Security Measures Document

Revised Edition – September 2025

OBLIGATIONS OF USERS WITH ACCESS TO PERSONAL DATA

- Access only the data necessary for the performance of their work duties.
- Do not destroy or alter data without authorization.
- Do not copy or disclose data to third parties without authorization.
- Report and correct errors in data.
- Safeguard and do not disclose the assigned username and password. These credentials must not be used outside the company’s premises.
- Do not transmit data over the Internet without authorization.
- In customer service departments, do not disclose personal data without authorization. In all cases, verify the identity of the person requesting the data.
- If documents are printed on paper, do not allow access by unauthorized persons.

ORGANIZATIONAL MEASURES

Information Security Management

Security Policy

There is an established security policy, consisting of this document and the following:

- Rules for the use of information systems and resources.
- Security breach management procedure.
- Contingency plan for processing systems and services.
- The following documents for compliance with security measures:
- Confidentiality and security commitment.
- Password receipt document and definition of access profiles and permissions.
- Portable equipment delivery document, where applicable.

Roles and Responsibilities

A security officer and the persons responsible for the resources that process personal data have been appointed.

Access Control Policy

Each user or process accessing the system has a unique identifier, allowing it to be known who accesses the system, which access rights are assigned, and what actions have been carried out.

When a user has different roles within the system (for example, as a citizen, internal employee, or system administrator), a separate unique identifier is assigned for each role, ensuring that privileges and activity logs are clearly differentiated.

User accounts are associated with a unique identifier and are disabled when the user leaves the organization, ceases to perform the function for which the account was required, or when the authorizing person orders otherwise. Accounts are retained for the necessary retention period to meet traceability requirements for associated activity logs.

Access rights to each resource are established according to decisions made by the resource owner and are periodically reviewed to ensure that granted permissions are appropriate to each user's profile.

User access rights are assigned according to the principles of:

- Least privilege, limiting access to the minimum strictly necessary.
- Need to know, restricting access to information required to perform duties.
- Authorization capacity, whereby only the competent authority may grant, modify, or authorize access.
- At a minimum, the following functions are segregated: development, configuration and maintenance, and auditing.

RESOURCE MANAGEMENT AND CHANGE MANAGEMENT

An up-to-date inventory of all assets associated with personal data and information processing resources is maintained, detailing their nature and identifying the person responsible for decisions relating to each asset.

All changes announced by manufacturers or suppliers are analyzed to determine whether they should be implemented.

Before deploying a new or patched version into production, it is tested on a non-production system to verify correct operation and ensure that it does not reduce the effectiveness of functions required for daily work.

The test environment is equivalent to the production environment in the aspects being verified. Changes are planned to minimize the impact on affected services.

A list of applications requiring regular updates is maintained, along with procedures and alerts to analyze, prioritize, and determine when security updates, patches, improvements, and new versions should be applied, as well as a record of installed updates and patches.

PERSONNEL MANAGEMENT

Duty of Confidentiality and Security

All personnel with access to personal data are aware of their information security obligations and sign a confidentiality, security, and data protection agreement.

Training and Awareness

Necessary actions are taken to regularly raise staff awareness of their role and responsibility in ensuring that system security meets required levels.

Staff receive regular training relevant to their functions, particularly regarding system configuration, incident detection and response, and the storage, transfer, backup, distribution, and destruction of media containing personal data.

INCIDENT RESPONSE AND BUSINESS CONTINUITY

Incident and Security Breach Management

In the event of a security breach, the responsible party must assess whether it involves the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

All employees must inform the data controller of any personal data security breaches so that they may be reported to the competent data protection authority and, where applicable, to the affected data subjects, in accordance with the guidelines set out in this document. Independently of breach notification obligations, appropriate mechanisms for incident logging, documentation, and management must be implemented.

Business Continuity Plan

In the event of an incident involving accidental or unlawful destruction, loss, or alteration of personal data affecting critical systems or processes, a continuity or contingency plan has been defined to restore normal operations within a reasonable timeframe and ensure business continuity.

TECHNICAL MEASURES

ACCESS CONTROL MECHANISMS

User Identification and Authentication

Access control to any system resource for performing specific actions is enforced through identification and authentication.

System resources are protected by mechanisms preventing their use unless sufficient access rights are granted.

Access rights are established according to decisions made by the resource owner, in compliance with system security policies and regulations.

Credentials or passwords are activated once they are under the exclusive control of the user, following acknowledgment of receipt and acceptance of custody and confidentiality obligations, and immediate reporting in case of loss.

Passwords must be changed at least annually and are revoked when the user, device, or process terminates its relationship with the system.

The number of permitted login attempts is limited, blocking access after three consecutive failed attempts.

Minimum password requirements include:

- At least eight characters.
- A combination of alphabetic and numeric characters.
- Passwords must be changed at least every six months and the last three passwords may not be reused.
- Passwords must not be written down in visible locations.

Staff changes require changing passwords for all systems, services, and devices to which departing staff had access.

Administrator accounts are managed by the security officer and passwords are changed whenever they must be disclosed to technical personnel for justified reasons.

ACCESS MONITORING

User Activity Logging

User activities within the system are logged, recording who performs the activity, when it is performed, on which information, and whether actions succeed or fail. Logs also include activity by operators and administrators insofar as they access configuration or maintenance functions.

Activity logs are reviewed to detect abnormal patterns.

DATA SECURITY

Protection Against Malicious Code

Preventive and reactive mechanisms against malicious code (including viruses, worms, trojans, spyware, and malware) are implemented and maintained in accordance with manufacturer recommendations, using a comprehensive security suite providing antivirus, antispam, anti-phishing, and, where possible, anti-ransomware protection. Free antivirus software is never used, multiple antivirus solutions are not installed simultaneously, and all systems are properly installed, updated, and fully enabled.

Pseudonymization

Special categories of personal data are pseudonymized so that they cannot be attributed to a data subject without additional information stored separately.

COMMUNICATIONS SECURITY

Secure Connection

The router is configured as follows:

- Default configuration access credentials are changed.
- Connection activity is monitored.
- Only essential ports are kept open.

Default wireless network settings are modified, enabling encryption on routers and access points using WPA security protocols and strong access passwords.

Firewall

A firewall is installed and configured with more restrictive settings than default, remaining active at all times.

Encryption of Communications

When special categories of personal data (e.g. health data) are communicated to third parties, data is encrypted to prevent unauthorized access.

Network Segmentation

Access to information and incident propagation are limited by network segmentation, ensuring:

- Controlled user access to each segment.
- Controlled outbound information flows per segment.
- Segmentation may be physical or logical. Interconnection points are particularly secured, maintained, and monitored.

BACKUPS

Backup and Recovery Procedures

Backup copies are performed at least weekly to allow recovery from accidental or intentional data loss. Backup integrity and recovery capabilities are periodically tested. Backup media are labeled and recorded.

Backup copies are subject to the same integrity, confidentiality, authenticity, and traceability requirements as original data.

Off-Site Backups

Backups are stored on independent systems outside the organization’s premises.

PORTABLE DEVICES

Protection of Portable Devices

- Corporate mobile devices authorized to leave organizational premises implement specific protection measures, including:
- A device request and assignment procedure defining permitted data storage and directory structures.
- Authentication and periodic password changes.
- Prevention of remote access credentials enabling access to other organizational systems.
- User awareness on safe device usage in public areas and reporting channels for loss or theft.
- Authorization requirements for external network connections with restricted access.
- Encryption of special categories of data stored locally.
- Non-corporate mobile devices used externally implement measures ensuring separation of private and business use, data ownership renunciation, data cleansing upon termination, automatic device locking, and secure corporate network access (passwords, two-factor authentication, VPN).

SECURE DEVELOPMENT

Security Requirements for Systems and Applications

- Manufacturer specifications for installation and maintenance are followed, with continuous monitoring of vulnerability announcements. Prior to deployment, systems are configured to:
- Remove default accounts and passwords.
- Apply the principle of minimum functionality.
- Organize storage according to information classification policies.
- Disable unnecessary functions.
- Apply “security by default” principles.
- Maintain updated software license records and authorized software repositories.

INFORMATION DESTRUCTION

Reuse and Destruction of Media

Reusable media must be securely formatted to prevent data recovery. Non-reusable media are securely destroyed by shredding or incineration. Certified destruction services must be used for media containing special categories of data.

PHYSICAL SECURITY MEASURES

Protected Areas

Critical information systems are installed in dedicated secure areas with controlled and logged access.

Server Room Protection

Server rooms maintain appropriate temperature, humidity, cable protection, electrical supply, emergency lighting, and fire protection equipment. Alternative secure facilities are available when necessary.

Fixed Equipment Protection

Workstations are positioned to minimize unauthorized viewing, automatically lock after inactivity, and maintain clear-desk policies.

Storage and Transport of Media

Secure cabinets are used for storage. Media transport is logged and protected using reliable courier services and adequate packaging.

DATA SUBJECT RIGHTS MANAGEMENT

The data controller informs employees of procedures to handle data subject rights.

Rights include access, rectification, erasure, objection, portability, and restriction, with responses provided within statutory deadlines and proper documentation retained.

VERIFICATION OF SECURITY MEASURES

Risk analyses relating to security measures are conducted annually.