time requirements.
9.5	Are ARO Business Continuity & Disaster Recovery plans stored in multiple locations and updated regularly?	Yes, all plans are stored in multiple locations to ensure access when required. All plans are reviewed and updated at least annually or as required for relevant changes.

9.6	Does ARO have automatic restart and recovery procedures in place to restore data files in the event of a processing failure?	Yes, where possible automatic recovery procedures are in place, most particularly within our data centre operations.
9.7	Does ARO have contingency arrangements in place for hardware, software, communications and staff?	Yes, our resource management policies and procedures ensure for contingency arrangements when required.

Compliance

#	Question	ARO Answer
10.1	Are the ARO security policies and procedures routinely tested?	Yes, all policies and procedures are reviewed and tested on a regular basis, the frequency of which is determined by the criticality & risk of each.
10.2	Are exceptions to ARO security policies and procedures justified and documented?	Yes, any exceptions to the standard policies are fully documented and must be approved by the Head of Information Security.
10.3	Are audit logs or other reporting mechanisms in place on all ARO platforms?	Yes, all systems are configured to maintain activity logs for review. Where possible alerts will be raised in real time for investigation.
10.4	When an ARO employee is found to be in non-compliance with the security policies, has appropriate disciplinary action been taken?	Yes, where required formal disciplinary action is taken and all outcomes documented. Where appropriate follow up actions are also taken to ensure awareness of, and compliance with, the relevant policies are enforced throughout ARO.
10.5	Are audits of the ARO management system performed on a regular basis?	Yes, ARO maintains an ongoing internal audit schedule and external ISO certification audits are conducted annually.
10.6	Does ARO conduct unscheduled / surprise audits performed?	Yes, the ARO internal audit schedule includes unscheduled audits.
10.7	Has someone been identified within ARO as responsible for managing audit results?	Yes, all audit results are managed & communicated by the Head of Information Security and ISMS Manager.