

Information Security During Disruption Policy

(ISO 27001:2022 Organisational Controls – Clause 5.29)

Author	Greg Nott
Version	2.0
Date Created	02/06/2023
Last Update Date	24/05/2024
Document Control	Released
Document ID	230602-IMS-POL-InformationSecurityDuringDisruptionPolicy-V2
Security Classification	Public

Table of Contents

Information Security During Disruption Policy.....1

Approval.....3

Review.....3

Change History.....3

Associated Documents.....3

Scope.....4

 Purpose.....4

 Exceptions.....4

 Identify and Assess Potential Disruptions.....4

 Establish a Response and Recovery Plan 4

 Establish Alternative Business Processes.....4

 Protect Critical Information Assets 5

 Communicate with Stakeholders 5

 Learn from Disruptions 5

 Policy Review 5

Approval

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

Review

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

Change History

Author	Change	Issue	Date
Paul Langan	Creation	1.0	02-Jun-23
Greg Nott	Review & Rebrand	2.0	23-May-24

Associated Documents

Document	Version
230517-IMS-POL-Communications-V2	2.0
230501-IMS-PLN-AROBusinessContinuityPlan-V1	2.0
230607-IMS-POL-ProtectionAgainstMalware-V2	2.0

Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and describes the Information Security During Disruption 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, suppliers, customers, regulators, and other interested parties that may be affected by our business activities.

Purpose

The purpose of this policy is to define the measures and responsibilities necessary to maintain the security of our information assets during disruptions, including but not limited to natural disasters, cyber-attacks, infrastructure failures, and other emergencies. This policy aims to ensure the uninterrupted delivery of our services, protect our sensitive information, and minimise the impact of disruptions on our organisation.

Exceptions

- Any exceptions to the application of this policy or where controls cannot be adhered to MUST be presented to the Head of Information Security or a member of the management team.
- All exceptions to this policy MUST be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

Identify and Assess Potential Disruptions

ARO will proactively try to identify potential disruptions that may affect our operations, such as power outages, natural disasters, cyber-attacks, or supply chain interruptions. We will regularly review and update our risk assessment to identify new threats and vulnerabilities that may arise during disruptions.

Establish a Response and Recovery Plan

ARO will develop and maintain a comprehensive incident response and business continuity plan, aligned with ISO 27001:2022 requirements. This plan will define roles, responsibilities, and procedures to ensure the timely and effective response to disruptions, including communication and coordination with relevant stakeholders.

Establish Alternative Business Processes

Where possible, ARO will identify alternative business processes and systems that can be activated during disruptions to ensure continuity of critical operations. These processes will be regularly tested and maintained to ensure their effectiveness and efficiency.

Protect Critical Information Assets

We will prioritise the protection of critical information assets during disruptions. This includes ensuring appropriate backup and restoration processes are in place, and implementing additional security controls if necessary, such as increased monitoring or access restrictions.

Communicate with Stakeholders

ARO will maintain open and transparent communication with our stakeholders, including employees, customers, partners, and regulatory bodies, during disruptions. Clear communication channels and procedures will be established to provide timely updates on the status of operations and actions being taken to mitigate the impact.

Learn from Disruptions

ARO will conduct thorough post-incident reviews after disruptions to identify lessons learned and areas for improvement. Recommendations and corrective actions will be implemented to enhance our resilience to future disruptions.

Policy Review

This policy will be reviewed at least annually or whenever there are significant changes to ARO's operations, systems, or threat landscape.