

Security Incident Response Policy

(ISO 27001:2022 Organisational Controls – Clause 5.24 /
DSPT)

Author	Greg Nott
Version	3.0
Date Created	19/06/2023
Last Update Date	21/10/2025
Document Control	Released
Document ID	230619-IMS-POL-SecurityIncidentResponse-V3
Security Classification	Public

Table of Contents

Security Incident Response Policy	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Purpose	4
Policy.....	4
Data Centre Incident Response Policy	4
Categories	5
Severity and Criticality.....	6
Security Team.....	6
Objectives of the Security Team	6
Responsibilities of the Security Team	6
Key Components of Critical Security Incident Response Protocol	7
Required Documentation for Critical Incident Response Meetings.....	8
Post-Incident Review (PIR)	8
Just Culture	8
Appendix A – Incident Sensitivity and Criticality Levels.....	10
Appendix B – Incident Containment Activities.....	13
Appendix C – Corrective Measures.....	14

Approval

Author	Issue	Approved By	Date
Greg Nott	1.0	Simon Naylor	15-Aug-23
Greg Nott	2.0	Paul Langan	16-May-24
Greg Nott	3.0	Greg Nott	21-Oct-25

Review

Reviewer	Review Criteria	Issue	Date
Paul Langan	ISO 27001:2022	1.0	14-Aug-23
Paul Langan	Review & Rebrand	2.0	16-May-24
Greg Nott	Annual Review	3.0	21-Oct-25

Change History

Author	Change	Issue	Date
Greg Nott	Creation	1.0	19-Jun-23
Greg Nott	Review & Rebrand	2.0	16-May-24

Associated Documents

Document	Version
Reporting Security Incidents Policy	3.0
ITSM Policy & Process Guide	1.0
Critical Security Incident Response Plan(s)	All
NHS Just Culture Guide	n/a

Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and describes the Security Incident Response Policy adopted by ARO.

- ISO 27001:2022 – Information Security Management Systems
 - ISO 27017:2015 – Code of Practice for Cloud Services
 - ISO 27018:2020 – Code of Practice of Personally Identifiable Information (PII)
- ISO 9001:2015 – Quality Management System
- DSPT (Data Security and Protection Toolkit) for the NHS.
- Cyber Essentials Plus

This policy applies to all employees, contractors, and any third-party entities with access to ARO's systems, networks, and data.

Purpose

This document describes the policy regarding the response to a security incident.

A rapid response to incidents that threaten the confidentiality, integrity, and availability (CIA) of ARO information assets, information systems and the networks that deliver the information is required to protect those assets. Without a rapid response, those assets could be compromised, and ARO could be in breach of UK Legislation, and our own stated policies, there is also the potential of breaching the trust of our customers.

Policy

The organisation has established procedures for the effective management of security incidents. The purpose of these procedures is to return to a secure state as quickly as possible whilst minimising the adverse impact on the organisation.

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 cover both internal and customer related incidents & events and will be communicated to all employees.

All ARO staff involved (or associated with) a security event or incident will be treated in a consistent, constructive and fair way.

Due to the nature of the operations conducted by the Liverpool Data Centre, the following procedures have been established to manage incidents impacting the Data Centre specifically.

Only employees working within the Liverpool Data Centre should familiarise themselves the following policy & procedures.

Data Centre Incident Response Policy

This policy underlies the establishment and ongoing deployment of a trained incident response team (Security Team), formed with the purpose of managing information security incidents at the Liverpool Data Centre. This effort is being taken to improve the response time to incidents, to provide consistent response, and improve incident reporting. The purpose of the Information Security Incident Response Procedure is to establish procedures in accordance with applicable legal and regulatory requirements and

ARO policy to address instances of unauthorised access to or disclosure of both the organisations and its customers information, to be known as an Incident.

This policy specifically excludes the following:

- Non-electronic information including paper mail.
- Fax and Copier
- Physical Security
- Business Continuity Planning (covered by a different set of policies)

The primary emphasis of the guidelines described within this policy is the return to a normal (secure) state as quickly as possible, whilst minimising the adverse impact on the organisation. The capture and preservation of incident relevant data (e.g., network flows, data on drives, access logs, etc.) is performed primarily for the purpose of problem determination and resolution, and methods currently employed are suitable for that purpose. It is understood and accepted that strict forensic measures are not used in the data capture and retention. Forensic measures will be determined on a case-by-case basis.

The Security Team will monitor and co-ordinate all activities arising out of the security incident and will communicate to all interested parties in a timely manner to ensure accurate assessments and avoid efforts that may be duplicated or at cross-purposes.

The Security Team will also provide consistent and timely response to the organisations customers and ensure that sensitive information is handled appropriately. This document provides the guidelines needed for the Security Team to classify the case category, criticality level, and sensitivity level for each Security Team case.

Consistent case classification is required for the Security Team to provide accurate reporting to management on a regular basis. In addition, the classifications will provide Security Team with proper case handling procedures.

Categories

For the purposes of this protocol, incidents are categorised as 'Unauthorised Access' or 'Unauthorised Acquisition' and can be recognised by associated characteristics.

Unauthorised Access

The unauthorised access to or disclosure of ARO (or our customers) information through network and/or computing related infrastructure, or misuse of such infrastructure, to include access to related components (e.g., network, server, workstation, router, security system, system, application, data, etc.).

Characteristics of security incidents where unauthorised access might have occurred may include but are not limited to:

- Evidence (e-mail, system log) of disclosure of sensitive data
- Anomalous traffic to or from the suspected target
- Unexpected changes in resource usage
- Increased response time
- System slowdown or failure
- Changes in default or user-defined settings
- Unexplained or unexpected use of system resources
- Unusual activities appearing in system or audit logs
- Changes to or appearance of new system files
- New folders, files, programs, or executables
- Users lock out

- Appliance or equipment failure
- Unexpected enabling or activation of services or ports
- Protective mechanisms disabled (security system, anti-virus)
- Data loss and corruption.

Unauthorised Acquisition

The unauthorised physical access to, disclosure or acquisition of assets containing or providing access to ARO (or customer) information (e.g., removable drives or media, hardcopy, file or document storage, appliance hardware, etc.).

Characteristics of security incidents where unauthorised acquisition might have occurred may include but are not limited to:

- Theft of computer equipment where sensitive data is stored
- Loss of storage media (removable drive, CD-ROM, DVD, flash drive, magnetic tape)
- Illegal entry (burglary)
- Suspicious or foreign hardware is connected to the network
- Normally secured storage areas found unsecured
- Broken or non-functioning locking mechanisms
- Presence of unauthorised personnel in secured areas
- Disabled security cameras or devices

Severity and Criticality

Incidents are further delineated by the actual and potential impact on the organisation. For additional information on severity assignments and associated symptoms, see “Appendix-A Incident Severity and Criticality Levels.” The primary focus of this policy is the handling of Severity 1 incidents.

Security Team

The Incident Response Team (Security Team) comprises of the individuals listed below and is charged to manage and resolve any security incident(s) that may arise.

- Technical Director – Security Team Lead
- Projects Director
- IMS Manager
- Network Security Manager
- Business Development Director
- Contract Manager

Objectives of the Security Team

The Security Team’s objective is to:

- Coordinate and oversee the response to Incidents in accordance with the requirements of UK Legislation & ARO policies.
- Minimise the potential negative impact to the organisation, customers, and 3rd Parties because of such Incidents.
- Where appropriate, inform the affected customers and 3rd Parties of action that is recommended or required on their behalf
- Restore services to a normal and secure state of operation.
- Provide clear and timely communication to all interested parties.
-

Responsibilities of the Security Team

To ensure an appropriate and timely execution of this protocol, the Security Team lead is required to:

- Confirm the occurrence of an Information Security Incident requiring the execution of this protocol.
- Confirmation activities include but are not limited to:
 - Examination or analysis of anomalies or untoward events
 - Review of system logs or audit records
 - Direct conversation with Customer, 3rd Party, Service Desk, IS personnel,
 - “On call” engineer, Security Team members or others having information about the event
 - Collection of any evidence supportive of the event
 - Supervise and direct the consistent, timely, and appropriate response to an Information Security Incident
 - Provide appropriate communication to parties having a personal stake in the incident.
 - Offer support to the Customer or 3rd Party as appropriate until the Incident is resolved.
 - Conduct a Post-Incident Review (PIR).
 - Maintain the procedures contained in this document.

Key Components of Critical Security Incident Response Protocol

The Critical Security Incident Response Protocol consists of five key components:

- Assessment
- Notification/Communication
- Containment,
- Corrective Measures
- Closure

Assessment

The Security Team Lead or Security Team IM will determine the category and severity of the Incident and undertake discussions and activities to best determine the next best course of action, i.e., decide if protocol execution is required.

Notification/Communication

Designated persons will take action to notify the appropriate internal and external parties, as necessary.

Containment

The Security Team will determine and cause to be executed the appropriate activities and processes required to quickly contain and minimise the immediate impact to ARO, our customers and 3rd Parties.

Recommended activities addressing Unauthorised Access and Unauthorised Acquisition are described in Appendix B “Incident Containment Activities.”

Containment activities are designed with the primary objectives of:

- Counteract the immediate threat.
- Prevent propagation or expansion of the incident.
- Minimise actual and potential damage.
- Restrict knowledge of the incident to authorised personnel.
- Preserve information relevant to the incident.

Corrective Measures

The Security Team will determine and cause to be executed the appropriate activities and processes required to quickly restore circumstances to a normal (secure) state. Recommended activities addressing Unauthorised Access and Unauthorised Acquisition are described in Appendix C “Corrective Measures.”

Corrective measures are designed with the primary objectives of:

- Secure the processing environment.

- Restore the processing environment to its normal state.

Closure

The Security Team will stay actively engaged throughout the life cycle of the Information Security Incident to assess the progress/status of all containment and corrective measures and determine at what point the incident can be considered resolved. Recommendations for improvements to processes, policies, procedures, etc. will exist beyond the activities required for incident resolution and should not delay closing the Information Security Incident.

Required Documentation for Critical Incident Response Meetings

All Incident activities, from receipt of the initial report through Post-Incident Review, are to be documented. The Security Team Lead is responsible for ensuring all events are recorded, assembling these records in preparation and performance of the post-incident review, and ensuring all records are preserved for review. Security Team members may be employed in these efforts.

1. **General overview of the Incident** → Summary of the Incident providing a general description of events, approximate timelines, and parties involved, resolution of the incident, external notifications required and recommendations for prevention and remediation.
2. **Detailed review of the Incident** → Description of Incident events, indicating specific timelines, personnel involved, hours spent on various activities, impact to clients and 3rd parties (e.g., system not available, business continuity issues), ensuing discussions, decisions and assignments made, problems encountered, successful and unsuccessful activities, notifications required or recommended, steps taken for containment and remediation, recommendations for prevention and remediation (short-term and long-term), identification of policy and procedure gaps, results of post-incident review.
3. **Retention** → All relevant documentation will be retained by Security Team Lead for archival in a central repository. Access to the documentation and repository is typically restricted to Security Team membership.

Post-Incident Review (PIR)

A review of Information Security Incident-related activities is a required element of this policy.

The Security Team Lead will host a PIR after each Incident has been resolved and scheduled within 2-3 weeks of the Information Security Incident's remediation. The review is an examination of the Incident and all related activities and events. All activities performed relevant to the Incident should be reviewed with the aim of improving and honing the over-all incident response process.

1. **Recommendations** → The Security Team's recommendations on changes to policy, process, safeguards, etc. are both an input to and by-product of this review. "Fix the problem, not the blame" is the focus of this activity. All discussions, recommendations and assignments are to be documented for distribution to the Security Team and follow-up by Security Team Lead.
2. **Follow-up** → The Security Team Lead will follow-up with the Client and 3rd Party or other parties, as required and appropriate.

Just Culture

The 'Just Culture' approach is a term coined by NHS England and is targeted around patient safety. Basically, it treats staff that are involved in patient safety incident in a consistent, constructive, and fair manner.

ARO does not provide any products or services that could have a direct impact on patient safety.

However, ARO have adapted this approach in treating staff involved in any incident in a consistent, constructive, and fair manner.

Appendix A – Incident Sensitivity and Criticality Levels

INCIDENT CATEGORY AND SENSITIVITY LEVELS

All incidents managed by the Security Team should be classified into one of the categories listed in the table below:

Incident Category	Sensitivity	Description
Denial of Service	S3	DOS or DDOS attack
Forensics	S1	Any forensic work done by ICT
Compromised Information	S1	Attempted or successful destruction, corruption, or disclosure of sensitive information or IP
Compromised Asset	S1, S2	Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	Theft / Fraud / Human Safety / Child Pornography. Computer-related incidents of a criminal nature, involving law enforcement or Loss Prevention.
Internal Hacking	S1, S2, S3	Reconnaissance or Suspicious activity originating from inside the internal network, excluding malware.
External Hacking	S1, S2, S3	Reconnaissance or Suspicious Activity originating from outside AIMEs's network (partner network, Internet), excluding malware
Malware	S3	A virus or worm typically affecting multiple AIMEs devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	Spoofed email, SPAM, and other email security-related events
Consulting	S1, S2, S3	Security consulting unrelated to any confirmed incident.
Policy Breaches	S1, S2, S3	- Sharing offensive material, sharing/possession of copyright material. - Deliberate violation of Information Security policy. - Inappropriate use of university asset such as computer, network, or application. - Unauthorised escalation of privileges or deliberate attempt to subvert access controls.

Note: Sensitivity levels may vary depending upon circumstances

Sensitivity Classification

The Security Team should always apply the “need to know” principle when communicating case details with other parties. The sensitivity matrix below helps to define “need to know” by classifying cases according to sensitivity level. The ‘Required’ column defines the parties that “need to know” for a given sensitivity level. The ‘Optional’ column defines the other parties that may be included on communications, if necessary.

Sensitivity Classification

Sensitivity Level	Sensitivity Level Definition	Typical Incident Categories	Required on case communications	Optional On Case Communications	Access
S1	Extremely Sensitive	- Global Investigations Initiated - Forensics Request - Destruction of property - Compromised asset - Compromised Information - Unlawful activity - Inappropriate use of property - Policy violations	Security Team Lead	ABC Board	Security Team, ABC Board
S2	Sensitive	- External Hacking - Internal Hacking - Unauthorised Access	Security Team Lead	ABC Board	Security Team, ABC Board
S3	Not Sensitive	- Denial of service - Virus/Worm - email	Security Team Lead	ABC Board	All ABC Staff

Criticality Classification

The criticality matrix defines the minimal customer response time and ongoing communication requirements for a case. The criticality level should be assigned the case when created, and it should not be altered at any point during the case lifecycle except when it was incorrectly classified in the first place.

Criticality Classification						
Level	Critical Level Definition	Typical Incident Categories	Initial Response Time	Ongoing response (Critical phase)	Ongoing Response (resolution phase)	Ongoing Communications Requirement
C1	Incident affecting critical systems or information with potential to be revenue or client impacting.	- Denial of service - Compromised Asset (critical) - Internal Hacking (active) - External Hacking (active) - Virus / Worm (outbreak) - Destruction of property (critical)	60 mins	Security Team Lead or Security Team Lead nominee assigned to work case on 24x7 basis	Security Team Lead or Security Team Lead nominee assigned to work case during normal business hours	Case update sent to appropriate parties daily during critical phase. If Security Team involvement is necessary to restore critical systems to service then case update will be sent a minimum of every 2 hours. Case update sent to appropriate parties on a weekly basis During resolution phase.
C2	Incident affecting noncritical systems or information, not revenue or customer impacting. Employee investigations	- Internal Hacking (not active) - External Hacking (not active) - Unauthorised access. - Policy breaches - Unlawful activity. - Compromised information.	4 hrs	Security Team Lead or Security Team Lead nominee assigned to work case on 24x7 basis	Security Team Lead nominee assigned to work case during normal business hours	Case update sent to appropriate parties daily during critical phase. Case update sent to appropriate parties on a weekly basis

	that are time sensitive should typically be classified at this level.	- Compromised asset. (non-critical) - Destruction of property (non-critical)				During resolution phase.
C3	Incident, noncritical systems. Incident or employee investigations that are not time sensitive. Long-term investigations Involving extensive research and/or detailed forensic work.	- Email - Forensics Request - Inappropriate use of property. - Policy breaches	48hrs	Security Team Lead nominee assigned to work case on 24x7 basis	Security Team Lead nominee assigned to work case during business hours	Case update sent to appropriate parties on a weekly basis

Appendix B – Incident Containment Activities

The Security Team will determine and execute the appropriate activities and processes required to quickly contain and minimise the immediate impact to ARO, customers and third parties.

Containment activities are designed with the primary objectives of:

- Counteract the immediate threat
- Prevent propagation or expansion of the incident
- Minimise actual and potential damage
- Restrict knowledge of the incident to authorised personnel
- Preserve information relevant to the incident

CONTAINMENT ACTIVITIES UNAUTHORISED ACCESS

ACTIVITIES THAT MAY BE REQUIRED TO CONTAIN THE THREAT PRESENTED TO SYSTEMS WHERE UNAUTHORISED ACCESS MAY HAVE OCCURRED.

1. Disconnect the system or appliance from the network or access to other systems.
2. Isolate the affected IP address from the network.
3. Power off the appliance(s), if unable to otherwise isolate.
4. Disable the affected application(s).
5. Discontinue or disable remote access.
6. Stop services or close ports that are contributing to the incident.
7. Remove drives or media known or suspected to be compromised.
8. Where possible, capture and preserve system, appliance and application logs, network flows, drives and removable media for review.
9. Notify Security Team of status and any action taken.

CONTAINMENT ACTIVITIES UNAUTHORISED ACQUISITION

ACTIVITIES THAT MAY BE REQUIRED TO CONTAIN THE THREAT PRESENTED TO ASSETS WHERE UNAUTHORISED ACQUISITION MAY HAVE OCCURRED.

1. Identify missing or compromised assets.
2. Gather, remove, recover, and secure sensitive materials to prevent further loss or access.
3. Power down, recycle or remove equipment known to be compromised.
4. Where possible, secure the premises for analysis by local management and law enforcement.
5. Gather and secure any evidence of illegal entry for review by local management and law enforcement.
6. Where possible, record identities of all parties who were a witness to events.
7. Preserve camera logs and sign-in logs for review by local management and law enforcement.
8. Notify Security Team of disposition of assets and any action taken.

Appendix C – Corrective Measures

The Security Team will determine and cause the execution of the appropriate activities and processes required to quickly restore circumstances to a normal secure state.

Corrective measures are designed with the primary objectives of:

- Secure the processing environment
- Restore the processing environment to its normalized state

CORRECTIVE MEASURES – UNAUTHORISED ACCESS

ACTIVITIES THAT MAY BE REQUIRED TO RETURN CONDITIONS FROM UNAUTHORISED ACCESS TO A NORMAL AND SECURE PROCESSING STATE.

1. Change passwords on all local user and administrator accounts or otherwise disable the accounts as appropriate.
2. Change passwords for all administrator accounts where the account uses the same password across multiple appliances or systems (servers, firewalls, routers).
3. Re image systems to a secure state.
4. Restore systems with data known to be of high integrity.
5. Apply OS and application patches and updates.
6. Modify access control lists as deemed appropriate.
7. Implement IP filtering as deemed appropriate.
8. Modify/implement firewall rule sets as deemed appropriate.
9. Ensure anti-virus is enabled and current.
10. Make all personnel “security aware.”
11. Monitor/scan systems to ensure problems have been resolved.
12. Notify Security Team of status and any action taken.

CORRECTIVE MEASURES – UNAUTHORISED ACQUISITION

ACTIVITIES THAT MAY BE REQUIRED TO RETURN CONDITIONS FROM AN UNAUTHORISED ACQUISITION TO A NORMAL AND SECURE PROCESSING STATE.

1. Retrieve or restore assets where possible.
2. Store all sensitive materials in a secure manner (e.g., lockable cabinets or storage areas/container).
3. Install/replace locks and issue keys only to authorised personnel.
4. Restore security devices and/or apparatus to working condition.
5. Remove and retain unauthorised equipment from network/area.
6. Implement physical security devices and improvements (e.g., equipment cables, alarms) as deemed appropriate.
7. Make all personnel “security aware.”
8. Notify Security Team of status and any action taken.