IT Security Policy

2innovate

Objective

The purpose of this document is to specify the minimum mandatory requirements for the proper use and protection of information, as well as to provide a framework for all activities related to IT Security within 2innovateIT.

The objective of the security policy is to protect information so that 2innovateIT's legal and contractual business obligations are met and the value of the business and its information is preserved.

The objective of IT Security is to ensure:

- Confidentiality: Prevent unauthorized individuals, entities, or processes from accessing the information.
- Integrity: Protect the information from unauthorized modification, manipulation, or reproduction.
- Availability: Ensure that all business-critical information and services are available when required to authorized users, entities, or processes.
- Non-Repudiation: Ensure that the information has been originated by a specific individual, entity or process.

Information is one of the main assets of 2innovateIT's business. All sensitive information must be kept confidential, accurate, and available in an appropriate manner to meet business needs.
Each employee must be aware of the need to secure the information and act to preserve it.

This document defines:

- Guidelines that must be followed by 2innovateIT employees. Third parties involved (suppliers, contractors, others) must also be mandatorily included in the requirements of this Policy.
- A framework for all processes and their security mechanisms.
- The classification of information and the definition of fundamental principles to secure it according to business objectives within the scope of information security.
- Minimum requirements for the management of Information, Access Control, Physical Security, Communications, Operations, and Systems Development.

2innovateIT is free to define and implement stronger security requirements and mechanisms as long as they do not contradict this Policy.
When the policy is affected by laws and/or regulations, it must be aligned to comply with them, trying, as far as possible, not to distort 2innovateIT's requirements.

This Policy must be reviewed at least annually or more frequently as defined by IT Security based on the Company's needs.

The regulatory framework must be accessible to staff and third parties involved; it defines the following levels of documents:

- Security Policy
- Standards
- Procedures/Guides/Standards

Scope

This Policy applies to every person carrying out any activity at 2innovateIT, regardless of their conditions (executive, employee, contractor, consultant, temporary worker, others).

Policy

1.1 Implementation of the security policy

It is implemented through the publication of Norms, Procedures, Guides, or Standards that are aligned with and complement the provisions of this Policy.

These documents must be made available in accessible locations for employees. The publication of these documents must be accompanied by formal notification to the responsible parties of the involved areas.

Any document published in accordance with the aforementioned guidelines becomes effective at the time of publication.

1.2 Management

To meet the objective of IT Security, it is essential that:

- The implementation of specific security mechanisms is **justified** in relation to the risks to which the information being protected is exposed.
- All employees and third parties **will be** responsible for handling the information.
- Event logs exist for transactions and changes made to the information.
- An independent review of the management and use of information is conducted.

1.2 Roles and responsibilities

1.3.1 Separation of roles and responsibilities

Certain privileged or sensitive tasks must be separated from similar ones to minimize the risk of privilege abuse and maximize the ability of those responsible for controlling the tasks of others.

Respecting the principle of segregation of duties, some roles should be performed by different individuals or groups, such as access administration or control over operating systems, normal use of systems and applications, auditing, and security management.

1.3.2 Data Owner

2innovateIT's operations rely on various data sets or information groups, which are managed across different sectors or business units. Each information group must have a designated data owner, appointed by IT Security.

1.3.3 Users

Employees must be regularly informed about the existing regulatory framework and receive training as necessary.

Security awareness should be conducted through multiple communication and education methods (e.g., posters, web-based training, meetings, etc.).

A cybersecurity awareness program, managed by IT Security, must be created and maintained and should be delivered at least once a year.

1.3.4 Third Parties Involved

Third parties must adhere to the guidelines established by this Policy.

1.3.5 IT Security

This department has the following responsibilities:

- Resolve potential conflicts between the regulatory framework and the country's legislation or customer regulations.
- Coordinate activities and investigations related to system incidents.
- Manage the awareness program.
- Continuously evaluate new vulnerabilities and maintain a reasonable level of security for the assets being protected.
- Advise on security-related aspects when considering the selection of contractors.
- Monitor the daily implementation and use of system mechanisms, including access to information.
- Manage user accounts and handle authentication for information systems.

1.3.6 Audit

Evaluate whether the consistency of the implemented security mechanisms aligns with the security design and requirements. These controls cover the entire organization.

1.4 Risk Analysis and Information Classification

A proper risk analysis and classification must be performed, identifying threats and vulnerabilities related to information. This analysis must be conducted at least annually.

Some risk evaluation methodologies to consider include ISO 31000, NIST SP 800-30, among others.

1.5 Access Control

The IT resources provided by 2innovateIT to users are intended for use in daily business activities. 2innovateIT reserves the right to access all equipment and systems used in its operations for operational support and/or asset protection purposes.

1.5.1 Business Guidelines for Access Control

Information systems and networks must have defined and implemented security mechanisms to provide an appropriate level of protection for the information they handle.

User access to systems or applications must be authorized, and the user's identity verified by at least their direct superior or a company manager.

Operational audit mechanisms are used to control the utilization of access rights to applications and ensure that the access level granted is consistent with each user's role.

1.5.2 User Access Management

All IT resources are provided for business use within 2innovateIT and must be used accordingly. Personal use is permitted if it complies with the restrictions outlined in this Policy, such as:

- Conducted outside working hours so as not to interfere with productivity.
- Does not consume resources that compete with production (e.g., Internet bandwidth).
- Does not incur costs for 2innovateIT (e.g., communications, paper, magnetic media, etc.).
- Does not pose a legal risk to 2innovateIT (e.g., copyright violations).

1.5.3 Access Control for Operating Systems and Applications

Access to information systems must be controlled and restricted to authorized users to minimize the risk of unauthorized access. Application security devices must be able to identify and verify the identity of each authorized user using authentication mechanisms defined by IT Security.

1.5.4 Monitoring System Access and Usage

Adequate monitoring must be implemented to ensure that all security-related events are identified and corrected. Monitoring activities must comply with the privacy regulations and legislation in place at each of the locations where 2innovateIT operates.

System access must be logged and monitored to ensure compliance with access regulations.

1.6 Physical Security of Information

All IT resources critical to the continuity of 2innovateIT's operations must be physically secured.

Physical access to network and communication infrastructure must be restricted to authorized employees.

Whenever staff leave their office or desk, they must ensure that no confidential information or other sensitive materials are left unprotected.

1.7 Protection Against Malicious Software

IT Security must provide or control appropriate tools to protect computing devices against malware threats. Users must follow security practices to minimize risks, such as not using unauthorized software or opening emails from unknown or suspicious sources.

1.8 Information and Software Exchange

1.8.1 Business Email Usage

2innovateIT's email systems must be used for business purposes. Personal use is permitted as long as:

- It does not consume significant resources.
- It does not hinder any business activity.

Employees are prohibited from using any non-2innovateIT email system to send or receive business-related information.

All emails sent from 2innovateIT must comply with this policy, local legislation, and the company's content standards.

Confidential or strictly confidential information must not be sent by email unless it is encrypted according to approved standards.

1.8.2 Instant Messaging

Instant messaging must be conducted through Google Hangouts, which is PCI-DSS certified.

1.8.3 Communication Monitoring

IT Security reserves the right to monitor any electronic traffic as part of its normal operational activities, within the framework of applicable legislation.

1.8.4 Internet

Employees of 2innovateIT may be provided with Internet access to assist them in their work.

Internet usage must be specifically focused on tasks relevant to the employee's role within the company. Personal use is permitted within reasonable limits and provided that accessed sites are neither illegal nor inappropriate for a well-controlled work environment (e.g., pornography, gambling, drugs, etc.).

Access to resources other than web pages is reserved for authorized users. Downloading electronic files from the Internet is not permitted unless necessary for the user's work.

1.8.5 File Transfer

Sensitive information must not be sent via any file transfer mechanism unless it is encrypted according to 2innovateIT's standards.

1.8.6 Remote Access

Remote access by 2innovateIT staff to the company's resources outside the internal network must be carried out through an authorized Remote Access mechanism.

1.9 Production Release

Software must be released into production in a controlled manner. All production systems must have versioning and proper change control.

Key tasks and responsibilities in the production environment must be segregated to ensure appropriate opposition of interests and minimize the risk of privileged function abuse.

All third-party software must be sourced from trusted sources and used strictly according to the license terms. Intellectual property rights of software must be respected and observed in all cases.

1.10 Software Development

The development and maintenance of software used at 2innovateIT must follow the security standards defined by the company.

Development and production environments must be segregated. Any access between these environments must be granted under exceptional circumstances, be temporary, justified, and logged.

Developments go through different stages before going into production.

1.11 Network Connectivity

2innovateIT's networks must be protected against unauthorized access.

All 2innovateIT networks must be classified as trusted or untrusted based on their level of security.

All communications between internal and external networks (e.g., Internet) or between network areas with varying security classifications must be safeguarded using security devices.

1.12 Incident Response

IT Security must respond to situations or events where systems have been or could be compromised. IT Security must have the capability to detect intrusions, conduct tracing tasks, and perform forensic analysis on the IT systems where incidents have occurred.

1.13 Continuity of Processing

Risks threatening the continuity of critical information processing for business operations must be analyzed, and preventive controls and recovery plans must be implemented to reduce these risks to acceptable levels.

System operation continuity must be ensured through an appropriate Contingency Plan.

1.14 Use of Critical Technologies

When using critical technologies, the following aspects must be considered:

- All assets must be inventoried and accepted/approved by the organization.
- Secure authentication must be in place for the use of critical technology.
- A responsible person must be designated for handling or using the asset, if needed.
- Automatic session disconnection for remote access technologies must be required after a specific period of inactivity.
- The activation of remote access technologies for vendors and business partners must only occur when necessary, with immediate deactivation after use.

- Cloud environments do not require virtual removable media drives to be activated on their systems, and these must remain deactivated.

1.15 Database Encryption

The company's policy is to encrypt confidential data at the database level with secure encryption and proper key management.

1.16 Supplier Policy

Suppliers accessing the company's assets must comply with at least the following security policies:

- Have a confidentiality agreement or confidentiality clause in the contract.
- Be PCI certified or agree to reviews/audits if necessary.
- Be responsible for reporting any security incidents.
- Be liable for reputational or financial damage to the organization caused by willful misconduct or negligence of their assigned staff.
- Provide security training to their employees assigned to the organization.

1.17 Secure Deletion Policy

A secure deletion process must be implemented for all systems to ensure that information cannot be recovered.

1.18 Update Policy

All software must be updated to its latest stable version. If a software version is not up to date due to instability or performance issues, its vulnerabilities must be identified and the impact on systems assessed.