Elevaite365

Secure Development and Maintenance Policy

Version 1.0

PURPOSE

This policy and procedure aim to define and incorporate appropriate security controls when acquiring, developing, and maintaining business information systems in Elevaite365 (herein referred to as organization) information processing environment.

SCOPE

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

DEFINITION

Following is an explanation of various terms used within this document

Information System: This is an integrated set of components for collecting, storing, and processing data and providing information, knowledge, and digital products. Business firms and other organizations rely on information systems to carry out and manage their operations and interact with their customers and suppliers.

Application Software: Application software is commonly defined as any program or number of programs designed for end-users. People often use the term “application software” to talk about bundles or groups of individual software applications, using a different term, “application, proparticularrefer to individual applications.

Software Development: It is the process of conceiving, specifying, designing, programming, documenting, testing, and bug fixing involved in creating and maintaining applications, frameworks, or other software components.

Software Testing is a process of evaluating the functionality of a Software application with the intent of finding whether the developed software meets the specified requirements and identifying defects to ensure that the product is defect-free in order to produce a quality product.

Security Testing: It is a process intended to reveal flaws in the security mechanisms of an information system that protect data and maintain functionality as intended. Typical security requirements may include specific elements of confidentiality, integrity, authentication, availability, authorization, and non-repudiation. It is a type of Software Testing that uncovers vulnerabilities, threats, and risks in a software application and prevents malicious attacks from intruders. The purpose is to identify all possible loopholes and weaknesses of the software system that might result in a loss of information, revenue, and reputation in the hands of the employees or outsiders of the Organization.

Vulnerability Assessment (VA) is the process of defining, identifying, classifying, and prioritizing vulnerabilities in computer systems applications and network infrastructures. It provides the organization conducting the assessment with the necessary knowledge, awareness, and risk background to understand the threats to its environment and react appropriately.

Penetration Test: PT – A penetration test is an authorized simulated cyberattack on a computer system performed to evaluate the system’s security. The test is performed to identify both weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system’s features and data, as well as strengths, enabling a full risk assessment to be completed. A penetration test target may be a white box (which provides background and system information) or a black box (which provides only essential or no information except the company name). A gray box penetration test is a combination of the two (where limited knowledge of the target is shared with the auditor)

Segregation Of Duties: SOD - It refers to the principle that no user should be given enough privileges to misuse the system on their own. The principle of separation of duties involves assigning different tasks of a process to more than one individual such that no one employee can solely initiate, record, authorize, and reconcile a transaction without the intervention of another.

Input validation is the process of testing input received by the application for compliance with a standard defined within the application.

Non-Repudiation— Non-repudiation is the assurance that someone cannot deny the validity of something. It is a legal concept widely used in information security and refers to a service that provides proof of the origin and integrity of data.

LT: Leadership Team

ISG Team: Information security group

RESPONSIBILITIES

1. The primary responsibility for implementing this policy lies with the IT/Security/Relevant Team.
2. The IT/Security/Relevant Team will implement this Policy under the guidance of the Leadership Team and in coordination with Department Heads.

POLICY

SECURE DEVELOPMENT AND MAINTENANCE

SECURITY REQUIREMENTS FOR INFORMATION SYSTEMS

1. Information security requirements for new information systems or enhancements to existing information systems must be documented according to the change management process.
2. New projects should consult the ISG and IT/Security/Relevant Team for guidance on information security requirements.
3. A review of potential information security controls that can be implemented for risk reduction should be considered during the requirements stage of development, such as:
    - Encryption
    - Authorization Processes
    - Segregation of Duties
    - Network Security
    - Input Validation
    - Non-repudiation
4. A vulnerability assessment/penetration test must be performed before new software is released to production to identify any additional security requirements that need to be addressed.

SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

1. System environments (development, test, production, etc.) must be segregated.
2. Systems must not be developed in the production environment; each developer has their development environment where possible.
3. Feature changes, production support, and emergency changes must follow the change management process.
4. Where software development is outsourced, the projects must address the following points:
    - Developers' security approach should be gathered during the selection process.
    - A Consulting Agreement, or equivalent agreement approved by the Legal team, must be in place.
    - The developer should know the relevant organization's policies, procedures, and engineering best practices.
    - The development team must do an architectural review.
    - A security assessment of the software design must be done.
    - A vulnerability assessment/penetration test must be done to confirm the developed software meets the security requirements defined for the design.

SYSTEM SECURITY AND ACCEPTANCE TESTING

1. Peer review is required for all software developed by the organization
2. Software testing and static code analysis must be performed before deployment.
3. New information systems (including wholly and entirely new systems) must undergo suitable acceptance tests before production.
4. No personal, confidential, or operational information is used during testing.
5. The management/ IT/Security/Relevant Team is responsible for ensuring the validity of all software released to the production environment.
6. A penetration test is required before new applications and changes to customer-facing websites are released to production.

RESTRICTIONS ON SOFTWARE PACKAGE CHANGES

1. Wherever possible, vendor-supplied software packages should be used without modifications.
2. Where it is essential to modify a vendor-supplied software package, the following considerations must be made:
3. The possibility of obtaining the required changes from the vendor as standard program updates.
4. The vendor's consent must be obtained in advance.
5. The associated risks and potential impact must be obtained in advance. Al-thorough languages must be fully tested, controlled, and documented.

RELEASE MANAGEMENT

Operating systems and application software must be subject to strict change management control. Significant changes with new code and maintenance windows for production must follow the Release Management Process. The following items should be formally documented as part of the change and release management process:

1. Proper identification and recording of significant changes
2. Planning and testing
3. Assessment of the potential impacts, including Security impacts of changes
4. Formal approval
5. Communication of change details to all relevant persons
6. Fallback procedures for recovering from unsuccessful changes and unforeseen events.

Version Details

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