elevaite365

TECH THAT MATTERS

Elevaite365

Information Classification Policy

Version 1.0

PURPOSE

This Information Classification Policy aims to establish a standardized process for defining and applying classifications to information, data, and documentation within Elevaite365 (hereby referred to as organization). This policy ensures that all information is managed appropriately based on its sensitivity, value, and criticality level, thereby safeguarding the confidentiality, integrity, and availability of the Organization's information assets.

SCOPE

This policy applies to all information and data created, stored, and processed within the organization. It encompasses internal information, which includes all data generated and managed internally by the organization, as well as external and third-party information, covering information procured, stored, or processed from external sources and third parties as part of the organization's business activities. Additionally, the policy applies to all personnel, including employees, contractors, consultants, and third-party partners, who have access to the organization's information assets. By addressing these areas, the policy ensures comprehensive protection and management of all information the organization handles.

DEFINITION

Following is an explanation of various terms used within this document:

Information: Meaningful data that is processed, stored, or transmitted by the Organization.

Asset: Any item that carries information and is of importance to the Organization, including hardware, software, data, and documentation.

Classification: The process of assessing the criticality, sensitivity, and importance of data and information and categorizing them to ensure appropriate controls are applied during handling, storage, and transmission.

ISMS: A systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes, and IT systems by applying a risk management process.

Information Security: The preservation of the confidentiality, integrity, and availability (CIA triad) of information to protect against unauthorized access, use, disclosure, disruption, modification, or destruction.

CEO: Chief executive officer, The highest-ranking executive in the Organization, responsible for overall management and decision-making.

RESPONSIBILITIES

Leadership Team

1. **Policy Endorsement:** Approve and endorse the Information Classification Policy.
2. **Resource Allocation:** Ensure adequate resources are provided for implementing and maintaining the policy.
3. **Oversight:** Monitor the effectiveness of the policy and ensure alignment with organizational goals and regulatory requirements.

Information Security Group (ISG)

1. **Policy Implementation:** Develop, implement, and maintain the Information Classification Policy within the Information Security Management System (ISMS) scope.
2. **Guidance and Support:** Provide advice and support to departments for proper classification and handling of information.
3. **Training and Awareness:** Conduct training sessions to educate employees on classification standards and procedures.

Department Heads

1. **Policy Enforcement:** Implement and enforce the Information Classification Policy within their departments.
2. **Classification Oversight:** Ensure all information, data, and documentation within their department are classified appropriately.

3. Incident Reporting: Report any classification-related incidents or breaches to the ISG promptly.

All Employees, Contractors, and Third Parties

1. Compliance: Adhere to the Information Classification Policy and apply appropriate classifications to the information they handle.

2. Reporting: Promptly report any suspected or actual security incidents or breaches related to information classification.

3. Training Participation: Participate in mandatory training and awareness programs on information classification and security.

POLICY

TYPE OF CLASSIFICATIONS

Confidential: This information is of moderate sensitivity and confidentiality value to the Organization. Unauthorized sharing or disclosure may result in financial or organizational loss contractual or regulatory non-compliance.

1. Internal Sharing: Allowed without specific approvals.

2. External Sharing with Relevant Parties: Allowed without specific approval by the concerned custodian or owner.

3. External Sharing with Unrelated Entities: Requires approval from the department head.

Internal Use: This type of information is of low sensitivity and confidentiality value to the Organization.

1. Internal Sharing: Allowed without specific approvals.

2. External Sharing: This may be done without approval, provided it does not contain sensitive or proprietary information.

Public: This type of information is of low sensitivity and confidentiality value to the Organization. It is intended for public dissemination and general sharing.

1. Internal and External Sharing: Freely allowed within and outside the Organization without restrictions.

2. Impact: Sharing or disclosing public information will not negatively impact the Organization's operations, assets, or reputation.

External Origin: This includes any information, data, or documentation from external sources, such as clients, partners, or third-party vendors. Ownership and control remain with the external entity, and the Organization acts as a custodian while handling, processing, or storing such information.

1. Classification by Originator: Follow the classification and handling rules the external entity provides.

2. No Classification Provided**:** The Organization will classify the information based on sensitivity and confidentiality.

Classification Guidelines

Confidential Information:

Examples: Financial records, employee personal information, strategic plans, and proprietary research data.

Handling Requirements: Access is restricted to authorized personnel. Encrypted storage and transmission. Physical documents are stored in secure locations.

Internal Use Information:

Examples: Internal memos, standard operating procedures, and non-sensitive project documentation.

Handling Requirements: Accessible to all employees within the Organization. Stored in internal systems without encryption unless specified.

Public Information:

Examples: Press releases, marketing materials, publicly available reports, and published research findings.

Handling Requirements: There are no restrictions on access or distribution. It can be freely shared within and outside the Organization.

External Origin Information:

Examples: Client-provided data, partner agreements, and third-party vendor documentation.

Handling Requirements: Follow external classification and handling instructions. If none are provided, classify based on internal guidelines.

CLASSIFYING THE INFORMATION, DATA AND DOCUMENTS

Classifying Internal Information

1. Responsibility:

The creator or owner of the information, data, or document is responsible for assessing its sensitivity, value, and criticality.

2. Assessment:

Evaluate the potential impact of unauthorized access, disclosure, alteration, or destruction on the Organization’s operations, assets, individuals, mission, or reputation.

3. Classification Application:

Applying the appropriate classification level (Confidential, Internal Use, Public) is based on the assessment.

4. Implementation:

4.1. Ensure the classification is consistently applied across all mediums (e.g., electronic, physical).

4.2 Adhere to each classification level’s handling, storage, and sharing requirements.

Handling Externally Originated Information

1. Follow Originator’s Classification:

When receiving information, data, or documents from external sources, adhere to the classification and handling instructions provided by the originator.

2. No Provided Classification:

2.1 The organization must assess the information’s sensitivity and criticality if the external originator does not provide classification guidelines.

2.2 Apply the appropriate internal classification level based on the assessment.

3. Documentation:

Maintain records of the classification decisions and their rationale for accountability and future reference.

Rules for Storing, Sharing, and Access

1. Storing Information:

1.1. Confidential: Encrypted storage, access restricted to authorized personnel, secure physical storage for hard copies.

1.2. Internal Use: Stored in internal systems with appropriate access controls.

1.3. Public: Stored in systems accessible to all employees and publicly accessible repositories.

4. External Origin: Stored according to the classification guidelines provided by the originator or the Organization’s internal classification if none are provided.

2. Sharing Information:

2.1. Confidential: Shared internally with authorized personnel only. External sharing requires approval from the information custodian or department head.

2.2. Internal Use: Shared within the Organization without the need for specific approvals. External sharing is permitted if it does not contain sensitive information.

2.3. Public: Freely shared within and outside the Organization without restrictions.

2.4. External Origin: Shared externally per the originator's guidelines or the Organization's classification standards.

3. Access Control:

3.1. Confidential: Strict access controls are enforced through role-based access control (RBAC) and multi-factor authentication (MFA).

3.2. Internal Use: Access is controlled based on job functions and responsibilities.

3.3. Public: No access restrictions.

3.4. External Origin: Access is controlled based on the originator's guidelines or internal classification policies.

LABELING OF CLASSIFICATION

Proper labeling of information ensures easy identification and appropriate handling. The following guidelines must be adhered to for labeling classified information:

Labeling Requirements

Confidential Information:

1. Hard Copies: Stamped in ink at the top or bottom of each page with a confidentiality label (e.g., "CONFIDENTIAL").

2. Soft Copies: Marked within the document (e.g., header/footer) or through metadata tagging in the document management system.

3. Digital Files: Use secure naming conventions and tagging systems to denote classification levels.

Internal Use Information:

1. Hard Copies: No specific labeling is required; it is considered internal by default.

2. Soft Copies: This may include a simple "Internal Use Only" label within the document or metadata.

Public Information:

1. Hard Copies and Soft Copies: Clearly labeled as "PUBLIC" to indicate no restrictions on sharing and distribution.

External Origin Information:

1. Hard Copies and Soft Copies: Follow the originator's instructions for labeling. If none, apply the Organization's internal classification labels based on the assessment.

Unlabeled Information

Default Classification: Any information, data, or document not explicitly labeled shall be considered **Internal Use**.

Handling Procedures: Apply the exact handling, storage, and access controls defined for the Internal Use classification.

Electronic Labeling and Tagging

Document Properties: Utilize document properties (e.g., headers, footers, watermarks) to indicate classification levels.

Tagging Systems: Implement tagging within the document management system to classify and track information systematically.

Access Control Integration: Ensure that classification labels are integrated with access control systems to enforce appropriate permissions automatically.

Database and Application Security

Confidential Data Protection: Ensure that confidential data stored in databases or applications is protected through access controls, encryption, and regular security audits.

Monitoring and Auditing: Continuously monitor access and usage of classified data to promptly detect and respond to unauthorized activities.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Aug 29 2025	Initial Release	Borhan	Linh	Borhan