# Information Security Management System

## 1. Introduction

"Tbilisi Electricity Supply Company 'Telmico'" provides electricity supply to the population of Tbilisi. The company was established as a result of reforms in Georgia's energy market and has been serving 719,000 subscribers in Tbilisi since July 1, 2021. We place significant emphasis on protecting the rights of our customers.

'Telmico' is a subject of Georgia's critical information systems, for which purpose an Information Security Management System (ISMS) has been implemented.

The Information Security Public Policy represents a set of policies adopted by 'Telmico', implemented processes, and best practices that ensure high standards of protection for information assets and the security of our customers' data."

## 2. Purpose

The objectives of this policy are:

- To provide a structured description of Telmico's Information Security Management System (ISMS);
- To define and regulate information security management processes within Telmico;
- To inform interested parties about information security requirements;

***Note:*** *This document describes general practices implemented at Telmico and, due to its interests, does not specify particular tools used to mitigate information security risks.*

## 3. Definitions of Terms

The following information security terms and their definitions are used:

- **ISMS** – Information Security Management System, including policies, processes, and control mechanisms to ensure information security.
- **Confidentiality** – Access to data only by authorized persons.
- **Integrity** – Maintaining the accuracy and reliability of data.
- **Availability** – Timely and continuous access to information for authorized users.
- **Risk Management** – A set of processes used to identify, assess, and treat information security risks.
- **Residual Risk** – Risk remaining after risk treatment.
- **Physical Security** – Security measures protecting physical assets, data centers, and devices.

- **Access Control** – Processes defining who, when, and how can access IT systems and data.
- **Authentication** – Process ensuring verification of a user or system identity (e.g., password, biometrics, multi-factor authentication).
- **Authorization** – Process determining whether a user is permitted to perform specific actions.
- **Data Classification** – Categorization of information based on its criticality and protection requirements (e.g., public, confidential, secret).
- **Encryption** – A method of encoding data using cryptography to ensure access only by authorized individuals.
- **Information Security Incident (hereinafter "Incident")** – Any event that threatens information security (e.g., data breach, DDoS attack, unauthorized access).
- **Incident Management** – Process ensuring timely detection, effective response, investigation, and resolution of incidents.
- **SIEM (Security Information and Event Management)** – A system that collects and analyzes logs and incidents from servers, networks, and security systems.
- **Third-Party Risk** – Risk associated with services and/or products provided by partners, vendors, or other legal or natural persons.
- **Business Continuity** – Processes ensuring uninterrupted operation of Telmico during crises.
- **Third Party** – Any organization or individual not directly involved in Telmico's internal operations but participating in or influencing its processes, services, or information. This may include external vendors, partners, or service providers trusted by Telmico.

## 4. Information Security Management System (ISMS)

To manage information security, Telmico has established an Information Security Working Group, composed of heads of various structural units. Daily information security processes are the responsibility of the Information Security Manager.

The following core processes are implemented at Telmico:

a) Inventory of information assets
b) Information security risk assessment and action planning
c) Daily monitoring of information security controls
d) Security risk assessment in new projects
e) Access review processes for key information systems
f) Information security awareness activities for employees
g) Access control and others

All necessary policies and procedures related to information security management are documented and communicated to employees as required.

Confidentiality and personal data protection considerations are incorporated in interactions with employees and third parties.

## 5. Network Security

Effective network security management in accordance with the ISMS includes various control mechanisms aimed at ensuring confidentiality, integrity, and availability (CIA) of information.

The following controls are implemented:

a) The internal network is segmented – user and server subnets are separated, and communication between them is conducted via firewall.
b) The external network perimeter is protected by commercial, vendor-supported NG Firewalls with IPS/IDS, Antivirus, and URL Filtering functionalities, configured according to internal policies and identified risks.
c) Employees access internal server resources remotely via corporate VPN from corporate laptops.
d) Network device logs are centralized in a SIEM system and monitored daily by a cybersecurity specialist.
e) TLS 1.2/1.3 encryption is used for network communications.
f) Periodic updates of network device operating systems are performed to address critical vulnerabilities.

## 6. Identity and Access Management Process

The purpose of identity and access management is to ensure that only authorized users, systems, and applications have access to Telmico's IT resources, and only at the minimum level required to perform their functions.

This process supports the protection of confidentiality, integrity, and availability (CIA) of information assets.

Critical business applications include systems used for both software development and administrative operations.

Each user has an individual username and a complex password compliant with Telmico's password policy, which must be changed periodically.

Telmico has implemented a comprehensive onboarding/offboarding process, ensuring appropriate access provisioning for employees and timely revocation of access for departing employees to minimize unauthorized access risks.

Access rights are reviewed at least annually by the Information Security Manager.

Each system has designated responsible persons ensuring access provisioning and revocation in accordance with the principle of least privilege.

A background check is conducted before hiring employees to assess their qualifications and relevance to job requirements and business processes. Where necessary (e.g., developers), technical tests are conducted.

## 7. Change Management Process

Change Management is a critical process for managing IT, business operations, and security. Its objective is to ensure that changes are implemented securely, in a structured and controlled manner, minimizing risks and maintaining operational stability.

Two types of changes are defined at Telmico:

a) Infrastructure changes in IT systems
b) Changes related to software development

A unified system is used for source code storage and version control, with access restricted based on roles and responsibilities.

The software development process includes:

a) **Test Environment** – where applications are tested before deployment
b) **Production Environment** – where stable and compliant applications are deployed

During the testing phase, business analysts and application testers are involved and responsible for ensuring code security and proper functionality.

## 8. Work Environment Security

The following controls are implemented to ensure a secure working environment:

a) Antivirus protection
b) Restriction of privileged access

c) Restriction of access to external storage devices
d) Use of complex passwords
e) Multi-factor authentication
f) Patch management process
g) Restriction of access to unnecessary web resources
h) VPN access for remote connectivity (limited and only when critically necessary)

## 9. Vulnerability and Patch Management

Telmico has implemented:

a) An automated vulnerability management system for regular scanning and reporting of critical systems
b) An automated patch management system covering downloading, testing, and installation of updates for servers and user computers

## 10. Physical Security

Telmico's head office is located at: Tbilisi, 0186, 10 Otar Chkheidze Street. Service centers are located in six different districts of Tbilisi.

The following physical access controls are implemented:

a) Magnetic card access systems at perimeter and office areas
b) Turnstiles
c) Security personnel
d) Continuous video surveillance monitoring

Data processing centers include:

a) Fire suppression system
b) Cooling system
c) Uninterruptible power supply (UPS)
d) Generator
e) Physical access control using magnetic cards and biometric authentication, with continuous monitoring
f) Video surveillance with continuous monitoring
g) Security personnel

## 11. Application Security

Application security is a critical component of software developed by Telmico.

Key principles applied during software development:

a) Compliance with OWASP Top 10 – protection against common threats (SQL Injection, XSS, CSRF, etc.)
b) Encryption – protection of data in transit
c) Zero Trust Authentication – access granted only to authenticated and authorized users
d) DevSecOps approach – security integrated into CI/CD pipelines

## 12. Personal Data Protection

Telmico is subject to the Law of Georgia on Personal Data Protection.

Telmico has a Data Protection Officer and a Personal Data Protection Policy available to all employees.

Employees are informed about:

a) What data is processed about them
b) The purpose of processing
c) Their rights as data subjects
d) Data retention periods
e) Third parties receiving their data and purposes
f) Security measures implemented to protect their data

A video surveillance policy has been developed, and appropriate signage is placed around the building perimeter.