# INFORMATION SECURITY POLICY

## 1. PURPOSE

The Company's Information Security Policy has been prepared to inform all employees, suppliers, business partners, and stakeholders about the Company's needs, scope, objectives, goals, principles, and fundamentals related to information security, as well as their roles and responsibilities in this context.

## 2. SCOPE

This policy covers the Company's data and information, including the scope and objectives of information security, its principles, management support, risk management framework, continuity, roles and responsibilities, compliance requirements, and the sanctions to be applied in the event of violations.

## 3. ROLES AND RESPONSIBILITIES

The Information Security Management Representative is responsible for ensuring the continuity and up-to-dateness of the Information Security Policy. Any updates to the policy are incorporated into the document by the Information Security Management Representative.

The roles and responsibilities of relevant parties are detailed in the "Information Security Roles and Responsibilities Procedure."

All unit managers are responsible for the continuous review and improvement of systems under their control, and all employees are responsible for using and implementing the most current version of the document. Details of the information security requirements and rules outlined in this policy are regulated by the information security procedures. Company employees and third parties are obliged to be familiar with and act in accordance with these procedures.

## 4. DEFINITIONS

| | |
|---|---|
| **ISMS** | **:** Information Security Management System |
| **QMS** | **:** Quality Management System |
| **Company** | **:** Everhub Bilişim Teknolojileri LTD. ŞTİ. |
| **MS** | **:** Management System |

## 5. RELATED DOCUMENTS / REFERENCES

- TS EN ISO 27001 Information Security Management System Standard
- TS EN ISO 9001 Quality Management System Standard
- Master Document List L.01
- PRO.02_Work Discipline and Conduct Procedure

## 6. INFORMATION SECURITY POLICY

In line with applicable national, international, and sectoral regulations, the Company adopts the following principles to ensure information security, maintain compliance with relevant legislation and standards, and fulfill its corporate responsibilities:

- Implements infrastructure and controls to ensure the confidentiality, integrity, and availability of information.
- Promotes employee awareness of information security and integrates it into the corporate culture
- Takes technical and administrative measures to protect the privacy of personal data
- Establishes authorization and approval mechanisms in accordance with the principle of segregation of duties
- Enforces access control in line with the “need to know” and “least privilege” principles
- Ensures network security against external threats
- Physically and logically separates development, testing, and production environments
- Builds and maintains a layered security architecture
- Ensures verifiability of services using technical methods
- Secures encryption keys
- Protects sensitive data on mobile devices
- Periodically assesses information security risks and prepares action plans
- Establishes an organization to manage information security activities in an integrated structure
- Identifies information assets, defines ownership, and manages associated risks
- Detects, reports, and takes preventive measures against information security incidents
- Controls access to information through physical and environmental security measures
- Integrates security requirements into acquisition, development, and maintenance processes of systems
- Ensures uninterrupted access to information through business continuity plans
- Continuously improves security controls by following current technologies
- Monitors, evaluates, and enhances ISMS effectiveness through internal and external audits

## 7. INFORMATION SECURITY OBJECTIVES AND GOALS

The Information Security Policy aims to guide the company’s employees, suppliers, representatives, business partners, and stakeholders to act in accordance with the company’s security requirements, to raise their level of awareness and consciousness, and thereby to minimize potential risks within the company, to protect the company’s reliability and corporate image, to ensure compliance with contractual requirements established with third parties, to implement technical security controls, and to ensure the continuity of the company’s core and supporting business activities with minimal interruption. In this context, the policy seeks to protect all physical and electronic information assets of the company against internal and external, intentional or unintentional threats that may arise throughout the course of operations.

## 8. INFORMATION SECURITY ORGANIZATION

The company management  establishes an information security organization within the company. Within this scope, the development, maintenance, and management of security policies through a holistic approach are carried out within the Information Security Management Process. Roles and

responsibilities for coordinating and managing the company's security control processes are defined within the "Information Security Roles and Responsibilities Procedure."

## 9. RISK MANAGEMENT FRAMEWORK

The approach to risk assessment in relation to information security is defined by the Information Security Management Representative and described within the Information Security Management Process.

This approach outlines the methods used to identify information security risks, how risk levels are calculated, and how risks are evaluated.

Risk identification, classification, treatment, and review activities are carried out in accordance with the defined risk assessment methodology.

As a result of the risk assessment, an "Information Systems Risk Assessment Report" is prepared, including action plans to mitigate the risks.

## 10. VIOLATION OF POLICY AND SANCTIONS

In the event of a violation of this policy, one or more of the following sanctions may be applied in accordance with the Work Discipline and Conduct Procedure: warning, reprimand, salary deduction, notification to legal authorities, and termination of contract.

## 11. REVIEW, PUBLICATION, AUDIT, AND REPORTING

Changes in regulations or information security implementation processes require the policy to be reviewed. The reviewed and updated policy is approved by the General Manager. Once approved, the policy is published in the "ISMS" folder on the shared file server accessible to all employees.

This procedure is audited at least once a year under the responsibility of the Quality Management Representative, within the scope of delivering services in line with a security oriented approach.

| **Document Revision Information** | | |
|---|---|---|
| **Change Made** | **Date** | **Revision No:** |
| Creation of the Information Security Policy | 25.05.2025 | 01.0 |