
	POLICY	Code	Review
		SEG-POL-001-018	4
	Supplier Information Security Policy	Information Classification	Page
		Public	1 of 7

INDEX

1. OBJECTIVE	2
2. APPLICABILITY AND AREAS INVOLVED	2
3. Definitions and Assumptions	2
3.1. <i>Information Security Principles.....</i>	<i>2</i>
3.1.1. Code of Conduct.....	3
3.1.2. TIVIT Information Security Regulatory Documentation	3
4. Responsibilities	4
4.1. <i>RESPONSIBILITIES OF TIVIT's Provider/Supplier</i>	<i>4</i>
4.1.1. Identification of process Deviations/ Risks	4
4.1.2. Reporting Information Security Incidents.....	4
5. Policy Description	4
5.1. <i>Asset management.....</i>	<i>4</i>
5.2. <i>Physical and logical access control.....</i>	<i>5</i>
5.3. <i>Perimeter delimitation and physical security protection</i>	<i>5</i>
5.4. <i>Acceptable use of assets and resources.....</i>	<i>5</i>
5.5. <i>Analysis and security assurance in information systems</i>	<i>6</i>
5.6. <i>Human Resources, Interactions and Communications</i>	<i>6</i>
5.7. <i>Continuity, Disaster, or Emergency Situation Plans</i>	<i>6</i>
5.8. <i>Additional legal and regulatory requirements</i>	<i>7</i>
5.9. <i>Encryption, Privacy and Monitoring.....</i>	<i>7</i>
5.10. <i>Sub-contracting.....</i>	<i>7</i>
6. REFERENCE TO OTHER DOCUMENTS	7

	POLICY	Code	Review
		SEG-POL-001-018	4
	Supplier Information Security Policy	Information Classification	Page
		Public	2 of 7

1. OBJECTIVE

The purpose of this information security policy is to guide TIVIT Providers/Suppliers in existing information security guidelines, as well as to describe their participation and responsibility in meeting the objectives and strategies of excellence set by TIVIT as a provider of information technology products and services. The instructions and rules described herein should be followed to ensure, consistently and efficiently, the protection of the information provided by TIVIT, as well as the appropriate use of the technological resources, environments, and dependencies accessed by TIVIT Providers/Suppliers due to the provision of services, ensuring proper custody and avoiding deliberate or accidental threats.

2. APPLICABILITY AND AREAS INVOLVED

TIVIT Providers/Suppliers and business partners. The responsibility of TIVIT Providers/Suppliers to completion of directives herein described is limited to contracted services or products.


3. DEFINITIONS AND ASSUMPTIONS

3.1. Information Security Principles

All TIVIT Providers/Suppliers must be committed to the observation of TIVIT's information security policy by not sharing or misappropriating unauthorized content and information resources, using technological systems and resources only in accordance with authorizations and instructions specified by TIVIT, caring for and preserving our assets. All TIVIT Providers/Suppliers must also be imbued with maintaining and preserving the basic principles of information security:

- Confidentiality –TIVIT's Providers/Suppliers must contribute to maintaining the confidentiality and restriction of access to shared or accessible information due to the exercise of its contracted function and service. All information shared or accessible to TIVIT's Providers/Suppliers must be classified as classified and belonging to TIVIT.
- Integrity –TIVIT's Providers/Suppliers are committed to the proper and authorized use of TIVIT assets, including information. The manipulation or editing of information assets other than its intended scope or in contradiction to limitations imposed by procedures or controls to information systems is not allowed.
- Availability –TIVIT's Providers/Suppliers care for the preservation of the environments, facilities and technological resources related to its use, supply or support, in order to favor TIVIT' business continuity and the uninterrupted services.

It is considered an information security incident involving TIVIT Providers/Suppliers, any violation of information security principles herein described and, in particular, data breach: characterized by a security breach leading to accidental or illegal data destruction, data loss or unauthorized

	POLICY	Code	Review
		SEG-POL-001-018	4
	Supplier Information Security Policy	Information Classification	Page
		Public	3 of 7

disclosure, unauthorized access to transmitted or stored protected data, and unauthorized processing or transformation.

Security incidents arising from TIVIT Providers/Suppliers may result in investigations resulting in penalties and legal liability, as well as contract cancellations and indemnity claims.

3.1.1. Code of Conduct


It is the responsibility of all employees, TIVIT Providers/Suppliers, and TIVIT partners, the correct and ethical conduct, obeying the precepts of respect for people, and preservation of TIVIT image and its commitment to information security maintenance.

Providers/Suppliers are expected to behave ethically and with high morale, respect, and compliance with applicable laws, as well as TIVIT regulations, including:

- Perform all duties professionally with responsibility, dedication, honesty, and justice, always looking for the best possible solution;
- Look for continuous education to continuously acquire technical and professional skills, always keeping up with advances in profession and specialties;
- Act within the limits of your professional competence;
- Maintain professional secrecy of the information to which you have access due to the exercise of your contracted activities;
- Meet the expectations of trust placed by TIVIT, accessing and using resources and information only within the limit of the need to carry out its work and granted authorization;
- Guide their relationship with colleagues based on the principles of consideration, respect, and solidarity, as well as carrying out professional activities, involving interaction or group contribution, without discrimination of any kind, be it of color, sex, nationality, age, religion, marital status or any other human condition;
- Comply with commitments and deadlines;
- Do not perform deliberate acts that may compromise security, privacy, or serve to reduce or cancel the security controls and protections established by TIVIT.

3.1.2. TIVIT Information Security Regulatory Documentation

To support TIVIT's Information Security Management System (ISMS), adhering to the (for Brazil) ABNT NBR ISO/IEC 27001:2013 or (for other countries) ISO/IEC 27001:2013 standard for implementing, monitoring, and improving controls and efficiency and effectiveness of the process that ensures information security at TIVIT, several documents, procedures, and instructions are constantly published and updated. It is the responsibility

	POLICY	Code	Review
		SEG-POL-001-018	4
	Supplier Information Security Policy	Information Classification	Page
		Public	4 of 7

of TIVIT's Providers/Suppliers to comply with these regulations, even if they are not explicitly contained in this specific policy. For this purpose, TIVIT's Providers/Suppliers will seek, provided that it does not find sufficient guidance in this document, specific instructions from TIVIT and will complement the understanding of information security requirements whenever necessary.

TIVIT's Providers/Suppliers must seek to keep informed of TIVIT's security requirements and standards governing its services, as well as updates to these documentations.

4. RESPONSIBILITIES

4.1. RESPONSIBILITIES OF TIVIT's Provider/Supplier

All TIVIT Providers/Suppliers must follow general information security guidelines and contribute to the identification of threats and risks to TIVIT's operation.

4.1.1. Identification of process Deviations/ Risks

Each and every impediment to the provision of the service in the manner agreed/contracted must be reported to TIVIT, so that its impact is assessed and communicated, internally, minimizing the impacts on TIVIT's reputation and image and/or to the specific deliverable under contract.

4.1.2. Reporting Information Security Incidents

TIVIT Providers/Suppliers are an integral part of the communication flow of security events that can negatively interfere with the management of contracted service/product or our capability to foresee abnormal behavior of the IT resources in use. Such events can be classified as information security incidents by TIVIT and treated properly to ensure the integrity and quality of TIVIT's IT infrastructure.


Any abnormal behavior of network services and information systems, perceived by TIVIT Providers/Suppliers, should be reported to: soc.hotline@tivit.com

5. POLICY DESCRIPTION

TIVIT Providers/Suppliers should follow specific information security guidelines whenever appropriate.

5.1. Asset management

- TIVIT Providers/Suppliers must observe rules for the use of TIVIT-authorized computer equipment in work environments such as mobile devices, tablets, personal computers and

	POLICY	Code	Review
		SEG-POL-001-018	4
	Supplier Information Security Policy	Information Classification	Page
		Public	5 of 7

wearables. All computing equipment brought to the work environment, at the premises of TIVIT, must be declared.

- TIVIT Providers/Suppliers using IT equipment owned by TIVIT should use it exclusively for the purposes described in the specific contract, being responsible for maintaining conservation of the equipment and its immediate return to our representative, once its contract with TIVIT has been terminated or expired.
- The need for storage or transportation of computing equipment provided by TIVIT Provider must be expressly authorized by TIVIT. TIVIT Provider may perform the storage and/or transit of this type of equipment in the authorized locations specified in the authorization granted.
- Only media for custody and transport of information assets expressly authorized by TIVIT may be used by TIVIT Provider.
- Custody of TIVIT information assets by TIVIT Providers/Suppliers is not permitted after the termination of the contract unless otherwise stated in the contract.

5.2. Physical and logical access control


- TIVIT Providers/Suppliers must carry clear and visible identification (license/badge/label) or provide personally identifiable documentation upon request.
- TIVIT Providers/Suppliers must use only the identification and authentication of system users formally granted by TIVIT to carry out their activities, reporting errors or accesses that do not correspond to or exceed the scope of their contracted compliance.
- The system access credentials made available to a TIVIT Provider/Supplier are not transferable.
- Information systems provided by TIVIT Providers/Suppliers, for the use of TIVIT employees, must use secure authentication and offer user actions tracking. The availability or integration of these systems should preferably use multi-factor authentication (strong authentication) and connect to TIVIT controllers using modern Azure AD authentication for user login.

5.3. Perimeter delimitation and physical security protection

- TIVIT Providers/Suppliers must act and transit only in places expressly authorized and related to their contracted services.

5.4. Acceptable use of assets and resources

- TIVIT Providers/Suppliers must use information assets only for the purpose related to their contracted services.

	POLICY	Code	Review
		SEG-POL-001-018	4
	Supplier Information Security Policy	Information Classification	Page
		Public	6 of 7

- TIVIT Providers/Suppliers cannot reconfigure or change the capabilities and restrictions defined in TIVIT-owned technology equipment and resources. Equipment and resources owned by TIVIT or by the TIVIT Provider, used in its contracted performance, must not offer risks and vulnerabilities. The use of such equipment may be subjected to inspection and assessment by TIVIT at any time, with no prior notice, and may result in usage prohibition.

5.5. Analysis and security assurance in information systems


- Information systems provided by TIVIT Providers/Suppliers, for the use of TIVIT employees and/or their customers, must assure the applied security for information protection. Certificates of security analysis in force, carried out by competent third parties and independent entities, shall be submitted upon request. Also, TIVIT reserves the right to perform security analysis (vulnerability analysis, penetration, or another testing) to maintain this security assurance of information security on these systems.

5.6. Human Resources, Interactions and Communications

- TIVIT Providers/Suppliers should use only human resources (employees) expressly declared and authorized for the provision of contracted activities (including in activities outside TIVIT facilities).
- Interactions between TIVIT Providers/Suppliers and TIVIT must be carried by the media and means authorized by TIVIT.
- Communication and sending of information must be carried out securely, observing the communication protocols and applications authorized by TIVIT.

5.7. Continuity, Disaster, or Emergency Situation Plans

- When triggered in a contingency scenario, activation of continuity plans and/or disaster recovery, TIVIT Providers/Suppliers responsible for emergency actions, should prioritize the actions according to the asset importance level dictated by TIVIT, respecting the Service Level Agreements (SLA) defined in the contract.
- If defined in the contract, TIVIT Providers/Suppliers that support critical business areas shall regularly provide test results for the execution of continuity and/or disaster recovery plans related to the scope of contracted products and services, in order to demonstrate compliance with the process and expected times agreed.
- All emergency actions implemented with the participation of TIVIT's Providers/Suppliers must comply with the information security principles established by TIVIT.

	POLICY	Code	Review
		SEG-POL-001-018	4
	Supplier Information Security Policy	Information Classification	Page
		Public	7 of 7

5.8. Additional legal and regulatory requirements

- All security compliance obligations, in addition to this policy, determined by legal requirements or sector regulations to which TIVIT is subject, generate obligation of compliance by TIVIT Providers/Suppliers, limited to its contracted service.
- If the TIVIT Provider/Supplier stores data from TIVIT or TIVIT's Customers outside the Brazilian national territory, it must inform TIVIT of the storage country. The change of storage to any country other than the one initially informed must be consulted in advance and expressly authorized by TIVIT.

5.9. Encryption, Privacy and Monitoring

- The TIVIT Provider handling personal data due to its contracted activity is responsible for ensuring that such data is handled in accordance with all applicable Privacy and Personal Data Protection rules.
- All confidential information, with access granted to TIVIT's Providers/Suppliers must comply with the security and key management principles established by TIVIT. The TIVIT Provider is not authorized to change permissions, tamper, or interfere with the access management governed by TIVIT.
- TIVIT reserves the right to monitor and control the actions of credentials provided by TIVIT and used by TIVIT Providers/Suppliers, as well as to inspect the content of messages and communications made through the use of the computer network under TIVIT management.

5.10. Sub-contracting

- The TIVIT Provider who chooses to outsource some part or all of the scope of the contracted services must obtain prior consent from TIVIT to do so.
- If the subcontracting is approved by TIVIT, it is the responsibility of the TIVIT Providers/Suppliers to guarantee the knowledge and compliance with all the guidelines set out here by the sub-contractors.

6. REFERENCE TO OTHER DOCUMENTS

Not applicable.