ORGANIZATIONAL POLICY

Subject: Corporate Information Security	**Identification:** PO-SICORP-01 **Version:** 04
Board in Charge: Information Technology	**Published on:** 03/11/2025
Related Rules: CODEC, NO-SICORP-03, ISO 27001.	**Review by:** 03/11/2028

1. Purpose

The TOTVS Corporate Information Security Policy aims to establish the concepts, guidelines, and minimum practices to be followed by all TOTVS Business Units, including new acquisitions and integrations, to ensure the protection of data and information belonging to its businesses, customers, Partners, and the general public.

This document was strategically created to promote the management of information security at TOTVS. Compliance with this policy is mandatory and essential to ensure the confidentiality, integrity, and availability of information maintained and processed by TOTVS.

This Policy clearly demonstrates the commitment of the Company's Statutory Board of Directors and Directors to safeguarding information under the Company's custody, complying with all applicable laws and regulations governing its business in every aspect, as well as the commitment of our Business Units to understand and meet our customers' specific needs.

2. Scope

This Policy applies to all TOTVS employees, suppliers, and Partners, except for the Techfin (and its subsidiaries) and Dimensa (and its subsidiaries) affiliates, which maintain independent Corporate Governance and follow their own Policies, provided these do not conflict with this Policy. Compliance with this Policy is mandatory and reflects applicable laws and regulations related to topics concerning Data Protection and Information Security legislation.

All TOTVS Business Units must implement measures to ensure that employees and, when necessary, Partners, customers, and Suppliers have access to and acknowledge awareness of the guidelines outlined in this policy. It is also the responsibility of the Business Units, when necessary, to ensure the execution of appropriate confidentiality and non-disclosure agreements for contracts entered into with employees, Partners, and Suppliers who have access to data and information owned by, or under the custody and responsibility of, TOTVS.

3. References

- General Personal Data Protection Law (LGPD) – Law No. 13.709/2018.
- ABNT NBR ISO/IEC 27001 – Information Security Management System.
- ABNT NBR ISO/IEC 27701 – Requirements and Guidelines for Information Privacy Management.
- ABNT NBR ISO/IEC 27017 – Information Security for Cloud Computing Services.
- ABNT NBR ISO/IEC 27018 – Information Security for the Protection of Personal Data in Cloud Environments.
- Copyright Law (Law No. 9.610/1998).
- Industrial Property Law (Law No. 9.279/1996).
- CMN Resolution No. 4.893/2021.
- BCB Resolution No. 85/2021.
- CVM Instruction No. 505/2011.

- CVM Instruction No. 617/2019.
- CVM Instruction No. 586/2017.
- CVM Resolution No. 35/2021.
- SUSEP 638.

4. Definitions

Brazilian General Personal Data Protection Law or LGPD: Law No. 13.709/2018, which regulates Personal Data Processing activities.
CODEC: TOTVS Code of Ethics and Conduct, a document aimed at establishing the ethical principles and rules of conduct that guide the TOTVS's commitment towards the integrity of its internal and external relationships and business activities, applicable to all directors, officers, shareholders of the company, employees, service providers, Suppliers and Partners.
High-impact Information Security Incident: an information security incident that, by compromising one or more security pillars, threatens business continuity, legal compliance, or the strategic survival of the organization, resulting in severe and unacceptable financial or reputational harm according to the risk scale defined by the company.
Employees: professionals who work in TOTVS Business Units under an employment contract.
Information Assets: are the data, systems, equipment, and technology infrastructure that hold value for TOTVS and therefore require protection and management to ensure their availability, integrity, and confidentiality.
Information Security: a method of managing an organization's information by preserving properties such as confidentiality, integrity, availability, authenticity, traceability, and legality, not limited to computer systems, electronic information, and/or storage systems.
Information Security Event: an occurrence related to assets or the environment that indicates a deviation from expected behavior or a potential compromise.
Information Security Incident: one or a series of undesirable or unexpected information security events that have a significant likelihood of compromising business operations and threatening Information Security.
ISO/IEC 27001: Information Security management system standard published by the *International Organization for Standardization* and *International Electrotechnical Commission*, detailing how to manage Information Security within an organization.
Local Information Security: TOTVS Business Units or internal Areas that maintain their own Information Security structure.
Personal Data: any piece of information related to identified or identifiable individuals.
Privileged Access: refers to authorizations or access rights to systems, functions, and resources that exceed those of a standard user. An account with Privileged Access is one that is authorized to execute security-critical functions that a regular user is not permitted to perform.
Risk Management, Internal Controls, and Compliance Policy: Policy PO-GC-03, which establishes the principles, guidelines, and responsibilities to be followed in the process of corporate risk management, internal controls, and compliance, in addition to promote the culture of Risk Management and the Integrity Program throughout TOTVS.
Sensitive Data: information that, if improperly disclosed or accessed, could compromise the privacy, security, and integrity of individuals or the organization itself, including personal, financial, and strategic data.
Sensitive Personal Data: personal data on racial or ethnic origin, religious beliefs, political opinions, membership to a union or organization of a religious, philosophical, or political nature, data regarding health or sex life, and genetic or biometric data, when linked to an individual.
Third-parties/Suppliers, and Partners: service providers that operate alongside TOTVS Business Units through contracts established with Suppliers of products and services.

TOTVS Business Units: TOTVS Management and RD Station.
TOTVS or Company: TOTVS S.A., its direct and indirect subsidiaries and affiliates, except for TechFin (and its subsidiaries) and Dimensa (and its subsidiaries).
Value of an Asset or Information: measured by the value of the asset or information itself and by the potential impact it may cause to the business in the event of a violation of one or more Information Security Pillars.

5. Guidelines

TOTVS is committed to protecting the information under its responsibility, in strict compliance with applicable laws, the provisions of its bylaws, the CODEC, and other corporate policies.

This Policy clearly defines the concepts, guidelines and responsibilities regarding the security of TOTVS information, as well as the information of its customers under its custody; allows the Information Security pillars to be preserved; ensures that the processing of Personal Data and Sensitive Personal Data is in compliance with applicable laws and regulations and that Information Security risks are managed properly, ensuring the protection and reliability of information and safeguarding TOTVS' image before the market and its investors.

TOTVS recognizes the diversity of activities carried out by its Business Units. Therefore, it establishes the minimum security standards to be adopted, evaluating and applying additional controls that are valid for the different scenarios of each of them.

This Policy is supported by a set of Information Security standards and procedures established by TOTVS.

5.1. Information Security Pillars

We characterize Information Security by preserving the following pillars:

Confidentiality: ensures that access to TOTVS information, as well as that of its customers, Suppliers, Partners, and employees, is granted exclusively to authorized individuals and solely for legitimate and ethical purposes;

Integrity: ensures the accuracy and completeness of information and its processing methods, as well as the integrity of data under the company's responsibility;

Availability: ensures that the information is always available to professionals who actually require access to them, and ensures that the data are available based on the service level required by the business areas and/or contracted by customers;

Traceability: ensures the availability of audit tracks of information and processing means, through records of transactions and changes made in systems and applications, allowing the unequivocal assignment of authorship for each action;

Legality: ensures that all procedures related to information within the company are conducted in compliance with applicable laws and regulatory rules;

Authenticity: ensures that data and information are genuine and legitimate through the authentication of users and systems, enabling traceability and certifying the accuracy of information, with no manipulation or interference from unauthorized external parties or Third Parties.

5.2. Information Security in Acquired Companies and Partnerships

TOTVS, as a technology company, not only recognizes the need to establish robust and consistent Information Security standards, but also strives to implement them across all its Business Units and operations, taking into account and respecting the specific nature of each business and the applicable

regulations, including when engaging with Partners and in companies it acquires. All Business Units must follow security practices that meet operational needs and applicable legal requirements, ensuring quality and efficiency in alignment with TOTVS security policies and procedures. This alignment ensures a cohesive and effective approach to information protection in a general and comprehensive manner, promoting the integrity and resilience of operations in all units.

5.3. Risk Management – Information Security Objectives and Incidents

All TOTVS Business Units must maintain an Information Security risk management process with the objective of identifying, assessing, addressing, and monitoring risks that may affect the confidentiality, integrity, availability, and privacy of their information and assets. This process must be integrated into the company's general risk management practices and must ensure that risks are managed proactively and effectively.

Due to the nature of associated risks, all Business Units involved in the development and provision of Cloud services must maintain specific processes to identify, analyze, assess, address, monitor, and report Information Security risks that may impact the objectives of their Cloud areas. Business Units must adhere to international standards for cloud storage security, as referenced in this document.

All TOTVS Business Units must maintain a channel for reporting, as well as tools for monitoring rvents and Incidents related to Information Security, to enable the evaluation of events that may impact the business and/or the company's strategies.

All Incidents related to Information Security within the Business Units of TOTVS, once identified by the business areas, must be promptly reported to their respective Corporate Information Security areas of TOTVS Management at csirt@totvs.com.br and to the Data and AI Governance team, at dpo@totvs.com.br, when personal data is involved, in order to ensure proper registration and handling. Business Units must also maintain mechanisms for handling Incidents involving personal data, in accordance with the requirements of the General Personal Data Protection Law.

High-impact Incidents occurring within TOTVS Business Units must also be reported periodically to the Statutory Audit Committee, through the Incident report presented by the TOTVS Corporate Information Security team during regularly scheduled meetings. In case of an Incident involving personal data, the Incident must also be reported to the TOTVS Data Privacy Committee.

5.4. Identity and Access Management

All TOTVS Business Units must establish and maintain an access and identity management process that restricts access to critical resources and sensitive data exclusively to authorized individuals, based on the principles of least privilege and segregation of functions, and ensuring access levels are consistent with the need of each role. The implementation of access controls must include multifactor authentication to enhance security, as well as clear procedures for granting, modifying, and revoking permissions.

All employees and Third Parties acting on behalf of TOTVS must have a unique, personal, and non-transferable identification (physical and logical) that enables them to be identified as the person responsible for their actions.

Privileged Access must be strictly controlled and monitored, ensuring that only authorized users are permitted to access systems and sensitive data, in compliance with the principle of least privilege. Business Units must ensure frequent processes for reviewing privileged access, ensuring their timely revocation as soon as they are no longer necessary.

The responsibility for maintaining access for Third Parties, including creation, review, and revocation, lies with the manager or employee responsible for the contract with Third Parties. In matters

involving contracts with third-party companies that include multiple users, it is the responsibility of the contract manager to ensure that all related access is always appropriate to the activities performed and revoked when no longer necessary. This measure reinforces shared responsibility in Information Security management, complementing the controls implemented by the access area.

Physical access for employees, Third Parties, and visitors must be authorized and controlled through the use of efficient processes and controls that meet and ensure the protection of environments and assets according to local needs. Employees who receive Suppliers or Third Parties at Business Unit facilities must always accompany them throughout the entire visit.

All TOTVS Business Units must implement a system for continuous monitoring and verification of access activities. Access records must be maintained, protected, and regularly analyzed to detect and respond to any anomalous or suspicious behavior.

All TOTVS Business Units must perform periodic access reviews—at least annually for general access and semiannually for privileged access—for the access granted to employees and Third Parties to their systems and facilities. For systems and facilities under centralized management by TOTVS, the incorporated Business Units must remain attentive to review periods and provide all necessary support to ensure the completion of the process.

All employees must receive ongoing training on access policies and secure practices to ensure they understand their responsibilities and the security implications associated with accessing data and systems.

5.5. Information Sorting and Processing

To ensure adequate protection of TOTVS information, all Business Units must adopt an information sorting and labeling method based on the level of confidentiality and criticality for TOTVS' business:

- Information must be sorted based on its value, sensitivity, and criticality. Sorting must determine the appropriate security controls for the protection of information. Confidential and critical information must be processed with the highest levels of security and protected from unauthorized access, disclosure, alteration, and destruction;
- All information must be properly protected, in accordance with TOTVS' Information Security guidelines, throughout their entire lifecycle, which includes: generation, handling, storage, transportation, and disposal;
- The information collected must be used for the purposes previously informed or contractually defined, and may be processed for additional purposes as long as they are compatible with the applicable legal basis and duly authorized;
- Personal Data must be processed in accordance with applicable privacy laws and regulations (national and international), in addition to abiding by the guidelines set out in TOTVS' Personal Data Protection and Privacy Policy.

5.6. Information Asset Management

All TOTVS Business Units must adopt a structured and systematic approach to the management of information assets that includes their identification and sorting. These assets must be recorded in a detailed inventory, including at minimum information regarding their significance, location, and owner. The sorting must reflect the value of the asset and the potential impact of its loss, compromise, or destruction.

The maintenance and disposal of Technology assets belonging to TOTVS must be carried out exclusively by duly evaluated and approved Partners, or by formally assigned and qualified internal

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

TOTVS teams. Business Units must maintain a record of equipment check-in and check-out, as well as signed statements of consent for use by employees and Third Parties at the time the equipment is issued and collected.

TOTVS Business Units must also implement appropriate security controls to safeguard information assets, ensuring their proper use and management. This includes access restrictions, encryption, and physical protection measures for equipment, as well as the use of controls to monitor and continuously review their security. Policies, rules, and procedures must be consistently updated to identify new threats and vulnerabilities, ensuring that assets remain protected against emerging risks. Mobile media and equipment ports must be managed to prevent the risk of infection and information leakage through those means.

5.6.1. Acceptable use of TOTVS assets

All employees and Third Parties must ensure the security and protection of the information assets provided by TOTVS Business Units for the execution of their activities, in accordance with the following rules:

- Use technology assets (computers, mobile devices, systems, and data) exclusively for work-related purposes, except in situations expressly authorized by the employee's manager, the Information Security area, and the IT area responsible for the business unit, in specific and exceptional cases;
- Only use assets for which the employee has been explicitly authorized;
- Do not share access credentials with Third parties;
- Protect confidential and sensitive information. Do not disclose or store sensitive data in unauthorized locations;
- Use encryption to protect data in transit and at rest;
- Use strong, unique passwords to access systems and data. Change passwords regularly and never share credentials;
- Whenever possible, use additional authentication methods to access information and systems;
- Install only software that has been authorized, approved, and licensed by the company. Do not use unverified applications;
- Keep computers and other devices provided by TOTVS secure. Use padlocks and other security devices when appropriate;
- Store mobile and portable devices in secure locations when not in use;
- Use authorized removable storage devices only when necessary and protect them with a password and encryption;
- Store data in locations designated by the company, such as secure folders on the corporate network;
- Send sensitive data through secure and protected channels, such as encrypted emails;
- Always verify the authenticity of recipients before transmitting confidential information;
- Remain vigilant for any suspicious behavior or warning and immediately report it to technical support and/or the Information Security team;
- Follow all established policies and procedures for the use of technology. Any breach must be immediately reported to the IT department of the Business Unit;

- Report any Incident related to security or improper use of assets to your supervisor, technical support, or the Information Security team.

5.7. Cryptography

All TOTVS Business Units must assess and implement encryption practices appropriate to the value of their information assets, in order to ensure the protection of critical, sensitive, and confidential data at rest or in transit.

Encryption must be applied to all electronic communications exposed to the internet and data transmissions in order to prevent unauthorized access and to ensure that information is transmitted securely. In addition, encryption must also be employed during data processing to protect temporarily stored or handled information, ensuring that TOTVS data remains protected from undue exposure and access.

All TOTVS Business Units must establish secure processes for the management of cryptographic keys, including their generation, storage, and rotation. The selection of algorithms must be based on an ongoing evaluation of best practices and security guidelines, ensuring that only secure and approved methods are utilized.

5.8. Physical and Environmental Security

All TOTVS Business Units must implement physical security controls for their facilities and environments to ensure the integrity and security of equipment, systems, and data, including the deployment of tools for restricting physical access and monitoring of sensitive areas and facilities. All TOTVS Business Units with local data centers must also be equipped with monitoring devices, climate control systems, and fire prevention controls for the rooms. The recovery plans for these sites must be included in the Disaster Recovery Plan of these Business Units.

In addition to access security, data centers must also implement measures to protect facilities against environmental risks and establish environmental control systems for the mitigation of potential harm to TOTVS equipment and data. The electrical infrastructure must be designed to support the power requirements of critical systems, including the installation of uninterruptible power supply (UPS) devices and generators to ensure operational continuity in the event of power grid failures.

5.9. Communications Security

All TOTVS Business Units must implement security measures for the internal and external transmission of information. Electronic communications, both internal and external, must be protected from interception and unauthorized access. This includes the use of encryption protocols, firewalls, intrusion detection and prevention systems, and the continuous monitoring of networks to identify and mitigate threats in real time, ensuring that data transmitted across networks is protected from cyberattacks and data breaches. The communication of confidential and sensitive data must be carried out exclusively by means that ensure security and privacy.

Network security must be reviewed regularly to ensure that defenses remain up to date. Access to communication networks and systems should be controlled and restricted to authorized personnel, and the use of unauthorized network devices should be prohibited.

For the provision of services, all employees and Third Parties must use only communication devices and information transmission systems that have been duly approved and provided by TOTVS. Any violation of this condition may be considered an Information Security Incident.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

5.10. Backups and recovery tests

All TOTVS Business Units must establish and maintain a process for generating and testing backups of their critical data in order to protect them against loss and corruption. This includes clearly defining the types and frequency of backups, the storage and protection of backups, as well as documentation on recovery processes and test results. It is mandatory to perform backups at regular and consistent intervals, covering all essential data and critical systems belonging to TOTVS, ensuring their storage in secure, geographically separate locations to provide protection against local disasters.

Business Units should also implement a regular restore testing program to verify the effectiveness of backups. Restore tests must be documented in order to ensure the integrity of safeguarded databases. Testing frequency must be determined based on the criticality of data and systems, and the results must be reviewed to ensure the continuity of recovery processes.

5.11. Vulnerability management and monitoring

All TOTVS Business Units of must implement vulnerability scanning tools and techniques to detect and classify security flaws in systems and applications that may pose risks to TOTVS information assets. The techniques must establish processes for the identification, sorting, prioritization, and remediation of vulnerabilities. Remediation must be based on the risk and potential impact to the assets and operations of the Business Units, ensuring that critical vulnerabilities are addressed with the highest urgency and efficiency.

TOTVS Business Units must also ensure the continuous monitoring of internal and external activities that may impact the integrity and confidentiality of the systems. All TOTVS Business Units must implement monitoring solutions for intrusion detection and prevention, as well as regularly analyze collected event logs to promptly identify and respond to suspicious or anomalous activities.

5.12. Information Security in Supplier Relationships

All TOTVS Business Units must implement a risk evaluation process associated with the contracting of Suppliers who will have access to sensitive data or to critical systems belonging to TOTVS.

The evaluation must verify the adoption of appropriate Information Security practices and controls that comply with regulatory requirements and ensure the security in the execution of contracted services, guaranteeing that these Suppliers implement adequate security practices.

The process must also include ongoing verification of compliance with security standards through monitoring of services, regular audits, and reviews of security reports, as well as the adoption of secure measures for contract termination, ensuring the secure removal of Supplier access to TOTVS data and systems, and the collection of information assets provided during contract execution.

5.13. Aquisition and secure development of systems

All TOTVS Business Units must maintain a process for the secure acquisition and development of software that includes the security evaluation of Suppliers and the products offered or developed. This includes verifying software compliance with security standards, performing vulnerability testing, and reviewing the supplier's security practices to ensure software quality and security. Additionally, all contracts with Suppliers must include security clauses addressing data protection and liability in the case of security Incidents, as well as the possibility of oversight/audit during the development process, which may be replaced by the submission of information security certifications, provided that such certifications are applicable and adequately address any information security concerns.

For software development, in addition to the risk assessments considered throughout the development lifecycle, the implementation of security and privacy controls in accordance with *Privacy by Design* and *Security by Design* methodologies during development, and the execution of security

testing, all TOTVS Business Units must comply with applicable regulations and best practices relevant to the type of system being developed, including but not limited to:

- Brazilian General Personal Data Protection Law (LGPD);
- Instructions on Information Security from the Brazilian Securities and Exchange Commission – CVM;
- Copyright Law (Law No. 9.610/1998);
- Industrial Property Law (Law No. 9.279/1996);
- Consumer Protection Code;
- ISO/IEC 27034;
- NIST Secure Software Development Framework (SSDF);
- ABNT NBR ISO/IEC 27001 – Information Security Management System;
- ABNT NBR ISO/IEC 27701 – Requirements and Guidelines for Information Privacy Management.

All TOTVS Business Units must understand the legal, regulatory, and other specific needs of customers in order to develop systems that ensure not only the protection of processed information, but also its legal and regulatory compliance. Business Units must monitor scenarios in order to ensure systems are updated whenever necessary to comply with changes in the legislative environment.

5.14. Incident Management

TOTVS Business Units must maintain communication channels for reporting Incidents to provide service to employees, Third Parties, and their customers. They must establish and maintain a process for the management of Incidents related to Information Security and privacy, encompassing the identification, response, and resolution of Incidents that may compromise the integrity, confidentiality, or availability of data and systems. The process must include response plans for Incidents and clear procedures for notifying and escalating Incidents to stakeholders, as well as communicating and acknowledging the responsibilities and the appropriate communication flow.

All Incidents treated should be investigated to determine their causes and impacts, so that corrective and preventive measures can be implemented to mitigate the risk of future recurrences. Incident records and lessons learned must be reviewed and used to continuously enhance security and privacy policies and procedures.

5.15. Business Continuity Management

All TOTVS Business Units must establish and maintain a business continuity management plan to ensure the continuous operation and efficient recovery of activities in the event of critical Incidents. The plan must include the identification and evaluation of risks that may impact operations, the definition of strategies to ensure the continuity of essential processes, and the deployment of measures to minimize service disruptions, as well as the execution of tests and simulations.

TOTVS Business Units must ensure that the recovery plans for their activities take into account, when necessary, the fulfillment of return timeframes and other specific, regulatory, or contractual needs of their customers. The information required for the development of continuity and recovery plans must be assessed in conjunction with the legal and Risk Management areas at TOTVS.

5.16. Intellectual property

All TOTVS Business Units must implement measures to safeguard both their own intellectual property and that of Partners, ensuring that property rights are respected and protected against unauthorized

access, misuse, or improper disclosure. Business Units must ensure that contractual agreements with customers, Partners, and Suppliers include specific clauses for the protection of software and applications, clearly establishing intellectual property rights, safeguards against unauthorized use, copying, and modification of the software and applications provided or used in collaboration.

TOTVS strictly prohibits any form of unauthorized or unlicensed use of software and applications, and maintains controls for the management of usage licenses for all systems it operates. The identification of situations contrary to this must be treated as an Information Security Incident.

5.17. Artificial Intelligence (AI)

5.17.1. Use of Artificial Intelligence by employees and Third Parties

All TOTVS Business Units must ensure the secure and ethical use of Artificial Intelligence (AI) in their operations, implementing measures to protect the integrity, privacy, and security of data shared within these tools. Business Units must adopt practices that ensure the secure use of AI, implementing appropriate access controls to assure that only authorized users may interact with the systems, in order to minimize vulnerabilities and protect against potential information leaks and cyberattacks. All employees and Third Parties authorized to Use AI must receive proper training regarding the associated risks and the secure use of these tools.

5.17.2. Ethical and secure development of Artificial Intelligence

In AI development, all TOTVS Business Units must follow security and ethical principles to ensure that systems are designed and implemented responsibly, conducting risk evaluations and security testing to identify and mitigate potential threats prior to entry. Additionally, development must consider ethical impacts, ensuring that AI solutions do not perpetuate bias, do not invade privacy, and respect applicable regulations. To maintain trust and ensure compliance in the use and development of AI, all TOTVS Business Units must regularly review and update their AI policies. Development and usage practices must be continuously monitored and adjusted in accordance with technological and regulatory changes related to the subject.

5.18. Data protection and privacy

TOTVS is fundamentally committed to ensuring the privacy and protection of data for all its *stakeholders* (employees, Suppliers, Partners, and customers). The processing of personal data within the company is governed by our Data Privacy Program, which ensures compliance with the General Personal Data Protection Law (LGPD) and with security and confidentiality practices. For details regarding governance, guidelines, and controls, please refer to the TOTVS Data Protection and Privacy Policy.

5.19. Legal, regulatory, and contractual compliance

All Business Units of TOTVS must ensure compliance with all applicable laws and regulations related to Information Security and data protection, as well as the regulations applicable to fulfilling contractual agreements with customers.

Business Units must maintain a process to monitor, identify, and understand the specific legal and regulatory obligations for each jurisdiction in which they operate, including those related to data privacy, cybersecurity, and individual rights. Business Units must implement controls and practices that meet these requirements, conducting regular evaluations to ensure that their policies and procedures are updated and compliant with changes in legislation.

5.20. Information Security Processes Audit

Internal and external audit teams may, at any time, audit Information Security processes to ensure the effectiveness and compliance of the practices implemented by TOTVS Business Units. These audits are intended to assess compliance with security policies, identify vulnerabilities, and verify the effectiveness of established controls and procedures. The audit may be conducted by independent external or internal teams, always seeking an impartial perspective on the current state of Information Security.

5.21. Continuous Improvement

TOTVS reaffirms its commitment to the continuous improvement of Information Security processes, ensuring that policies, procedures, and controls are consistently reviewed and enhanced in alignment with best practices. This approach guarantees that practices and controls evolve in response to technological advancements and emerging security challenges, with the ongoing objective of maintaining business continuity and safeguarding against emerging threats. This commitment is demonstrated by the deployment of a systematic cycle of evaluation and update, which incorporates feedback, audit results, and lessons learned. By adopting a proactive and adaptive approach, it continuously strengthens its security posture, effectively safeguarding critical assets and ensuring organizational resilience in an environment of constantly evolving threats.

5.22. Awareness Training

All Business Units of TOTVS must plan and maintain a training and communication program that ensures the awareness of all their employees regarding Information Security policies and practices. This program must include regular and refresher training sessions, updates on new threats and procedures, and ongoing awareness campaigns to reinforce the importance of data security. Business Units must monitor the effectiveness of the program and adjust approaches as necessary to ensure that the security culture is promoted and aligned with TOTVS' culture, best practices, and regulatory requirements.

All employees and Third Parties, when applicable, must understand their individual responsibilities in safeguarding information to ensure they are prepared for the performance of their activities, as well as to identify and respond to security Incidents.

6. Assignments:

In general, all TOTVS employees and service providers should:

- Faithfully comply with this Policy, the rules and procedures of Information Security applicable to their activities;
- Complete all mandatory training provided by TOTVS Business Units;
- Protect information against any access, tampering, destruction or disclosure not authorized by TOTVS;
- Ensure technological resources, information, and systems at their disposal are used only for the purposes approved by TOTVS;
- Abide by laws and standards that govern intellectual property;
- Refrain from discussing confidential work matters in public settings or exposed areas (elevators, land and air transportation, restaurants, social gatherings, etc.), including sharing comments and opinions in blogs and social media;

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

- Immediately notify the local Information Security area of any noncompliance or violation of this Policy, as well as report any Incidents of Information Security.

Local Information Security Teams

- Ensure broad dissemination of this Policy, as well as all Information Security Standards and Procedures, to all employees and Third Parties under the company's management and oversight;
- Promote awareness initiatives on Information Security for all local employees;
- Propose and manage projects and initiatives related to Information Security management;
- Implement, manage, and monitor systems and controls under the management of the local Information Security area or, when applicable, under the Corporate management of TOTVS;
- Propose eventual changes to this Policy;
- Identify, analyze, review, process, monitor, report and register IT security Incidents;
- Register and report Incidents in the corporate environment.

Cloud Information Security Team

- Ensure the operation of the Cloud Information Security and Privacy Management System, in accordance with the guidelines of the ISO 27001, ISO 27701, ISO 27017, and ISO 27018 standards;
- Define and implement security requirements for new Cloud initiatives and projects;
- Structure and improve security services for Cloud Customers;
- Support Cloud Customers in compliance and audit inquiries, whenever possible, through self-service tools;
- Ensure the correct identification and handling of Cloud security Incidents;
- Manage accesses based on the principle of least privilege, segregation of functions and periodic revision for assets managed via Cloud;
- Map and address security vulnerabilities in the Cloud environment, in accordance with the objectives of the ISO 27001, ISO 27701, ISO 27017, and ISO 27018 certifications;
- Ensure the correct registration and traceability of actions for assets under Cloud management;
- Support, develop and improve technologies for security operation in Cloud;
- Propose eventual changes to this Policy.

IT/System Maintenance

- Notify the Information Security areas upon identifying suspicious events that may indicate the occurrence of Incidents of Information Security;
- Approve and implement security improvements recommended by the Information Security areas.

Property Security

- Manage physical access to the company's facilities.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Ethics and Conduct Committee

- Analyze events of violations of this Policy and the enforcement of consequences, when applicable, in accordance with the duties of the Statutory Audit Committee regarding the indicators of Information Security Risks.

Statutory Audit Committee

- Monitor indicators of Incidents, Risks, and events of violation of the rules of this Policy regarding the routines of the Information Security areas, reporting the findings to the Board of Directors;
- Review the information received and monitor actions regarding the occurrence of events related to Information Security issues, based on the criticality characteristics defined for them;
- Review this Policy and its revisions, and submit recommendations to the TOTVS Board of Directors regarding its approval.

Board of Directors

- Become aware, through the Statutory Audit Committee, of the monitoring of relevant Incidents, risk indicators, submitted by the Information Security area, and listen to the Audit Committee, deliberating, as necessary, in order to safeguard Information Security;
- Approve this policy and revisions hereof.

7. Management Actions

The Corporate Information Security area must ensure compliance with this Policy, referring any cases of noncompliance to the Ethics and Conduct Committee.

8. Consequence Management

In the case of noncompliance with this Policy, management measures with appropriate consequences shall be adopted to address the nonconformity, and the Statutory Audit Committee shall be informed.

9. Approvals

Name/Position	Description
Mara Maehara Information Technology Director	Development
Marcos Corradi Executive Manager of Internal Controls, Risks and Compliance	Review
Patricia Vetri Thomazelli Magalhães Fonseca Legal Officer	Review
Gustavo Dutra Bastos Vice President of Platforms & IT	Review
Dennis Herszkowicz CEO	Review
Statutory Audit Committee	Recommendation
Board of Directors	Approval