INSERT LOGO

ISMS CHANGE MANAGEMENT POLICY

Classification: Internal

This document may only be shared internally without prior confirmation from the owner.

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Contents

1. Purpose

This policy defines the process for managing changes to the Information Security Management System (ISMS) to ensure that any changes do not adversely affect information security and that all changes are appropriately authorised, documented, and communicated.

2. Scope

This policy applies to all ISMS changes, including scope, procedures, and policies.

Technical changes to code, applications, services, and other IT infrastructure are outside the scope of this policy and should follow the organisation's formal IT change/release management process.

3. Policy Statements

3.1 Change Request and Authorisation

- All proposed changes to the ISMS must be formally requested using the Change Request Form (CRF).

- Change requests must include a description, the rationale for the change, potential impacts, and a risk assessment.
- The Information Steering Group (ISG) must review and approve change requests before implementation.

3.2 Impact Assessment and Planning

- Each change request must undergo a detailed impact assessment to evaluate its potential effects on information security, including confidentiality, integrity, and availability risks.
- A detailed change implementation plan must be developed, outlining the steps required to implement the change, including resource requirements, timelines, and rollback procedures.

3.3 Implementation and Documentation

- Approved changes must be implemented according to the change implementation plan.
- All changes must be documented, including the details of the change, the date of implementation, and the individuals involved.
- The ISMS documentation must reflect the changes, including policies, procedures, and scope documents.

3.4 Communication and Training

- Changes to the ISMS must be communicated to all relevant stakeholders, including employees, contractors, and third parties, as appropriate.
- Training sessions must be conducted if the changes significantly affect the ISMS processes or require new skills or knowledge.

3.5 Review and Monitoring

- Changes must be implemented and monitored to ensure they achieve the intended outcomes without introducing new security risks.
- A post-implementation review must be conducted to evaluate the effectiveness of the change and identify any lessons learned.

4. Responsibilities

- The Information Security Group (ISG) is responsible for reviewing and approving all change requests.
- The IS Manager is responsible for coordinating the change management process and ensuring compliance with this policy.
- All employees are responsible for adhering to this policy and participating in change-related activities as required.

5. Exceptions

Any exceptions to this policy must be approved by the ISMS Manager and documented accordingly.

6. Review

This policy must be reviewed and updated at least annually or whenever significant changes to the ISMS occur.