

# Summary of ARO Information Security & Quality Policies

(ISO 27001:2022; ISO 9001:2015)

|                         |                                               |
|-------------------------|-----------------------------------------------|
| Author                  | Greg Nott                                     |
| Version                 | 2.0                                           |
| Date Created            | 24/05/2024                                    |
| Last Update Date        | 06/12/2024                                    |
| Document Control        | Released                                      |
| Document ID             | 240524-IMS-POL-InfoSecQualityPolicySummary-V2 |
| Security Classification | Public                                        |

## Table of Contents

|                                                                         |          |
|-------------------------------------------------------------------------|----------|
| <b>Summary of ARO Information Security &amp; Quality Policies .....</b> | <b>1</b> |
| Approval.....                                                           | 5        |
| Review.....                                                             | 5        |
| Change History.....                                                     | 5        |
| Associated Documents.....                                               | 5        |
| Scope.....                                                              | 6        |
| Headline Statements.....                                                | 6        |
| Quality Policy Statement.....                                           | 6        |
| Information Security Policy Statement .....                             | 7        |
| Management Responsibilities Policy.....                                 | 8        |
| Integrated Management System Manual .....                               | 8        |
| Roles & Responsibilities Policy .....                                   | 8        |
| Communications Policy.....                                              | 8        |
| Review of Information Security Policy .....                             | 8        |
| Anti-Corruption & Bribery Policy .....                                  | 8        |
| Security in Marketing Policy.....                                       | 9        |
| Threat Intelligence Policy.....                                         | 9        |
| Contact with Special Interest Groups Policy .....                       | 9        |
| Analysis of Data Policy .....                                           | 9        |
| Acceptable Usage Policies.....                                          | 9        |
| Acceptable Use of Assets Policy.....                                    | 9        |
| Security in Email Policy .....                                          | 10       |
| Social Media Policy .....                                               | 11       |
| Mobile Computing Policy.....                                            | 11       |
| Installation of Software on Operational Systems Policy.....             | 11       |
| Use of Privileged Utility Programs Policy .....                         | 12       |
| Access Control Policies.....                                            | 12       |
| Access Control Policy .....                                             | 12       |
| User Registration Policy .....                                          | 12       |
| Identity Management Policy .....                                        | 12       |
| Password Management Policy .....                                        | 12       |
| Secure Authentication Policy .....                                      | 13       |
| Information Access Restriction Policy .....                             | 13       |
| Privileged Access Rights Policy.....                                    | 14       |
| Disabling Customer User Accounts Policy.....                            | 14       |

|                                                                 |    |
|-----------------------------------------------------------------|----|
| Access to Program Source Code Policy .....                      | 14 |
| Data Protection Policies .....                                  | 14 |
| Transparency & Privacy Policy.....                              | 14 |
| GDPR Compliance Statement.....                                  | 14 |
| Confidentiality Policy .....                                    | 14 |
| Information Labelling Policy.....                               | 15 |
| Information Handling Policy.....                                | 15 |
| Logging Policy.....                                             | 15 |
| Protection of Records Policy .....                              | 16 |
| Clear Desk & Screen Policy.....                                 | 16 |
| Information Backup Policy .....                                 | 16 |
| Use of Cryptography Policy .....                                | 16 |
| Customer Off-boarding Policy .....                              | 16 |
| Data Destruction Policy.....                                    | 17 |
| Secure Disposal & Reuse of Equipment Policy.....                | 17 |
| Securing Rooms, Offices & Facilities Policy.....                | 17 |
| Physical Security Monitoring Policy .....                       | 17 |
| Protection Against Physical & Environmental Threats Policy..... | 18 |
| Supporting Utilities Policy .....                               | 18 |
| Working in Secure Areas Policy.....                             | 18 |
| Privacy by Design Policy .....                                  | 18 |
| Data Masking Policy .....                                       | 18 |
| Information Exchange Policy.....                                | 19 |
| Data Leakage Prevention Policy .....                            | 19 |
| Biometric Policy .....                                          | 19 |
| People Security Policies .....                                  | 19 |
| Termination of Employment Policy.....                           | 19 |
| Segregation of Duties Policy.....                               | 20 |
| Information Security in Project Management Policy .....         | 20 |
| Incident Response / Business Continuity Policies.....           | 20 |
| Reporting Security Incidents Policy.....                        | 20 |
| Security Incident Response Policy.....                          | 20 |
| Data Breach Policy .....                                        | 20 |
| Learning from Security Incidents Policy .....                   | 21 |
| Redundancy of Information Processing Facilities Policy .....    | 21 |
| Information Security During Disruption Policy.....              | 21 |
| Infrastructure Security Policies .....                          | 21 |
| Change Management Policy .....                                  | 21 |
| Configuration Management Policy.....                            | 21 |

|                                                                                                                   |    |
|-------------------------------------------------------------------------------------------------------------------|----|
| Capacity Management Policy.....                                                                                   | 22 |
| Security of Network Services Policy .....                                                                         | 22 |
| Separation of Environments Policy .....                                                                           | 22 |
| Virtual Private Network Policy .....                                                                              | 22 |
| Information Security for the Use of Cloud Services Policy.....                                                    | 23 |
| Web Filtering Policy .....                                                                                        | 23 |
| Protection Against Malware Policy .....                                                                           | 23 |
| Vulnerability Management Policy .....                                                                             | 24 |
| Virtual Machine Hardening Policy.....                                                                             | 24 |
| Management of Storage Media Policy.....                                                                           | 24 |
| Clock Synchronisation Policy .....                                                                                | 24 |
| Monitoring Activities Policy .....                                                                                | 24 |
| Equipment Siting Policy.....                                                                                      | 25 |
| Cabling Security Policy .....                                                                                     | 25 |
| Supplier Management Policies .....                                                                                | 25 |
| Procurement Policy.....                                                                                           | 25 |
| Information Security in Supplier Agreements Policy .....                                                          | 26 |
| Information Security in Supplier Relationships Policy / Information Security in the ICT Supply Chain Policy ..... | 26 |
| Legal Policies .....                                                                                              | 26 |
| Compliance with Legal Requirements Policy .....                                                                   | 26 |
| Intellectual Property Rights Policy .....                                                                         | 26 |
| Software Development Policies .....                                                                               | 27 |
| Secure System Development & Engineering Principles .....                                                          | 27 |
| Secure Development Lifecycle Policy.....                                                                          | 27 |
| Test Information Policy.....                                                                                      | 27 |
| Outsourced System Development Policy .....                                                                        | 27 |

## Approval

| Author    | Issue | Approved By | Date      |
|-----------|-------|-------------|-----------|
| Greg Nott | 1.0   | Paul Langan | 31-May-24 |
| Greg Nott | 2.0   | Greg Nott   | 06-Dec-24 |

## Review

| Reviewer    | Review Criteria | Issue | Date      |
|-------------|-----------------|-------|-----------|
| Paul Langan | ISO 27001:2022  | 1.0   | 31-May-24 |
| Paul Langan | Minor Fixes     | 2.0   | 06-Dec-24 |

## Change History

| Author    | Change      | Issue | Date      |
|-----------|-------------|-------|-----------|
| Greg Nott | Creation    | 1.0   | 24-May-24 |
| Greg Nott | Minor Fixes | 2.0   | 06-Dec-24 |

## Associated Documents

| Document                                                 | Version |
|----------------------------------------------------------|---------|
| See document references in line with the below summaries |         |
|                                                          |         |

## Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and summarises the policies for Information Security Management and Quality Management 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 document applies to all Employees, contractors, and third-party collaborators who access, handle, or analyse data on behalf of the organisation.

## Headline Statements

### Quality Policy Statement

At ARO, we are dedicated to delivering exceptional products and services that exceed customer expectations while ensuring compliance with ISO 9001:2015 and other applicable requirements. Our commitment to quality is embedded in every aspect of our operations, within our organisation Values, and we strive to continually improve our processes, performance, and customer satisfaction.

#### Key Principles of our Quality Policy:

- **Customer Focus:** Our customers are at the heart of everything we do. We actively listen to their needs, expectations, and feedback, and use this insight to provide tailored solutions that add value to their businesses.
- **Continuous Improvement:** We believe in the power of ongoing improvement. By regularly evaluating our processes and systems, we identify opportunities to enhance efficiency, quality, and the overall customer experience.
- **Empowered Workforce:** Our Employees are our greatest asset. We foster a culture of empowerment, collaboration, and personal development, encouraging everyone to take ownership of quality and contribute to the organization's success.
- **Compliance and Standards:** We are committed to upholding the requirements of ISO 9001:2015 and other relevant industry standards. Our processes are designed and executed to ensure adherence to these guidelines consistently.
- **Supplier Partnerships:** We maintain strong partnerships with our suppliers, working together to deliver high-quality materials and services that align with our commitment to excellence.
- **Risk-Based Approach:** We employ a risk-based thinking approach to identify potential issues proactively and take preventive actions to mitigate risks and maximize opportunities.
- **Environmental Responsibility:** We embrace sustainable practices that minimize our environmental impact, striving to promote eco-friendly solutions in our products and operations.

- **Data-Driven Decisions:** Our decisions are based on accurate data and analysis, enabling us to make informed choices that contribute to the continuous improvement of our products and services.

This Quality Policy is communicated and understood at all levels of our organisation. It is regularly reviewed to ensure its ongoing relevance and effectiveness, supporting our journey towards becoming a leader in delivering quality products and services.

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

## 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.
- **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 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.

## Management Responsibilities Policy

At ARO, we are committed to maintaining the confidentiality, integrity, and availability of information assets, as well as continually improving our integrated management system (IMS). This policy outlines our management's commitment to the effective implementation, maintenance, and continual improvement of the ISO 27001:2022 standard. All managers within ARO should read the full policy.

## Integrated Management System Manual

The purpose of the Integrated Management System (IMS) manual is to establish and document the integrated approach to quality and information security management within ARO, outlining the processes required to ensure consistent delivery of high-quality products and services while maintaining the security of information assets in compliance with ISO 9001:2015 and ISO 27001:2022 standards. All managers / owners should read the full manual.

## Roles & Responsibilities Policy

It is crucial that everyone who works for ARO understands their roles & responsibilities in our operations, particularly with regards to quality management and information security. Specific roles and responsibilities are communicated through the contract of employment, training, policy, and process documents. Additionally, ARO maintains a register that details everyone's roles & responsibilities to successful maintenance of the IMS based on their functions within the business (i.e. as an Employee, as a line manager, as a system owner etc). All personnel should familiarise themselves with the register to understand the part they play.

## Communications Policy

It is important that we maintain effective communications with all interested parties and special interest groups that are relevant to ARO. We have established clear roles & responsibilities for communication in the organisation including through the Interested Parties register, Information Asset register, and Business Continuity & Disaster Recovery plans. Numerous effective channels for communication are authorised and maintained within ARO including email, social media, website, face-to-face meetings, training documents, policy documents, and staff handbook.

## Review of Information Security Policy

To maintain our Information Security Management System, we periodically check the effectiveness of the system and its controls. As well as regular internal audits and periodic external audits, ARO undertakes other reviews of its IMS including penetration tests, vulnerability scanning, phishing simulations, Cyber Essentials assessments, financial regulatory audits, insurance provider cyber maturity assessments.

## Anti-Corruption & Bribery Policy

ARO is bound by the provisions of the Anti-bribery Act 2010. It is our policy to conduct all our business in an honest and ethical manner. We take a zero-tolerance approach to bribery and corruption and are committed to acting professionally. During induction, and as directed by the Head of Legal from time to time, all Employees of ARO must ensure they read, understand, and comply with the full policy.

## Security in Marketing Policy

Sensitive marketing information such as prospect data, customer data, market research and other competitive intelligence must be protected. In line with the policies of this IMS access to marketing information shall be restricted to only those users that require it and only to the extent necessary to perform their duties. Controls should be put in place to monitor activity within marketing information for suspicious activity. Personally Identifiable Information (PII) must be handled in accordance with relevant data protection laws, ensuring appropriate consent, storage and processing practises including suitable retention, backup, and disaster recovery mechanisms.

## Threat Intelligence Policy

We need to be equipped with the necessary tools and processes to proactively identify, assess, and mitigate potential information security threats. Threat intelligence should be collected from our internal systems and reputable external sources. Threat intelligence should be logged, analysed, disseminated to relevant stakeholders with ARO and customers as appropriate, and mitigating activity should be planned, approved, and documented in line with relevant Change Management processes. Threat intelligence should be utilised efficiently and effectively across the organisation with analysts collaborating to this end.

## Contact with Special Interest Groups Policy

ARO will maintain contact with Special Interest Groups, specialist security forums and professional associations to improve knowledge about best practice, keep up to date, receive early warnings, gain advice, and share knowledge. All Employees are also encouraged to consider subscribing for a membership in special interest groups where appropriate to their role.

## Analysis of Data Policy

ARO recognises the importance of analysing data to drive continuous improvement. Data analysis practices must be consistent whilst also safeguarding privacy, integrity and support informed decision making. Guidelines have been established for data collection, preparation, analysis methods, data integrity, quality, privacy, security, and decision making. Personnel involved in the analysis of information should read the full policy.

# Acceptable Usage Policies

## Acceptable Use of Assets Policy

### General Principles

- Information and associated assets shall be used in a lawful, ethical, and responsible manner.
- Users shall protect the confidentiality, integrity, and availability of information and assets.
- Users shall comply with applicable laws, regulations, and contractual obligations.
- ARO reserves the right to monitor and audit the use of information and associated assets to ensure compliance with this policy.

### User Responsibilities

- Users shall access and use information and associated assets solely for authorised business purposes.
- Users shall not disclose sensitive or confidential information to unauthorised individuals or organisations.
- Users shall not misuse or abuse information and assets for personal gain or malicious purposes.
- Users shall report any suspected or actual unauthorised use, loss, or disclosure of information and associated assets to the appropriate authority within the organisation.

### **Protection of Information and Associated Assets**

- Users shall apply appropriate security controls, such as passwords, encryption, and access controls, to safeguard information and associated assets.
- Users shall not install or use unauthorised software or hardware that may compromise the security of information and associated assets.
- Users shall promptly update and patch software and systems to mitigate known security vulnerabilities.
- Users shall not intentionally introduce viruses, malware, or other malicious code to information and associated assets.

### **Acceptable Use Guidelines**

- Users shall use email, internet, and other communication tools in accordance with ARO's policies and guidelines.
- Users shall not engage in activities that may harm ARO's reputation, such as spreading false or misleading information.
- Users shall not download, upload, or distribute copyrighted materials without proper authorisation or licensing.
- Users shall not engage in activities that may disrupt or degrade the performance of information and associated assets.
- Where assets need to be removed off-site, management approval for the removal of such assets must be obtained by raising a ticket on the relevant ITSM platform (i.e. BOLT, Autotask).

### **Return of Information Assets**

When an information asset is returned the following needs to be done:

- The associated entry on the Asset allocation form should be updated.
- Any data held on the asset that is relevant to ARO (or its Customers) needs to be transferred to suitable media within ARO. This must be recorded by creating a change request on the relevant ITSM platform (i.e. BOLT, Autotask).
- Any data on the asset should be cleaned (removed) before re-use in line with the Secure Disposal and Reuse of Equipment Policy.

### **Mobile and Remote Assets**

- Users shall adhere to ARO's mobile and remote access policies and guidelines.
- Users shall use secure connections and encryption when accessing information and associated assets remotely.
- Users shall not store sensitive or confidential information on personal devices without proper authorisation or encryption.

## **Security in Email Policy**

Email traffic makes up most of the information transfer within ARO and is accessible by all Employees so it requires special attention to ensure its secure use.

- Access to email accounts must not be shared - if a user is unable to access their own inbox due to holiday for instance, email systems should be configured to allow delegated access to authorised users only.
- When an Employee leaves their email account(s) must be disabled immediately.
- Emails containing sensitive information must not be sent or forwarded to anyone unless you know the recipient is authorised to view the information.
- You cannot guarantee who will view an email once sent so be conscious of including sensitive information in emails.
- It is easy to send emails to the wrong address - be extra vigilant of whom you are including.

- If necessary to include sensitive information in an email consider adding it to a secured attachment rather than in the body of the email, email must not be used to send passwords or other secrets in plain text.
- Users must not open email / open attachments / click on links in email / follow instructions received in email unless they are sure the origin and intent of the email is genuine. If suspicious, notify the IT team and wait for verification before doing anything else with the email.
- ARO email accounts must not be used for inappropriate, abusive, discriminatory, or other inappropriate communication.
- All messages must be relevant to ARO.

## Social Media Policy

It is the responsibility of all staff to protect the company's interests so they should not post anything on social media that would compromise our information security or our reputation.

- Confidential, sensitive or ARO proprietary information should never be posted on social media.
- Where you can be identified as a member of ARO, you must never criticise the company, our customers, suppliers, business associates, colleagues, or other professional acquaintances.
- Bullying, harassment, abusive language, and illegal activities will not be tolerated.
- You must never use company logos, trademarks or other corporate artwork in any personal posts or profiles unless authorised to do so, and only to promote the organisation.
- Users with access to ARO social media channels must not post personal content and must ensure that all posts are authorised, in the interests of the company and that all content is authorised to be made public, including content from third parties.

## Mobile Computing Policy

Anyone that uses mobile devices (including personal devices) to access ARO information must use extra care to keep them secure.

- Do not leave devices unattended in a public place.
- Do not assume even locked locations outside of your control are secure - hotel rooms are notoriously insecure for example.
- Do not leave devices in an unattended vehicle for extended periods of time.
- If a device is lost or stolen, even a personal device, you must alert IT immediately.
- The amount of data stored locally should be kept to an absolute minimum - access information from secure servers / cloud services where possible.
- Avoid using devices in open locations where you may be vulnerable to having them snatched.
- When not in use, keep devices in a pocket or zipped bag wherever possible.
- In the case of mobiles / tablets:
  - devices must be encrypted with a passcode, Face ID or similar,
  - devices should not be rooted or jailbroken,
  - devices should be kept up to date,
  - Android devices should have an antimalware app installed (many free ones are available), automatic screen lock settings should be set to 30 seconds.

## Installation of Software on Operational Systems Policy

- All new software must be risk assessed, and installation must be carried out by an authorised person.
- As of November 2024, any new software to be installed to operational systems must have been approved by appropriate stakeholders, through the formal Application Evaluation Process.
- All software must have a valid license and must not pose a risk to the security or operations of ARO. When no longer required, or supported, software must be removed from the device.

- Users are not permitted to install software on personal devices that directly connect to ARO's operational systems, with the exception of mobile applications where an appropriate user account already exists. Examples of approved mobile applications include Microsoft Office (Outlook, Teams, OneNote, Word, Excel etc), Microsoft Authenticator, BOB, PassPortal mobile application.

## Use of Privileged Utility Programs Policy

- Privileged Utility Programs (PUP) such as RMM and Endpoint management tools require an elevated level of privilege to perform their roles so use of these programs must be controlled.
- Access to such programs must be formally authorised.
- Any new PUPs must be formally authorised.
- Access to PUPs shall be strictly limited and must be protected with strong passwords and other conditional access mechanisms.
- All activity within PUPs must be logged for future review if necessary.
- Shared / generic user accounts must NOT be used to access or administer PUP's.

## Access Control Policies

### Access Control Policy

Access to our data, systems and facilities must be strictly controlled to protect our assets.

- User accounts must be set-up and revoked following strict guidelines, protected by appropriately strong passwords and other controls, and audited regularly.
- Access to information should be limited with stricter controls in place for users who need more privileged access.

### User Registration Policy

- User accounts must be requested through a ticket to IT / System Owner and must be authorised.
- Accounts must only be granted the minimum level of access required for their duties.
- Upon termination of employment user accounts should be disabled / deleted immediately.
- All System Owners must periodically review the user accounts in their systems to ensure they are still necessary and appropriate.

### Identity Management Policy

- User accounts (including system accounts) must be unique and NOT shared.
- Where possible MFA and other conditional access mechanisms must be used.
- Where users leave or change job role, access rights must be modified / deactivated immediately.
- All users are responsible for maintaining the confidentiality and security of their user credentials.
- Any suspected security incidents must be reported immediately.

### Password Management Policy

System Owners should read the full policy to ensure application of the appropriate password policy to their respective systems.

All users should follow the below guidance and rules for their credentials:

#### **Standard User Account Password Guidance & Usage Rules:**

- Use of a Password Management tool is strongly encouraged to store and create strong passwords

(i.e. PassPortal 'Personal Vault' where the user already has access).

- If creating a new password manually users should use 3 random, unrelated words together as a 'passphrase' – do NOT use words related to you personally, or the organisation, or that in any other way could be easily discoverable or guessed (i.e., pet names, sports clubs, addresses etc)
- Users must not share their password with anyone, including system Administrators or more senior members of the team.
- Users must not use the same password for any other accounts whether business or personal.
- Users must change their password promptly as soon as they become aware, or suspect, that it has been compromised. In either instance, the user must also notify the IT team and Information Security Manager of the known / suspected compromise who will then instigate an investigation.
- If a user becomes aware of another user's password by whatever means, they must notify the IT team and Information Security Manager immediately.
- Use of another individual's user account for any purpose, whether their password was disclosed in the process, is strictly prohibited.

#### **Administrator / Privileged Role User Account Password Guidance & Usage Rules:**

- Organisation Password Management tools (PassPortal, IT Glue) must be used to store and create strong passwords.
- Users must not share their password with anyone, including other system Administrators or more senior members of the team.
- Users must not use the same password for any other accounts whether business or personal.
- Users must change their password promptly as soon as they become aware, or suspect, that it has been compromised. In either instance, the user must also notify the IT team and Information Security Manager of the known / suspected compromise who will then instigate an investigation.
- If a user becomes aware of another user's password by whatever means, they must notify the IT team and Information Security Manager immediately.
- Use of another individual's user account for any purpose, whether their password was disclosed in the process, is strictly prohibited.

## **Secure Authentication Policy**

- Technology & procedures must be used to ensure users and devices are securely authenticated before they are granted access to ARO networks or systems.
- User accounts must remain unique to the person or device and be secured per the password policy.
- Single Sign On (SSO) functionality should be used where possible, as should VPNs where appropriate. Data centre networks which contain customer information must employ more stringent controls including enhanced MFA solutions.

## **Information Access Restriction Policy**

Procedures for granting, reviewing and revoking access rights to assets including systems, networks, databases, applications, and physical locations must be always followed.

- Users shall only be granted the minimum access necessary to perform their duties.
- Strong authentication methods must be used. Users must protect their account information, and only use their accounts as authorised.

- Higher privileged roles should be restricted to accounts separate of the users day-to-day account and not used for public facing activity such as email or web browsing.
- User access should be logged and monitored in all systems.
- Access to physical locations must follow these same principles: visitors / contractors should have their ID verified, be escorted when on the premises and may be subject to monitoring.

## Privileged Access Rights Policy

- Only the minimum access necessary to perform a user's duties should be granted, and only after appropriate authorisation.
- Privileged user accounts, such as admins, should be separate from normal user accounts, have strong password policies and be monitored closely.
- Suspicious activity related to privileged user accounts should be investigated with the highest priority following established incident response plans.

## Disabling Customer User Accounts Policy

The purpose of this policy is to define the principles and guidelines for consistently and securely handling the deactivation and reactivation of customer user accounts. It aims to ensure the confidentiality, integrity, and availability of sensitive information by strictly controlling and monitoring access to customer assets specifically when user accounts need to be deactivated or reactivated, or when sat in a state of deactivation. All personnel responsible for managing customer user accounts should see the full policy for more detail.

## Access to Program Source Code Policy

Where ARO maintains control of source code for programs it develops, access to that code must be strictly controlled to prevent unauthorised access. Access controls, physical & logical security, logging, and incident management should all be applied appropriate to the high level of risk associated with source code. All personnel involved in the development of systems, or responsible for the procurement of third-party development services, should see the full policy for more detail.

# Data Protection Policies

## Transparency & Privacy Policy

ARO is committed to ensuring the privacy and security of our Employees and our customers personal data. We are fully compliant with UK GDPR as incorporated in the Data Protection Act 2018 and other privacy regulations as relevant to our operations. See the full policy for details on how we process personal data and your rights as an individual over the information we process about you.

## GDPR Compliance Statement

This policy describes how we are compliant with UK GDPR and should be read in full in conjunction with our Transparency & Privacy Policy.

## Confidentiality Policy

ARO and its Employees process confidential information of various parties which must be protected. Confidentiality or non-disclosure agreements reflecting these needs shall be identified, documented, reviewed, and signed by personnel and other relevant parties including but not limited to:

- Contracts of employment.
- Partner / supplier / sub-contractor agreements.
- Customer contracts.

All non-disclosure agreements must be practical, with appropriate scope and specific purpose. All non-disclosure agreements must be reviewed by the Head of Legal before being presented to a Board representative for approval and signature.

## Information Labelling Policy

All information assets and documents (physical or electronic, emails, databases etc) owned or created by ARO must be labelled per their respective classification:

- Confidential (strictly need to know)
- Commercial in Confidence (need to know, but co-authored with Partners)
- Public (general release)
- Internal (ARO information not confidential but not for public release)

All information asset owners must ensure the data within their systems is labelled correctly. All Employees are responsible for adhering to this policy and appropriately labelling information they handle or create, even in the absence of automated labelling mechanisms.

## Information Handling Policy

All information assets should be handled according to their classification with appropriate controls for each level. Asset classification will be identified and documented in the Information Asset Register. All Employees are responsible for ensuring that documentation created is clearly labelled with the appropriate classification.

Special consideration must be given when handling Personally Identifiable Information (PII) within the organisation, ensuring we apply the principles of GDPR. See full policy for more detail.

Where SDCS process NHS Patient data, more stringent controls apply. See full policy for more detail.

## Logging Policy

Activity relevant to information security and quality within the organisation must be logged securely to allow us to identify and respond to security incidents, mitigate vulnerabilities and threats, support compliance with regulations and contracts and facilitates incident investigation. All systems should be configured to log activity including but not limited to:

- User authentication.
- Network traffic.
- Security events.
- Errors.
- Configuration changes.
- IP and location information.

In the absence of any other system or information specific requirements, logs should be retained for a minimum of 30 days. Where possible automatic alerts should be applied to log information based on agreed criteria and suspicious activity should be investigated immediately per the Security Incident Response Policy.

Logs and records shall also be maintained for non-system activity including:

- Customer complaints.
- Non-conformities and corrective actions.
- Changes and maintenance activity.
- Supplier management records.

- Risk mitigation.

## Protection of Records Policy

Records of our activities shall be kept for monitoring, evidential and continuous improvement purposes. Records must be clear, accurate, detailed, and maintained securely. All users are responsible for creating records in line with this policy and storing them in the correct place, and where appropriate are responsible for applying appropriate security controls to those records (for instance by encrypting individual files, applying strong access controls to their systems, or encrypting storage media in their control). As well as applying logical controls to electronic records, physical records should be stored in secure locations and transferred through secure, documented procedures.

## Clear Desk & Screen Policy

- Desks should be kept clear of sensitive information / equipment whenever possible.
- When not in use documents and equipment should be stored in a secure location.
- Sensitive documents should not be kept on desks longer than necessary nor be left unattended.
- All workstations should be locked with the Ctrl + Alt + Del > Lock function when left unattended.
- If leaving a workstation unattended for an extended period, log out of systems or even switch the device off.
- When at your desk be conscious who can see information on your desk or screen - other staff, and particularly visitors, may not be authorised to see that information.
- If in doubt, close / reduce active windows containing sensitive information and turn documents face-down to mask the information.

## Information Backup Policy

Critical information and systems must be backed up to protect the availability of assets in the event of loss, hardware failure, attacks, or other unforeseen events, and ensure business continuity in the event of a disaster. Information Owners, System Owners and IT staff are responsible for adopting mechanisms to securely backup assets on an appropriate schedule, apply appropriate access controls and conduct regular testing to ensure the integrity and recoverability of the assets. Dependent upon the nature of the asset, backups may be conducted on-site, off-site, to public cloud services or a combination of all.

## Use of Cryptography Policy

- Sensitive data, whether in databases, file systems, or any other storage media **MUST** be encrypted when at rest using up-to-date, approved encryption methods & protocols.
- Sensitive data must only ever be transmitted by secure methods such as encrypted, digitally signed email and cloud sharing tools.
- Where we are generating cryptographic keys there are specific considerations for generation, distribution, storage, rotation and sharing of those keys.
- Algorithms, key lengths, and transmission protocols must be up-to-date and approved (we recommend following NHS England & NCSC guidance).

See full policy for more detail.

## Customer Off-boarding Policy

We are responsible for looking after Customer assets including information, privileged access mechanisms, intellectual property (such a network / configuration information & procedures) and hardware which may be hosted in ARO premises. When a Customer contract ends these assets must be returned or destroyed securely. Such assets must be identified & assessed, and a suitable off-boarding plan agreed with the Customer and/or their new service provider (if relevant). During off-boarding Customer access rights to ARO systems / information should be removed and Customer information held

on ARO systems should be destroyed when it is no longer required. All off-boarding activity must be recorded in the appropriate ITSM (BOLT, Autotask) and or project planning documentation.

## Data Destruction Policy

When no longer required the data within ARO, both our own and our customers, must be destroyed securely in line with legal and regulatory requirements:

- Paper documents and physical media containing sensitive information must be shredded, ideally using an approved shredding services partner.
- Information stored electronically should be deleted from the file system / database as a minimum and ideally overwritten where possible.
- Within our own data centres, information should be purged by degaussing the original media, and/or physically shredding the storage media, as is appropriate to the level of sensitivity and risk of the information in question.
- Records of data destruction activities, including certificates of destruction, should be maintained for auditing and compliance purposes.

## Secure Disposal & Reuse of Equipment Policy

Any device that stores data (inc. workstations, servers, storage media, printers, and photocopiers) must be handled securely when being disposed of or reused (either internally or when passed to another organisation). All devices must have their storage cleaned and purged of all information, and disposal should be conducted by an approved supplier to ensure compliance with all WEEE regulations. All activity regarding the disposal and reuse of equipment should be conducted by competent persons and documented, included appropriate proof of destruction / sanitisation (certificates, toolset logs etc).

## Securing Rooms, Offices & Facilities Policy

- All ARO facilities must be secured to prevent unauthorised access. Controls should include:
- Access control (i.e. access cards, biometric readers, keys) granted on a least privilege basis.
  - CCTV
  - Security alarms
  - Exterior fencing
  - Security personnel etc
- Critical infrastructure, assets and physical data should all be stored in secure locations such as locked offices, vaults or filing cabinets.
- All visitors must sign in, wear ID badges and be escorted in secure / restricted areas.
- All staff should ensure their screens and desks are kept clear of sensitive information when left unattended and take steps to prevent information being viewed by unauthorised persons when they are using it.
- Data Centres must apply additional security measures commensurate to the elevated risk.
- Those staff based at the Liverpool Offices should read the full policy for site specific obligations.

## Physical Security Monitoring Policy

As well as protecting our facilities with controls such as CCTV and alarms, it is important that these controls be monitored to ensure their effectiveness:

- Alarms should be monitored in real time to allow for immediate response if required.
- CCTV and access control systems must retain activity records for appropriate periods to allow for review in the event of an incident, or to identify suspicious activity.
- All controls should be audited at least annually to ensure compliance with ARO policies and identify any gaps or weaknesses which require remediation.

## Protection Against Physical & Environmental Threats Policy

We must also take steps to protect our assets from physical threats such as fire, flood, extreme weather, power failures / spikes, extreme temperatures / humidity which could all damage or destroy those assets and information. Appropriate controls must be put in place appropriate to the level of risk. Controls include but are not limited to:

- Monitoring equipment (fire alarm, temperature sensors).
- Fire suppression equipment.
- Appropriate siting of infrastructure away from water or magnetic interference.
- Air conditioning.

All controls should be reviewed for effectiveness on a regular basis and systems must be maintained to ensure uninterrupted operations.

## Supporting Utilities Policy

To support our Protection Against Physical & Environmental Threats Policy will require the use of utilities such as electricity, gas, water, cooling, and telecommunications. It is important that these utilities are controlled to ensure continuous protection:

- Contracts should be maintained with reputable, reliable providers, containing SLAs appropriate to the criticality of the service.
- Where critical infrastructure is located at a site, a minimum of an Uninterruptible Power Supply (UPS) should be installed and tested regularly.
- Datacentres should also install secondary power circuits or back-up generators.
- Data centres and other critical locations should install additional back-up broadband / ethernet connections, including diversely routed connections where appropriate to the criticality.

## Working in Secure Areas Policy

ARO implements secure areas within its facilities for sensitive / critical business operations, including the siting of critical infrastructure (i.e. server rooms) and the storage of sensitive information assets (i.e. locked filing cabinets / storage cupboards). Data centres operated by ARO will be considered secure areas in their entirety. Enhanced controls must be adopted in secure areas:

- secure areas must always be locked,
- photography / videography in secure areas is prohibited unless authorised,
- visitors within secure areas must be escorted or monitored,
- access to secure areas must be strictly limited,
- access to secure areas should be controlled through physical methods appropriate to the risk such as keys, smart cards, biometric systems.
- Data centres must be monitored by CCTV throughout 24/7.
- Any security incidents suspected within secure areas must be reported immediately to management or the Head of Information Security.

## Privacy by Design Policy

We must consider data protection and privacy issues as part of the design and implementation of all systems, services, products, and practices. We must ensure that personal data is secure and uphold the rights of individuals over their data in line with GDPR. We must also ensure that these high standards of data protection will be upheld by any third-party services or sub-processors that we employ.

## Data Masking Policy

When using data for non-production purposes such as development, testing and staging, data masking techniques should be used wherever possible to ensure the confidentiality of personal and other sensitive information whilst retaining the usability of the data. It is the responsibility of those acquiring

data sets for non-production use to ensure the data is masked in a secure environment before being transferred. Various data masking techniques such as nulling and substitution can be recommended to be used. ARO personnel responsible for processing these data sets should see the full policy for more detail.

## Information Exchange Policy

When any information is exchanged between ARO, and other organisations adequate controls must be applied to protect from loss, modification, or misuse of that information:

- Information must be classified and handled appropriate to that classification.
- Agreements with relevant third parties must contain clauses regarding information exchange.
- All information must be protected in transit and must never be transferred by insecure methods.

Additional protections and authorisations are required for the exchange of any PII. PPI must not be sent outside of the EEA unless the recipient country has adequate levels of protection for information and the rights of individuals.

## Data Leakage Prevention Policy

Within its IMS ARO employs several measures to prevent unauthorised disclosure or loss of sensitive information including information classification & labelling, access controls, encryption, network segmentation, endpoint security, Employee training and incident response planning.

## Biometric Policy

To enhance our security posture, we may employ systems that collect and process individuals' biometric information (i.e. fingerprints). We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and rights of individuals are protected:

- A Data Protection Impact Assessment will be carried out for all biometric processing activities and made available upon request.
- Biometric data cannot and will not be collected or processed without consent.
- As a Special Category of PII as defined by GDPR individuals have the right to object to the use of their biometric data.
- In that instance ARO will implement alternative solutions.

All individuals considering the use of their biometric data within ARO should read the full policy in conjunction with the Transparency & Privacy Policy and GDPR Compliance Statement.

## People Security Policies

### Termination of Employment Policy

When an Employee leaves ARO proper exit procedures must be followed to prevent unauthorised access to sensitive information, assets and systems. HR will initiate and coordinate the leavers process:

- Working with the IT team and system owners, access rights, system accounts and any other privileges will be removed / disabled with immediate effect.
- Working with IT team, department heads and line managers, HR will coordinate the safe return of any assets in the departing Employee's possession including hardware, keys, other access devices, documentation.
- Department heads / Line managers must ensure that HR are notified of impending leavers as soon as possible.

- At the end of their employment all personnel are obligated to return company assets in a safe and secure fashion and uphold confidentiality and non-disclosure requirements per their contract of employment.

## Segregation of Duties Policy

ARO has implemented Role-based Access Control (RBAC) mechanisms to define and enforce access rights and privileges based on job functions and responsibilities. RBAC shall be designed to ensure that no individual has access to all necessary privileges to compromise the confidentiality, integrity, or availability of critical information assets or business processes. Critical business processes that require segregation of duties shall be identified and documented. Formal processes for authorising access to assets, processes and privilege shall be established with all such requests recorded.

## Information Security in Project Management Policy

We must ensure that appropriate controls are in place to safeguard our, and our customers, information assets throughout the project lifecycle. Project Managers are responsible for ensuring information security risks are identified, assessed, and mitigated throughout the project lifecycle. Information security plans must be included in project planning, appropriate access controls adopted, and incidents responded to in a timely fashion following established plans.

## Incident Response / Business Continuity Policies

### Reporting Security Incidents Policy

- **Security Event:** an occurrence or change that may indicate a security problem.
- **Security Incident:** an event that is confirmed to pose a threat to our security.
- **Security Weakness:** a flaw in a system or process that could be exploited to compromise it.

All personnel are required to report all Events, Incidents or Weaknesses they become aware of immediately via BOLT. Reports can also be raised directly to the Head of Information Security or members of the Security Advisory Board.

### Security Incident Response Policy

A rapid response to incidents that threaten the security of ARO (or customer) information assets is required to protect those assets. We have established procedures for the effective management of security incidents. The Incident Management procedures for ARO are detailed in the ITSM Policy & Process Guide document (Service / Operational incidents) and Critical Security Incident Response Plan documents, to be read alongside the Reporting Security Incidents Policy. These procedures and plans must be followed and documented for all incidents.

### Data Breach Policy

If a breach of personal data does occur, we have an obligation to ensure that the correct procedures, controls, and measures are in place. This includes our regulatory and contractual obligations to notify the subject(s) of the data breach and the relevant authorities. If during the implementation of the Critical Security Incident Response Plan a breach of personal data has been confirmed, it must be reported to the DPO (or suitable deputy at the time) who will invoke the procedures in this document working alongside the incident response team. All personnel who may act as an Incident Owner for the CSIRP should familiarise themselves with the full policy.

## Learning from Security Incidents Policy

All Security Incidents must be investigated and remediated in line with our Security Incident Response plans, including post-incident steps to perform root cause analysis from which identified changes should be made to prevent further occurrence. All incidents shall be comprehensively documented in our standard ITSM platforms (Autotask, BOLT) to allow for further analysis and identification of problem areas and for appropriate improvement plans to be devised.

## Redundancy of Information Processing Facilities Policy

It is vital that critical systems are built and configured with redundancy in mind to minimise the risk of service disruptions and data loss. Measures should include:

- Backing up and replicating data to redundant locations.
- Dual network paths and redundant switches / routers within networks.
- Servers to be configured in redundant clusters.
- Secondary power supplies to be installed at appropriate locations.
- Critical applications to be designed with redundancy and failover mechanisms built in.

Capacity of our systems must also be maintained to ensure ongoing availability. System administrators / Owners should see full policy for more detail.

## Information Security During Disruption Policy

We have applied measures to maintain the security of our information assets during disruptions including natural disasters, cyber-attacks, infrastructure failures and other emergencies. Measures include proactively identifying potential disruptions, establishing incident response, business continuity and disaster recovery plans, establishing alternative business processes and clear communications channels with stakeholders. It is crucial that all personnel comply with all such measures during a disruption. ARO will conduct post incident reviews after disruptions to identify lessons learned and areas for improvement.

## Infrastructure Security Policies

### Change Management Policy

Change Management is an essential control element that enables prioritisation and surety of deployment success. Change Management must be applied in a manner that balances the need for control with the need for agility. It is the responsibility of users when creating, modifying, or removing any information asset, service, or process that belongs to ARO or one of its supported customers to ensure that the Change Management process is followed as outlined in the ITSM Policy & Process Guide. All changes must be risk assessed, reviewed, approved, and documented per the process. In rare cases, minor changes may be carried out without a formal change request if authorised by the appropriate Information Asset Owner. A log of any such changes must still be kept.

### Configuration Management Policy

Hardware, software and/or network components (collectively 'Configuration Items' / 'CI') should be identified, categorised, and documented in an appropriate system (i.e. SharePoint, BOLT, IT Glue, PassPortal etc) by relevant System Owners / Service Owners / IT team(s). Changes to CI must be formally managed and documented including risk assessment, approval, and verification of the changes. This policy should be read in conjunction with the Change Management policy and associated procedures.

## Capacity Management Policy

Capacity management is essential to ensure that no business or production IT system suffers a reduction in performance or loss of service due to a lack of available resources. To this end:

- No components should be added to systems without proper planning and consultation.
- Measures such as load-balancing or automatic failovers should be implemented on systems where capacity limitations are a risk.
- Additional capacity should be fitted to existing systems where possible / necessary.
- Where failure of a component would affect availability of critical systems, spare components or redundant systems should be provided.

System owners should ensure appropriate monitoring is in place to alert to impending capacity issues, and that systems are maintained to a high standard in line with vendor recommendations / best practice.

Note: Cloud based SaaS systems are out of scope of this policy as responsibility for capacity and related SLA's falls to the vendor.

## Security of Network Services Policy

- Access to ARO networks shall be protected in line with our Access Control policies and employing the use of firewalls, NAC and IDS/IPS systems.
- Network segmentation shall be employed to isolate sensitive data and critical systems.
- Where possible internal networks should be segmented by functional unit / geographical location / operational unit, for instance with the use of VLANs or other technologies.
- Publicly accessible services should be segregated in a 'Demilitarised Zone' (DMZ).
- Visitors / Guests should only be provided access to separate network(s) dedicated to public internet access.
- Wireless networks should be segregated from wired networks.
- Users must not attempt to bypass security measures, disrupt, or damage the network or use the networks for personal or inappropriate purposes.
- Remote access to our networks shall be granted only through approved methods.
- Data transmitted on our networks should be encrypted and network activity should be logged.
- Critical systems should be backed up, and backups tested, regularly.
- Network devices should be security patched up to date and default device configurations must be changed before deployment.

## Separation of Environments Policy

- Development, test, and production environments must be separated to prevent unauthorised access and avoid potential conflicts that may impact system stability and data integrity.
- Development and test environments must be subject to the same controls applicable to production including access control, change management, monitoring, and auditing.
- Incident Response, Disaster Recovery and Business Continuity plans should also explicitly account for development and test environments.
- Access Control to development and test environments should be based on the principle of least privilege and, by their nature, should not necessarily replicate that of production environments.
- Unless necessary, and only if authorised, production environments should NOT be used for development or testing.
- The use of data for development and test is governed in the Test Information Policy.

## Virtual Private Network Policy

- Remote access to ARO networks shall be allowed only with the use of approved VPN mechanisms unless otherwise approved.

- Access to VPN must be strictly controlled following documented approval procedures.
- Detailed controls must be applied to VPNs that are connecting to ARO networks including but not limited to; encryption, strong passwords, MFA, device tokens / pre-shared keys, traffic management, connection time-outs.
- All VPN traffic and activity must be monitored and logged.
- Specific considerations must be given to site-to-site VPNs, as a part of the risk assessment process.
- It is the responsibility of users with VPN access to ensure no unauthorised users are allowed access to ARO networks, and that their credentials and other secret information remain secret.

See full Policy document for detailed VPN requirements.

## Information Security for the Use of Cloud Services Policy

The use of cloud services must be done securely and responsibly to protect our and our customers information:

- Cloud services and their respective vendors must be formally assessed and approved before use, including full risk assessment.
- Information stored in cloud services must be classified and handled appropriately (see Information Classification Register).
- Information in cloud services must be encrypted both at rest and in transit with approved protocols and access should be controlled on a need-to-know basis in line with our Access Control policies.
- Cloud services should be contractually obliged to adhere to our information security requirements, and all activity should be logged with any suspicious activity investigated and responded to immediately.

## Web Filtering Policy

Where possible ARO will implement technical solutions to filter web site access such as hardware firewalls, software firewalls and approved web browsers with inbuilt protections. We acknowledge that we cannot be too restrictive, particularly in supporting our extensive customer base. As such all ARO users are expected to exercise extreme caution when visiting websites never knowingly visiting sites that are known to distribute malware, involve phishing attacks or similar, or host illegal or inappropriate content.

## Protection Against Malware Policy

To protect our assets from malware we must:

- Prohibit the installation and use of software not formally approved.
- Patch our systems and assets in a timely fashion.
- Mandate the use of anti-virus / EDR software on all operational systems unless otherwise approved by the Head of Information Security.
- Restrict the use of external media and mandate it is scanned for malware when it is used.
- Mandate that all downloaded files be scanned for malware before opening.
- Standard user accounts used for email, web browsing etc shall NOT be granted elevated / administrator privileges.
- All users must remain vigilant to phishing attacks and NOT open files or click on URLs unless they know they are legitimate.
- Where anti-malware tools are used within ARO appropriate alerts must be configured to highlight issues related to the tool to facilitate swift remediation.

## Vulnerability Management Policy

We shall employ methods to identify vulnerabilities in our systems including system monitors, log reviews, vulnerability scanning and threat intelligence from multiple sources including system vendor updates. As vulnerabilities are identified system owners / threat intelligence stakeholders shall assess and take appropriate action to remediate as soon as is practically possible. Assessment and response should consider the criticality of the system, the risk severity of the vulnerability and the operational impact of mitigation (which may include system patches, workarounds, isolation / disabling of the affected system). To proactively combat vulnerabilities system updates and patches should be applied as soon as is practically possible. In line with Cyber Essentials Plus guidelines, security patches should be applied within 14 days or release.

## Virtual Machine Hardening Policy

Best practices must be employed to apply recognised hardening techniques when configuring virtual machines (also physical machines and devices where possible). Minimum hardening techniques include:

- Using best-practise baseline configuration templates for machine deployments only allowing necessary ports and protocols.
- Ensuring a secure network environment for machines (see Security of Network Services Policy).
- Removing unnecessary / default system and user accounts.
- Regularly applying security patches.
- Implementing secure authentication mechanisms such as MFA.
- Enabling audit logging.
- Implementing secure backup and disaster recovery mechanisms.
- Performing regular vulnerability assessments.

## Management of Storage Media Policy

All storage media, including hard drives, USB drives, DVD's, network storage etc, must be handled properly to ensure its security:

- Media should be labelled with appropriate identification and classification to ensure proper handling and tracking.
- Media should be stored securely and protected from environmental factors such as temperature, humidity, and magnetic interference.
- Information should not be deleted from media without permission of the Information Owner.
- At the end of its useful life, storage media must be disposed of securely per the Secure Disposal and Reuse of Equipment Policy.
- Sensitive data on storage media must be encrypted at rest.
- When required storage media should be transported using secure, approved methods only.

## Clock Synchronisation Policy

Without synchronised time, accurately correlating log files between our devices is impossible. ARO systems must be synchronised to a recognised time source such as Microsoft NTP (time.windows.com) or Google Public NTP (time.google.com). Where we use Public Cloud services, we acknowledge that time synchronisation is controlled by the provider. All servers residing on networks maintained by ARO should be set to the correct time using an approved NTP source. To try and ensure parity between networks, including those hosted in Microsoft Azure platform the preferred NTP source is Microsoft NTP wherever possible. When configuring time synchronisation on a new network see the full policy for more details.

## Monitoring Activities Policy

Best practices must be employed to monitor our information assets to identify vulnerabilities, threats, and risks, respond to security incidents in a timely manner, measure the effectiveness of our existing

security controls and improve the overall security posture of the organisation. System Owners, System Administrators, and IT staff are all responsible for configuring systems to generate logs and implementing other approved monitoring solutions as appropriate. As well as monitoring of activity logs other activities shall include vulnerability scanning, penetration testing, incident monitoring and response and internal / external compliance audits. Working with these stakeholders and monitoring mechanisms the Head of Information Security shall be responsible for reporting on Key Risk Indicators to senior management.

## Equipment Siting Policy

Equipment used to process information should be located where conditions can be met for proper operation, minimal disruption, and maximum security:

- Equipment should be sited so that access can be restricted appropriately, with servers confined to separate secure rooms for example.
- Secure rooms should be kept locked and any third-party access to secure spaces should be escorted or monitored.
- Outside of secure spaces equipment should be sited to prevent unauthorised viewing of information on screens wherever possible.
- Where not practical to do so more emphasis must be given to the Clear Desk and Screen Policy.
- Equipment should be sited to allow for protection from physical and environment threats per the Protection against Physical and Environmental Threats Policy.
- Equipment not owned and controlled by ARO, such as customer assets, should be clearly segregated from those owned by ARO.

## Cabling Security Policy

Network cabling can still present a risk to the availability and confidentiality of the information we hold:

- Damage or interference to cabling can prevent transmission, restricting access to critical data.
- Unprotected cables can be attacked by cyber criminals who can gain access to our networks.

To prevent such occurrences as much as possible controls must be applied to protect our cabling infrastructure including but not limited to:

- External cables should enter premises underground.
- Internal cabling should be protected in trunking, trays, cable ladders and plenum spaces.
- Data cables should be segregated from power cables to prevent magnetic interference.
- Ideally only shielded cable should be used.

Due to the elevated risk, additional controls should be applied in ARO data centres including:

- Secured cabling rooms.
- Regular inspections of cables and junction boxes.
- Installation of redundant cabling runs.

## Supplier Management Policies

### Procurement Policy

Procurement processes must be implemented that are effective, efficient and comply with legal and regulatory requirements (inc. ISO 9001):

- Procurement plans should be developed to ensure a systematic approach.
- Suppliers must be evaluated for their ability to meet our requirements before being approved.
- Purchase orders and contracts should be used to document the procurement process and terms must include provisions for quality, payment terms, warranties, and information security.
- The performance of all suppliers should be monitored and reviewed on a regular basis.

- Non-conformities, disputes and performance issues should be appropriately addressed and resolved asap, including as an extreme, termination of the supplier relationships and cease of all procurement activity with that supplier.

## Information Security in Supplier Agreements Policy

When forming an agreement with a new supplier, the roles, responsibilities, and obligations regarding Information Security must be clear and match the requirements of management system. Topics that must be addressed include:

- Confidentiality & non-disclosure.
- Data Protection and Privacy of personal information.
- Minimum security controls expected from the supplier.
- Incident response procedures and obligations for the supplier.
- Responsibilities regarding any subcontractors or other third parties the supplier will be using.
- The supplier's liability for security issues.

Supplier agreements must only be entered into by authorised ARO representatives and new suppliers must go through a thorough assessment process before they will be authorised.

## Information Security in Supplier Relationships Policy / Information Security in the ICT Supply Chain Policy

It is essential to maintain a robust information security framework throughout our supply chain. Suppliers will only be approved following a thorough assessment process, and contracts must contain obligations as laid out above. Any ARO personnel responsible for onboarding a new supplier or for managing vendor relationships in-line should read the full policy for more detail.

## Legal Policies

### Compliance with Legal Requirements Policy

It is ARO's policy to ensure that it avoids, and prevents, breaches of all applicable laws and statutory, regulatory, or contractual obligations in relation to information security. ARO maintains a register of all relevant legislation. Changes that might impact upon the organisation are updated on the legal register, reviewed and actions taken to maintain compliance. As supported by appropriate policies ARO maintains strict controls to ensure compliance with intellectual property rights, safeguarding our organisational records, data protection and privacy laws and the collection of evidence during security incidents. It is the responsibility of all Employees to always comply with these policies and procedures.

### Intellectual Property Rights Policy

ARO is committed to protecting its intellectual property rights and the rights of others:

- Intellectual Property created by any Employee of ARO in the course of their duties for the organisation shall automatically belong to ARO to the fullest extent permitted by law.
- When creating materials for use by ARO it is not permitted to include third-party properties including trademarks, logos, names without the express permission of the rights holder.
- Where third party intellectual property is in use, credit should be given to the rights holder wherever possible unless deemed unnecessary by the rights holder.
- Intellectual property rights are a complex legal matter so anyone with doubts / queries about their use of IP should first refer to the full policy for more detail.

Further guidance should then be sought from the Head of Marketing and/or Head of Legal.

## Software Development Policies

### Secure System Development & Engineering Principles

ARO personnel and contractors who are involved in the development of systems have a responsibility to ensure they use secure system architecture and engineering practices to protect the information that will be processed by those systems. Secure development principles include defence-in-depth, least privilege, separation of duties, security defaults, secure coding best practice, vulnerability management, security testing. All personnel involved in the development of systems, or responsible for the procurement of third-party development services, should see the full policy for more detail.

### Secure Development Lifecycle Policy

ARO personnel and contractors who are involved in the development of systems have a responsibility to ensure they follow a consistent, secure development lifecycle (SDLC) to ensure security considerations are embedded into all phases. All personnel involved in the development of systems, or responsible for the procurement of third-party development services, should see the full policy for more detail.

### Test Information Policy

To effectively test our systems, it is often required to use extracts / copies of data relevant to the system being tested. When data is being extracted for testing purposes, it is essential that the security of that data be maintained to the same standards required of the live system and its classification:

- Test information should be selected as much for the ability to ensure confidentiality as for reliability of test results.
- Where possible data should be masked / anonymised to ensure privacy in non-production environments and should only be used for the authorised testing purposes.
- Test data should not be shared without appropriate controls and contracts in place.
- Test environments and test data should be always isolated from live environments.
- Test data should only be retained while testing after which it must be securely destroyed.

### Outsourced System Development Policy

When outsourcing software development, strict controls must be put in place to ensure the quality and security of planned systems as well as the confidentiality, integrity and availability of information used during the development project. ARO must carefully consider the scope & requirements of the project, legal & compliance obligations, security, and confidentiality. The project must be risk assessed and vendor approved following a thorough assessment. Vendors must follow strict data handling procedures and comply with our data protection and system development policies (particularly the Test Information Policy). All personnel involved in the development of systems, or responsible for the procurement of third-party development services, should see the full policy for more detail.