

Change Management Policy

(ISO 27001:2022 Technological Controls - Clause 8.32)

Author	Greg Nott
Version	2.0
Date Created	20/06/2023
Last Update Date	14/05/2024
Document Control	Released
Document ID	230620-IMS-POL-ChangeManagement-V2
Security Classification	Public

Table of Contents

Change Management Policy	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Policy.....	4
Restrictions on Changes to Data Centre Software Packages.....	5

Approval

Author	Issue	Approved By	Date
Greg Nott	1.0	Simon Naylor	07-Aug-23
Greg Nott	2.0	Paul Langan	14-May-24

Review

Reviewer	Review Criteria	Issue	Date
Paul Langan	ISO 27001:2022	1.0	03-Aug-23
Paul Langan	Review & Rebrand	2.0	14-May-24

Change History

Author	Change	Issue	Date
Greg Nott	Creation	1.0	20-Jun-23
Greg Nott	Review & Rebrand	2.0	14-May-24

Associated Documents

Document	Version
239619-IMS-POL-ITSNProcessGuide-V1	1.0

Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and describes the Change Management 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 service providers who have access to or are responsible for information assets and critical business processes within the organisation.

Policy

- It is the responsibility of users when creating / modifying or removing any information asset 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.
- Change Management is in place to ensure that Changes to the organisation's services are managed and implemented in a way that minimises risk and impact to our users and customers.
- It ensures the organisation considers the impact, risk assessment, cost benefit, deployment, and mitigation as it protects live service from any unauthorised change.
- Change Management is an essential control element that enables prioritisation and surety of deployment success. In an ever-increasingly digital marketplace, Change Management will be applied in a manner that balances the need for control with the need for agility.
- In rare cases work may be carried out without a change request being raised if authorisation is given by the applicable Information Asset Owner. A log of any such work carried out must still be kept.
- Transactional services such as Mobile services, will not be subject to Change control.
- It will be the responsibility of the Change Requestor to ensure relevant communications are issued via the agreed channels to (potentially) impacted customers.
- All Changes will be logged in the appropriate IT Service Management tool (i.e. BOLT, Autotask).
- Software developed by ARO for customers will not be modified unless a change request has been raised by the customer.
- Any changes made to an ARO Cloud Service by ARO will be relayed to the Cloud Service Customers.

Restrictions on Changes to Data Centre Software Packages

Modifications to software packages should only be made under the following circumstances:

1. No longer 'fit for purpose'. The software cannot perform its task/service unless it is upgraded.
2. A security leak has been found and a fix for it has been released by the vendor.

In both cases it is to job of the Senior System Administrator to monitor the software's performance and if the associated vendor releases any patches for the software. Any software patches released will be analysed by the Senior System Administrator who will decide if the patch needs to be implemented.