CORPORATE POLICY

Subject: Corporate Information Security	**Identification:** PO-SICORP-01 Version: 01
Department Responsible: Information Technology Department	**Published on:** 14/08/2019
Related standards: ISO 27001, CODEC	**Reviewed by:** 30/05/2020

1. Purpose

To establish information security concepts and guidelines in order to safeguard the information of TOTVS and its clients. It is a strategic document aimed at promoting the safe use of TOTVS' information assets. As such, it should be understood as a formal declaration by Top Management of its commitment to protecting information under its custody, and must be complied with by all employees, interns and outsourced employees of TOTVS.

2. Scope

This Policy applies to all areas of the TOTVS Group (Head Office, Own Units, Branches). Compliance with these guidelines is mandatory and reflects the corporate governance around the issues of Corporate Information Security of thee TOTVS Group.
After reading this Policy, TOTVERs, interns and executives must sign the TE-SICORP-Confidentiality Agreement and Other Covenants, and outsourced employees must sign the TE-SICORP-Confidentiality Agreement for Suppliers, to confirm that the message of the Policy was understood and will reflect in their behavior.

3. Definitions

Information Security: Its aim is to preserve the properties of confidentiality, integrity and availability, and is not restricted to computer systems, electronic information and/or storage systems.

TOTVER: Name used by TOTVS to refer to its employees.

4. Guidelines

TOTVS is committed to complying with the applicable laws in force, as well as the Bylaws and Code of Ethics and Conduct of the Company. And to carry out its business activities, it is necessary to establish a structured and clear Information Security Policy that enables adherence and compliance.

4.1. Information Security Pillars

Information security here is characterized by the preservation of the following pillars:
Confidentiality: TOTVS aims to ensure that access to information of the company and its clients is obtained only by authorized people and when access is in fact necessary;
Integrity: TOTVS aims to guarantee the accuracy and completeness of information and the methods for its processing, as well as the integrity of data of clients that are under its responsibility.
Availability: TOTVS aims to ensure that information is always available to professionals who actually have the necessary access to it and to ensure that the data is available according to the level of service agreement contracted by clients.

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: 01

Traceability: TOTVS aims to guarantee the availability of audit trails of information and processing methods through records of transactions and alterations made in its systems and applications.

4.2. General Aspects

- Information (in physical or logical format) and the technological environments used by users are the sole property of TOTVS and cannot be interpreted as available for personal use;
- Client information must be handled in an ethical and confidential manner, in accordance with the guidelines established by the Code of Ethics and Conduct of TOTVS (CODEC) and the laws in force;
- Client information must be used only for the purposes for which they were authorized;
- All TOTVERs, interns and outsourced employees must be aware that the use of information and information systems may be monitored without prior notice and that records thus obtained may serve as evidence to take disciplinary action;
- TOTVS has a commitment to clients of adopting the most appropriate techniques and security measures available with regard to the security of the data transmitted, processed and/or stored in the TOTVS cloud.
- TOTVERs must have a single (physical and logical), personal and non-transferable identification that is capable of identifying them as responsible for their actions;
- Only authorized professionals must have access to information of TOTVS and its clients;
- Whenever possible, all the processes must, during their life cycle, ensure the segregation of functions through the participation of more than one person or team;
- Accesses must always obey the principle of least privilege, by which users must have only the permissions needed to perform their tasks;
- Confidential information such as passwords and/or any information that the professionals have under their power while exercising their duty must always be held secret, and sharing it is expressly prohibited;
- The responsibilities regarding the guarantee of the information security pillars mentioned above must be widely disseminated among the TOTVS Group companies and the application of the guidelines described here must be ensured.
- The information should be used in a transparent manner and only for the purpose for which it was collected and/or for statistical purposes without exposing the customers in an identifiable manner or to other system characteristics available to the customer himself.

4.3. Management of Accesses and Identity

The logical accesses of TOTVERs, interns and outsourced employees must be controlled in a way that only information that is needed for performing their tasks is available, requiring formal approval.

The physical accesses of TOTVERs, interns, outsourced employees and visitors to locations that have the technological resources of TOTVS must be controlled, requiring formal approval.

4.4. Processing the Information

To ensure adequate protection of TOTVS information, there should be a method to classify and label the information according to the degree of confidentiality and criticality for TOTVS' business:

- Classification must be according to the following labels: Restricted, Confidential, Internal or Public, considering the business needs;
- All the information must be adequately protected in compliance with the information security guidelines of TOTVS throughout its life cycle, which includes generation, handling, storage, transport and disposal;
- Information must be used in a transparent manner and only for the purpose for which it was gathered.

4.5. Risk Management, Objectives and Information Security Incidents

Risks must be identified through a process established for Evaluating Information Security Risks that affect the business and/or its strategies, which are aligned with the business environment in order to adequately preserve and protect TOTVS.

Information Security incidents should be analyzed, processed, recorded, monitored and reported to the person requesting said information and/or, depending on the case, should also be reported to the Ethics and Conduct Committee.

4.6. Awareness Training

TOTVS must hold regular and periodic training programs on Information Security awareness, which must be in different formats and addressed to different audience groups, and which may be but not limited to: On-site or Regular Training, Distance (EAD) and Social Engineering Campaigns.

5. Responsibilities

Following are the general responsibilities of TOTVERs, interns and outsourced employees:

- Faithfully comply with the Policy, the Standards and Procedures on Information Security of TOTVS;
- Undergo the compulsory training provided by TOTVS;
- Protect information from accesses, changes, destruction or disclosure not authorized by TOTVS;
- Ensure that technological resources, information and systems at their disposal are used only for the purposes approved by TOTVS;
- Comply with laws and standards that regulate intellectual property;
- Do not discuss confidential work-related matters in public places or open areas (airplanes, transport, restaurants, social gatherings, etc.), including comments and opinions in blogs and social networks;
- Immediately notify the Information Security department of any noncompliance or breach of this Policy and/or Standards or Procedures through seguridad.informacao@totvs.com.br, and report all Information Security incidents.

Following are the responsibilities of the Corporate Information Security area:

- Ensure broad dissemination and revision of the Information Security Policy, Standards and Procedures among TOTVERs and outsourced employees;
- Organize Information Security awareness programs for everyone at TOTVERs;
- Propose and manage projects and initiatives related to information security management at TOTVS;
- Manage and monitor the applied systems and controls under the management of the TOTVS Information Security department.

Following are the responsibilities of the Cloud Information Security area:

- Manage physical access to the Data Center;
- Manage logical access to the Cloud clients;
- Propose and manage projects and initiatives related to information security management for TOTVS clients;
- Manage and monitor the applied systems and controls under the management of the TOTVS Information Security department.

Following is the responsibility of the IT Support area:

- Manage the logical access to the tools and systems of the TOTVS operation.

Following is the responsibility of the Quality area:
- Manage the logical access to service management and project tools.

Following is the responsibility of the Property Security area:
- Manage the physical access to TOTVS facilities.

Following are the responsibilities of the Ethics and Conduct Committee:
- Analyze violations of the Security Policy reported and their consequences, where applicable, subject to the powers of the Audit Committee regarding the indicators of Information Security Risks.
- Request the Information Security area to check equipment and systems;
- Forward incidents to the respective Managers / Leaders for them to take appropriate measures.

Following are the responsibilities of the Audit Committee:
- Receive communications about important events;
- Analyze Risk Indicators and violations of the rules of this Policy regarding the routines of the Information Security area.

Following is the responsibility of the Board of Directors:
- Receive information from the Audit Committee about risk indicators and receive communications about events, and deciding on preserving information security, when necessary.

6. Management Actions

The Information Security area must supervise compliance with this Policy and refer all cases of noncompliance to the Ethics and Conduct Committee.

7. Approvals (Document)

Name / Position	Description
Mara Maehara Information Technology Officer	Preparation
Ricardo Guerino Executive Officer - Ombudsman, RCC, Processes, Risks and Compliance	Revision
Claudia Karpat Chief Legal Officer	Revision
Gustavo Dutra Bastos Vice President - Technology	Revision / Recommendation
Audit Committee	Recommendation
Board of Directors	Approval

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