TECH THAT MATTERS

Elevaite365

Information Security (IS) Policy

Version 1.0

PURPOSE

The document aims to provide Elevaite365 (herein referred to as Organization) with information on the need to protect the Confidentiality, Integrity, and Availability of Information assets.

1. Ensuring information and information systems are available to the intended

2. Protection of information against unauthorized access and maintain confidentiality of information

3. Protection of information against unauthorized modification

4. Adhere to relevant legislative, regulatory, and contractual requirements

5. Establish controls for protecting the organization's information and information assets against harm and loss, natural or deliberate

6. Motivate employees to maintain responsibility for, ownership of, and knowledge about information security to minimize the risk of security incidents.

7. Ensure that the organization is capable of continuing its services even if a major security incident occurs

8. Comply with international standards for information security, such as ISO 27001:2022

SCOPE

This policy applies to the organization, its employees, contractors, and its operations.

DEFINITION

1. CISO - Chief Information Security Officer

2. I**nformation Processing System** - The subsystems of the Information System in which data are recorded and processed following a formal procedure

3. Information— Information is an asset, like any other important business asset, that has value to an organization and needs to be suitably protected.

4. Confidentiality - The property in which information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity - The property of safeguarding the accuracy and completeness of assets.

Availability - The property that is accessible and usable upon demand by an authorized entity.

Information Security - The preservation of the confidentiality, integrity, and availability of information held in any medium, e.g., electronically, paper-based, or any other storage medium, is called information security

RESPONSIBILITIES

Chief Information Security Officer (CISO) is responsible for implementing, maintaining, and enforcing the policy.

Employees are responsible and/or accountable for ensuring adherence to this policy's terms during their job duties.

POLICY

1. All efforts shall be made to ensure Confidentiality, Integrity, and Availability of Information.

2. Information and information processing systems shall be used securely, supporting the organization's strategic goals and objectives.

3. A formal Information Security Management System (ISMS) process shall be established to implement, operate, maintain, monitor, and improve the security controls to safeguard the information.

4. Information shall be handled securely to avoid any loss of confidentiality, integrity, and availability during its creation, storage, processing, transmission, and disposal.

5. There shall be designated owners to classify information based on confidentiality, integrity, and availability requirements and protect against internal and external threats.

6. All risks related to information and information processing systems shall be identified and mitigated on a timely basis.

7. Employees shall be adequately trained and made aware of their roles and responsibilities regarding information security. They shall exercise discretion, common sense, and reasonable judgment regarding using the organization's Information.

8. Information and information processing systems shall be accessible to authorized users per their business needs.

9. Personnel, Information, and information processing systems shall be physically secured from physical and environmental threats.

10. A formal process shall ensure the regular identification, control, and monitoring of risks related to third-party vendors or suppliers.

11. All changes related to information and information processing systems shall be managed & controlled securely.

12. All information security incidents shall be reported and managed promptly

13. Business Continuity Plans shall be defined, implemented, and tested adequately to ensure the availability of information and information processing systems during any emergency

14. All applicable legal and/or regulatory requirements about information security shall be met

15. The posture of information security shall be continuously reviewed and improved to ensure continuous adherence to this policy

16. Employees are prohibited from divulging, copying, altering, or destroying any information, unless properly authorized, within the scope of their professional activities

17. Employees shall take appropriate measures to protect confidential information that is within the scope of their professional activities

18. Data Masking shall be done to limit the exposure of personal data and to comply with legal, statutory, regulatory, and contractual requirements

19. Data shall be deleted and stored in information systems, devices, or any other storage media when no longer required.

20. Employees shall adhere to the information security policies, procedures, standards, guidelines, etc, approved by the management.

21. Employees shall not attempt to circumvent or subvert any information security controls.

22. All information security incidents and threats shall be reported and managed promptly.

23. Information related to threats to information assets shall be collected and analyzed to facilitate informed decision-making, prevent threats from harming the organization, and reduce their impact.

SUPPORTING POLICIES

The following policy documents will support the Information Security Policy.

HUMAN RESOURCE SECURITY POLICY

This policy aims to ensure that Users understand their responsibilities and are suitable for the roles they are considered for.

INFORMATION CLASSIFICATION POLICY

This document defines guidelines and baseline security controls for protecting organization-owned data.

ACCESS CONTROL POLICY

1. The purpose of this policy is as follows:

2. To limit access to information and information processing facilities.

3. To ensure authorized user access and to prevent unauthorized access to systems and services.

4. To make users accountable for safeguarding their authentication information.

5. To prevent unauthorized access to systems and applications.

6. Segregation of duties

ASSET MANAGEMENT AND DISPOSAL POLICY

The purpose of this policy is as follows:

To identify the organization's assets and define appropriate protection responsibilities.

This ensures that information receives appropriate protection because of its importance to the organization.

To prevent unauthorized disclosure, modification, removal, or destruction of information stored in the media.

ENCRYPTION AND KEY MANAGEMENT POLICY

This policy ensures the proper and effective use of encryption management to protect information confidentiality, authenticity, and/or integrity.

ACCEPTABLE USE POLICY

This policy defines best practices for the acceptable use of information and IT assets by the Information Security Policy.

MOBILE AND TELEWORKING POLICY

This policy ensures that information is protected when accessed, processed, or stored on mobile devices and during teleworking.

LOG MANAGEMENT AND MONITORING POLICY

This policy aims to monitor and record information system events and generate evidence.

SECURE DEVELOPMENT AND MAINTENANCE POLICY

This policy ensures that information security is integral to information systems throughout the development and maintenance phases.

INCIDENT MANAGEMENT POLICY

This policy ensures a consistent and effective approach to managing information security incidents, including communication on security events and weaknesses.

CHANGE MANAGEMENT POLICY

This policy ensures that changes to the organization's business processes, information processing facilities, and systems that affect information security are controlled.

RISK MANAGEMENT PROCEDURE

This framework aims to manage information security risks throughout the organization's applications and infrastructure, promote an information security risk culture, and establish governance structures for managing identified information security risks.

PATCH AND VULNERABILITY MANAGEMENT POLICY

This policy ensures timely information about technical vulnerabilities of information systems being used is obtained, the organization's exposure to such vulnerabilities is evaluated, and appropriate measures are taken to address the associated risk.

NETWORK MANAGEMENT POLICY

This policy ensures the protection of information in networks and their supporting information processing facilities.

BACKUP AND RESTORE POLICY

This policy aims to define the rules for taking data backups and testing the restoration.

BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY

This policy provides details to ensure that business continuity and disaster recovery requirements are planned, built, operated, and maintained at various organizational levels and departments.

VENDOR MANAGEMENT POLICY

This policy ensures that all external providers, such as vendors, suppliers, service providers, and sub-service organizations, including cloud service providers, are introduced, maintained, and controlled through defined processes.

Version Details

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