

Access Control Policy

(ISO 27001:2022 Organisational Controls, Clauses 5.15,
5.17 and 5.18)

Author	Greg Nott
Version	3.0
Date Created	27/07/2023
Last Update Date	21/10/2025
Document Control	Released
Document ID	230727-IMS-POL-AccessControl-V3
Security Classification	Public

Table of Contents

Access Control Policy.....1

Approval.....3

Review.....3

Change History.....3

Associated Documents.....3

Scope.....4

 Purpose.....4

 Topic-specific Approach 4

 Supporting Policies.....4

 Compliance with Regulations.....5

 Managing Physical Access.....5

 Logging & Compliance 5

 Training & Awareness 5

 Review & Update 5

Approval

Author	Issue	Approved By	Date
Greg Nott	1.0	Simon Naylor	06-Aug-23
Greg Nott	2.0	Paul Langan	13-May-24
Greg Nott	3.0	Greg Nott	21-Oct-25

Review

Reviewer	Review Criteria	Issue	Date
Paul Langan	ISO 27001:2022	1.0	02-Aug-23
Paul Langan	Review & Rebrand	2.0	13-May-24
Greg Nott	Annual Review	3.0	21-Oct-25

Change History

Author	Change	Issue	Date
Greg Nott	Creation	1.0	16-Mar-23
Greg Nott	Review & Rebrand	2.0	13-May-24

Associated Documents

Document	Version
Statement of Applicability	1.0
Information Access Restriction Policy	3.0
Liverpool Data Centre Access Policy	2.0
Identity Management Policy	2.0
Password Management Policy	2.0
User Registration Policy	2.0
Privileged Access Rights Policy	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 Access Control 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 third-party vendors who handle sensitive data on behalf of the organisation.

Purpose

This Access Control Policy establishes the guidelines and procedures for managing access to resources, data, and systems within the organisation. This policy applies to all employees, contractors, vendors, and any other entities requiring access to ARO information assets.

Topic-specific Approach

To comply with ISO 27001:2022 Annex A Control 5.15, ARO follows a topic-specific approach for Access Control. Instead of a blanket policy, we implement individualised Access Control policies tailored to specific business functions.

Supporting Policies

The organisation has implemented a set of policies and procedures that support this Access Control policy including:

Information Access Rights Policy

Our Information Access Rights Policy outlines the process for granting access rights to various information assets based on employees' roles and responsibilities. It ensures consistency between the data to which access is granted and the type of access rights assigned.

Identity Management Policy

The Identity Management Policy governs the creation, maintenance, and revocation of user identities within our systems. It also includes provisions for role-based access control (RBAC) to ensure authorised access privileges are granted based on predefined job functions and responsibilities.

Password Management Policy

To maintain the security of our systems, the Password Management Policy mandates the use of strong, unique passwords for each user, based on up-to-date recognised best practice, including the use of Multi-Factor Authentication, guidance for the creation of secure passwords and secure handling mandates.

User Registration Policy

The User Registration Policy sets guidelines for onboarding and offboarding employees and other entities. When granting access, we follow a structured, formal access request and authorisation process, ensuring documented approval from the appropriate personnel.

Privileged Access Rights Policy

The Privileged Access Rights Policy defines the process for granting, monitoring, and auditing access privileges for users with elevated access rights. We closely monitor users with privileged access to prevent any compromise of our Access Control function.

Compliance with Regulations

Our Access Control policies comply with any prevailing legislation, sector-specific regulatory guidelines, or contractual obligations relating to data access, as outlined in ISO 27001:2022 Annex A Control 5.15. This includes the "need to know" principle for the distribution, security, and categorisation of information.

Managing Physical Access

Physical access to our facilities is controlled in accordance with Controls 7.2, 7.3, and 7.4 of ISO 27001:2022 Annex A. We maintain a robust set of building and room access controls, including managed entry systems, security perimeters, and visitor procedures.

Logging & Compliance

We maintain detailed logs of access events, file activity, and security events to ensure compliance with ISO 27001:2022 Annex A Controls 5.16 and 5.18. Access to these logs is strictly controlled to safeguard against unauthorised access.

Training & Awareness

This policy shall be communicated to all employees and stakeholders.

All employees and relevant stakeholders receive training on our Access Control policies and their responsibilities in adhering to these policies. Awareness of potential conflicts of interest is emphasised to prevent abuse of access levels.

Review & Update

This Access Control Policy is subject to regular review and update to ensure its effectiveness, relevance, and alignment with evolving business needs and regulatory requirements.