elevaite365

TECH THAT MATTERS

Elevaite365

Document Control Procedure

Version 1.0

PURPOSE

This procedure defines how Elevaite365 (hereby as organization) creates, reviews, approves, issues, revises, and disposes of Information Security Management System (ISMS)- related documented information. The goal is to ensure that all documents and records are properly controlled, accessible, and protected.

SCOPE

This procedure applies to all ISMS-related documented information, including, but not limited to, policies, procedures, formats, templates, manuals, reports, dashboards, and records. It applies to all departments and functions under the organization's ISMS scope. Documented information may be in paper, electronic, or other media and may be stored locally, on shared drives, or in the cloud (e.g., Google Drive).

DEFINITION

- **ISMS (Information Security Management System):** A systematic approach to managing sensitive information securely, covering people, processes, and IT systems.
- **ISG (Information Security Group):** The team oversees ISMS implementation and ensures compliance with security policies.
- **CEO (Chief Executive Officer):** The highest-ranking executive responsible for overall management.
- **ISMS-Related Process:** Any process defined for carrying out ISMS tasks or activities.
- **Documented Information:** Any document or record created under ISMS.
- **Document:** Information and its supporting medium (e.g., paper, electronic, optical disc).
- **Record:** A specific document that provides evidence of results achieved or activities performed.
- **Document Owner:** The individual or team with ultimate accountability for creating, accurately, and maintaining a specific document. Ensures it meets organizational standards and obtains appropriate approvals.
- **Master List:** A centralized index or register to track all controlled documents, including document title, version number, release date, and status (active/obsolete).
- **Version Control:** A method of tracking document changes through unique version or revision numbers, usually accompanied by dates and reasons for modifications.
- **Obsolete Document**: A document that has been superseded by a new version or is no longer relevant must be removed from active use or marked as archived.

RESPONSIBILITIES

ISG Team

1. Primary responsibility for implementing this procedure and ensuring all ISMS-related documents follow correct creation, approval, distribution, and archival processes.
2. Maintains access controls, defines retention periods, and coordinates with department heads to ensure compliance with ISMS requirements.
3. Periodically reviews the Document Master List and ensures all obsolete documents are withdrawn and properly archived or destroyed.

Heads of Departments

1. Oversee the creation, review, and update of departmental documents, ensuring alignment with ISMS and organizational policies.
2. Authorize the distribution of department-specific documents and maintain a departmental Master List if separate from the central register.
3. Coordinate with the ISG Team to handle any changes or revisions that affect the department's operations or policies.

Document Owner

1. Responsible for the accuracy and completeness of the document's content.

2. Coordinates with the ISG Team for version control and ensures the document progresses from draft to final approved state.
3. Follows change management procedures when initiating updates or revisions, including preparing any supporting impact analyses or justifications.

All Employees

1. Must adhere to the approved documents and refrain from using outdated versions.
2. Report any identified errors, inconsistencies, or potential improvements in existing documents to the Document Owner or ISG Team.

PROCEDURE

Creation of Documents

1. **Initiation**

   a. A document may be created when a need arises (e.g., system requirements, audit findings, corrective actions, or new policies).

   b. The document is not yet approved while in draft mode; any changes made in this phase are not tracked for version history.

2. **Identification**

   a. Assign a name that reflects its purpose (e.g., “Change Management Procedure”).

   b. Follow the Change Management Procedure when creating any ISMS-documented information.

Approval of Documents

Approval Authorities

1. The relevant authority must approve all documents before release.
2. The Leadership Team approves Apex ISMS documents (e.g., ISMS Policy).
3. The ISG Team approves other departmental ISMS documents from the head of that department.

Approval Records

1. Email approvals must be retained electronically.
2. Physical approvals can be captured via signature or documented meeting minutes.

Version Control

1. The creator’s Designation (optionally, name) must be mentioned (e.g., “Created by – ‘ISG Team’”).
2. Approver’s Designation (optionally, name) must be mentioned (e.g., “Approved by – ‘Leadership Team’”).
3. Release/Issue Date in DD-MM-YYYY or DD Month YYYY format (e.g., “August 15, 2018”).
4. Version Number starts at 1.0. Each newly approved revision increments by 1.0 (e.g., from 1.0 to 2.0).

Format Conversion

1. Approved documents should be converted to non-editable formats (e.g., PDF) where feasible to prevent accidental edits.
2. Templates or spreadsheets with built-in formulas may remain editable if necessary.

Issue of Documents

1. **Document Distribution**

   a. ISG Team or Department Heads control the distribution of approved documents.

   b. The Google Drive shared folder is the primary repository of legitimate and controlled copies.

2. **Availability**

   a. All relevant users must have access to the current version of the document (soft copy via shared folder or email).

   b. Documents are often stored in PDF format for easy use and to prevent accidental modifications.

3. **Retention**

   a. Hard copies should be stored in secure locations (locked cupboards).

    b. ISG Team (for ISMS documents) and the department heads (for departmental documents) ensure relevant versions are accessible and obsolete versions are withdrawn.

Revision to Document

1. **Initiation of Revisions**
    a. Revisions may occur due to system errors, audit results, corrective actions, or staff suggestions.
    b. The Change Management Procedure applies to changes to ISMS documents.
2. **Approval and Versioning**
    a. Each approved revision increases the version by 1.0 (e.g., 2.0, 3.0).
    b. Record the nature of change and purpose in an “amendment record” or “revision history.”
3. **Obsolete Versions**
    a. When a new version is approved, old versions are withdrawn and placed in a separate “Obsolete” or “Archive” folder if retained for legal or knowledge purposes.
    b. The ISG Team updates the ‘Master List’ with the current revision, ensuring all users have the latest version.

Documents and Records in electronic format or media

1. **Security and Access Control**
    a. Electronic documents must be adequately protected (user-level/system-level passwords, malware protection).
    b. Only authorized personnel, based on access rights defined by the ISG Team and department heads, may edit or delete documents.
2. **Shared Drive Management**
    a. Approved documents reside in Google Drive (or equivalent).
    b. The ISG Team manages access control lists, ensuring appropriate permissions (view, edit, etc.) for designated staff.

Documented Information of External Origin

1. **Definition**
    a. Any external standards, guidelines, policies, laws, or regulations the organization uses, references, or adopts.
2. **Exclusion from Internal Controls**
    a. This procedure's version control, approval, and distribution rules do not apply to external documents (e.g., ISO standards, government laws) maintained by third parties.
3. **Maintenance**
    a. The ISG Team (for ISMS) and department heads (for departmental references) track these external documents to ensure that current versions are accessible and that obsolete versions are withdrawn.

Disposal of Documents and Records

1. **Withdrawal**

    a. Obsolete or unneeded documents/records are removed from the point of use (shared drive, email, or physical files).

2. **Destruction**

    a. Hard copies are shredded or burned to prevent unauthorized disclosure.

    b. Electronic copies are securely deleted (erased from electronic media using secure disposal methods).

3. **Responsibility**

    a. ISG Team disposes of obsolete ISMS documents.

    b. Heads of Departments dispose of departmental documents accordingly.

Records and Evidence

1. All approvals, version histories, distribution lists, and obsolescence records must be kept as evidence of compliance.

2. Email records or digitally signed documents are recommended for traceability and audit purposes.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	-	Initial Release	Borhan	-	-