ORGANIZATIONAL POLICY

Subject: Corporate Information Security	**Identification:** PO-SICORP-01 Version: 02
Responsible Management: Information Technology Board	**Published on:** 03/05/2021
Related rules: ISO 27001, CODEC, NO-SICORP-03	**Review by:** 03/05/2024

1. Purpose

Establish the concepts, standards and guidelines of information security, in order to protect the data and information held by the TOTVS Group, as detailed below, clients, partners, suppliers and the public in general. This document was strategically created to promote the management of information security within the TOTVS Group.

Therefore, this Policy must be interpreted as the TOTVS Group management's commitment towards protecting the information in its custody.

2. Scope

This policy applies to the entire TOTVS Group, including employees, partners and employees of suppliers working for the TOTVS Group. Compliance with this Policy is mandatory and reflects applicable laws and regulations pursuant to the Brazilian General Data Protection and Information Security Act.

TOTVERS must sign the TE-SICORP-Nondisclosure Agreement and Other Covenants, and supplier employees must sign the TE-SICORP-Nondisclosure Agreement for Suppliers, upon requesting access to TOTVS environments, and undertake to comply with such instruments.

3. Definitions

CODEC: Code of Ethics and Conduct of the TOTVS Group, which establishes the ethical principles and rules of conduct that guide the TOTVS Group's commitment towards the integrity of its internal and external relationships and business activities, applicable to all directors, officers, shareholders of the company, TOTVERS, service providers, suppliers and partners;
TOTVS Group: TOTVS S.A., its directly or indirectly controlled subsidiaries and affiliates;
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;
Brazilian General Data Protection Act: Brazilian Law No. 13.709/2018, which governs Personal Data Processing activities.
Risks 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 the entire TOTVS Group.
Information Security: the manner through which an organization's information is managed. By preserving properties such as confidentiality, integrity, availability, authenticity and legality, not limited to computer systems, electronic information and/or storage systems;

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

Subject: Corporate Information Security	**Identification:** PO-SICORP-01 Version: 02

TOTVER: TOTVS' denomination in reference to its employees and interns.

4. Guidelines

The TOTVS Group is committed to protecting the information under its responsibility, in addition to complying with all laws in force, as well as its bylaws, the CODEC and other governance policies.

This policy clearly defines the concepts, guidelines and responsibilities regarding information security within the TOTVS Group, as well as the information of its customers under its custody; allows the Information Security pillars to be preserved; ensures compliance of data processing activities with applicable laws; and ensures information security risks are managed properly, guaranteeing the reliability of information and safeguarding the Group's image before the market and its investors.

4.1. Information Security Pillars

Information security is characterized by the preservation of the following pillars:

Confidentiality: ensures all information of the TOTVS Group, its customers, suppliers, partners and employees is only accessed by authorized personnel and strictly as necessary;
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.

4.2. General Aspects

The information (in physical or logical format) and technological environments of the TOTVS Group used by TOTVERS in the exercise of their professional duties are the executive property of the TOTVS Group and must be used solely for their established purposes, and never for personal use;

Customer data must be treated ethically and confidentially, in accordance with the guidelines set out in the CODEC (Code of Ethics and Conduct of the TOTVS Group) and applicable laws;

Non-anonymized customer data must only be used for the purposes for which they were authorized, in order to render contracted services;

All TOTVERS and supplier employees must be aware that the equipment and use of information and systems of the TOTVS Group may be monitored, without prior notice, and that the records obtained from such monitoring may be used as evidence to apply disciplinary measures, in the event of noncompliance with the established rules.

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

Subject: Corporate Information Security	**Identification:** PO-SICORP-01 Version: 02

The TOTVS Group is committed to adopting the most appropriate security means and techniques available regarding the security of data trafficked, processed and/or stored in the TOTVS cloud;

Only authorized personnel may access information under the TOTVS Group's responsibility;

All processes, whenever possible and throughout their entire lifecycle, must ensure the segregation of functions through the participation of more than one person of team;

Confidential information such as access passwords and any information professionals may have in their possession to carry out their professional duties must always be kept a secret. Sharing such information is strictly prohibited;

Commitments and responsibilities related to the aforementioned information security pillars must be extensively disseminated among companies of the TOTVS Group, ensuring strict compliance with the guidelines set out herein;

This Policy is supported by a set of information security standards and procedures established by the TOTVS Group.

4.3. Identity and Access Management

TOTVERS must have a unique, personal and non-transferable identification (physical and logical) to make them accountable for their actions;

The logical access of TOTVERS and supplier employees must be controlled to ensure only the information required to carry out their specific duties are available, and only upon formal approval of the line manager and/or the person responsible for the environment accessed, which must be regularly revised.

Accesses must always comply with the criterion of least privilege, in which users must have only the necessary permissions to perform their specific activities;

The physical access of TOTVERS, supplier employees and visitors in sites with technological resources of TOTVS must be authorized and controlled upon formal approval of the line manager and/or the person responsible for the environment accessed.

TOTVERS must accompany suppliers or third parties visiting the TOTVS Group's facilities at all times during their visit.

4.4. Information Processing

To ensure adequate protection of TOTVS information, an information classification and labeling method must be adopted based on the level of confidentiality and criticality for the TOTVS Group's business.

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

- The classification must be based on the following labels: Restricted, Confidential, Internal or Public, based on characteristics related to the information, as per the Standard NO-SICORP-03 - Classification and Use of Information;
- All information must be properly protected, in accordance with the TOTVS Group's information security guidelines, throughout their entire lifecycle, which includes: generation, processing, storage, transportation and disposal;
- Information must be used transparently and exclusively for the purpose for which it was collected; for statistical purposes, without identifying the customers; or for system characteristics available to the customer himself;
- Personal data must be processed in accordance with applicable privacy laws (national and international), in addition to abiding by the guidelines set out in the General Personal Data Protection Policy of TOTVS.

4.5. Information Security Risk, Objective and Incident Management

The Cloud Information Security area is responsible for identifying, analyzing, evaluating, processing, monitoring and reporting information security risks that may impact the Cloud area's objectives.

The Corporate Information Security area is responsible for identifying, analyzing, evaluating, processing, monitoring and reporting information security risks that may impact the TOTVS IT area's objectives; monitor compliance of procedures; information security standards and policies at TOTVS in general; and, upon request, help all other business areas manage their respective information security risks.

TOTVS business areas that operate and support products and systems outside the IT and Cloud areas are responsible for identifying, analyzing, evaluating, processing, monitoring and reporting information security risks that may impact the objectives of their respective areas and, as needed, may request technical support for other information security areas of TOTVS.

Whenever risks identified by the information security or business areas can potentially impact the objectives or results of the TOTVS Group and/or personal data under TOTVS' custody, they must be reported to the Internal Controls, Risk Management and Compliance area, as well as the Privacy Management area, respectively, which shall be responsible for assessing whether the identified risk is being addressed as defined in the Compliance, Internal Controls and Risk Management Policy and the General Personal Data Protection Policy of TOTVS.

Information security incidents and events must be identified through a process established by the business area to evaluate events that may impact the business and/or strategies of the company, and notified to the Corporate Information Security area, which shall coordinate Incident Response actions to adequately preserve and protect the TOTVS Group.

All Information Security incidents must be immediately reported to the Corporate Information Security area as soon as they are detected by the business areas, via the email address segurança.informacao@totvs.com.br, in order to be duly registered and reported to the Privacy Management area (whenever such incidents involve personal and/or sensitive data) and, depending on the case, also reported to the Ethics and Conduct Committee and the Data Privacy Committee.

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

4.6. Awareness Training

The TOTVS Group must carry out periodic information security awareness training with different formats to cover different audiences, including, among others: on-site training, distance learning ("EAD") and social engineering campaigns.

5. Responsibilities

All TOTVERS and supplier employees are generally responsible for the following:

- Faithfully comply with this TOTVS Policy, information security procedures and standards;
- Undergo all mandatory training provided by TOTVS;
- Protect information against any access, tampering, destruction or disclosure not authorized by the TOTVS Group;
- Ensure technological resources, information and systems at their disposal are used only for the purposes approved by the TOTVS Group;
- Abide by laws and standards that govern intellectual property;
- Refrain from discussing confidential work matters in public settings or exposed areas (land and air transportation, restaurants, social gatherings, etc.), including sharing comments and opinions in social media and blogs;
- Immediately inform the Corporate Information Security area of any case of noncompliance or violation of this Policy, via email: seguranca.informacao@totvs.com.br, in addition to reporting any Information Security incident.

Corporate Information Security

- Extensively promote and revise this Policy, as well as all Information Security Standards and Procedures among all TOTVERS and supplier employees;
- Promote awareness-raising actions on Information Security among all TOTVERS;
- Propose and manage projects and initiatives related to Information Security management at TOTVS;
- Implement, manage, and monitor systems and controls under management of the TOTVS Corporate Information Security area;
- 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

- Ensure the operation of the Cloud Information Security Management System, as per the ISO 27001 standard;
- 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 processing of Cloud security incidents;
- Manage accesses based on the principle of least privilege, segregation of functions and periodic revision for assets managed via Cloud;

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

- Map and address security vulnerabilities in the Cloud environment, as per the objectives of the ISO 27001 Certification;
- 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;
- Identify, analyze, review, process, monitor, report and register security incidents in the Cloud environment.

Privacy Management
- Define the security requirements to protect personal data and personal sensitive data;
- Define the tactics and strategies required to keep TOTVS' operations in compliance with applicable Data protection laws;
- Receive complaints and communications from Data Owners, clarification requests, and adopt corrective/preventive measures;
- Receive and make due arrangements regarding communications to the ANPD;
- Instruct TOTVERS and TOTVS contractors regarding the practices to be adopted regarding Personal Data protection;
- Reply to Personal Data Protection and Processing inquiries from business areas;
- Carry out the attributions assigned by TOTVS or established in supplementary Data Protection standards;
- Propose eventual changes to this Policy.

System Support
- Manage logical access to tools and systems under its management within the TOTVS Group;
- Notify Information Security areas upon detecting suspicious events, which may indicate the occurrence of Information Security incidents;
- Approve and apply security improvements recommended by security areas.

Property Security
- Manage physical access to TOTVS facilities.

Ethics and Conduct Committee:
- Analyze events of Information Security Policy violations reported; and apply consequences, as applicable, based on the attributions of the Audit Committee regarding Information Security Risks indicators;
- Request investigations in equipment and systems to the Corporate Information Security area;
- Forward occurrences to Managers/Leaders in charge in order for them to take proper measures;
- Propose eventual changes to this Policy.

Audit Committee
- Monitor indicators of incidents, risks and events of rule violations 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;
- Recommend eventual changes to this policy proposed by the respective areas.

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

Governance and Nominating Committee

- Review this Policy and revisions hereof, and present a recommendation to TOTVS' Board of Directors regarding its approval;

Board of Directors:

- Become aware, through the Audit Committee, of the follow-up on 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.

6. Management Actions

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

7. Consequence Management

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

8. Approvals (Document)

Name/Position	Description
Mara Maehara Information Technology Director	Development
Ricardo Guerino Director of Planning, Controllership, Internal Controls, Risks and Compliance	Review
Claudia Karpat Legal Officer	Review
Gustavo Dutra Bastos Vice President of Platforms & IT	Review
Audit Committee	Recommendation
Governance and Nominating Committee	Recommendation
Board of Directors	Approval