# Supplier Security Policy

*Information security and data protection in relationships with suppliers, partners, and service providers of PX.Center*

| | |
|---|---|
| ***Code:*** | *POL-SIP-011* |
| ***Responsible area:*** | *Information Security* |
| ***Issue date:*** | *24/06/2026* |
| ***Approval authority:*** | *CISO / CTO* |

## 1. PURPOSE/OBJECTIVE

This policy establishes the guidelines for managing information security in relationships with suppliers, partners, and service providers of PX.Center, ensuring that services rendered by third parties preserve the confidentiality, integrity, and availability of the Organization's information.

In accordance with controls 5.19, 5.20, 5.21, and 5.22 of ISO/IEC 27001:2022 and with ISO/IEC 27701:2019, this policy defines the selection, contracting, monitoring, subcontracting, and termination requirements applicable to the supply chain, including the specific personal data protection obligations when the supplier acts as a data processor on behalf of PX.Center, pursuant to Law 13.709/2018 (LGPD). This policy derives from the Information Security Policy (POL-SIP-001) and details its requirements in the domain of supplier relationships and the supply chain.

## 2. SCOPE/APPLICABILITY

This policy applies to all suppliers, partners, outsourced service providers, and cloud/SaaS providers whose services may impact information security or involve the processing of personal data of PX.Center, as well as to internal employees responsible for the contracting, management, and oversight of such services. It covers the entire lifecycle of the relationship with the third party: risk identification, classification, selection, contractual formalization, execution, monitoring, and termination.

It applies in conjunction with POL-SIP-029 (baseline standard for personal data processing) whenever the engagement involves personal data. It is subordinate to the Information Security Policy (POL-SIP-001), from which it derives, and complements it in the supplier domain.

## 3. USERS/TARGET AUDIENCE

Senior Management, Information Security Leader, Data Protection Officer (DPO), Legal, managers of areas requesting procurement, IT team, and all employees and third parties involved in the contracting, management, or oversight of suppliers who have access to PX.Center's information, systems, or personal data.

## 4. REFERENCE DOCUMENTS

- Law 13.709/2018 (Brazilian General Data Protection Law, LGPD)
- ISO/IEC 27001:2022 (controls 5.19, 5.20, 5.21, and 5.22)
- ISO/IEC 27701:2019 (control 6.12)
- POL-SIP-001: Information Security Policy
- POL-SIP-029: Privacy and Personal Data Protection Policy
- POL-SGI-001: Information Lifecycle Policy

- POL-SIP-016: Access Control Policy
- POL-SIP-004: Risk Assessment and Treatment Methodology
- POL-SIP-002: Incident Management Policy
- POL-SGI-002: Records Management Policy
- FOR-17-001: Supplier Due Diligence Questionnaire

## 5. GUIDELINES / RULES / CONTROLS

### 5.1 RISK IDENTIFICATION AND ASSESSMENT

The Information Security team, together with the requesting area and Legal, identifies, assesses, and addresses information security risks in every process involving third parties. The assessment takes place prior to contracting and is reviewed periodically or whenever there is a change in the scope of services. The criteria considered include, among others: access to sensitive or critical data, connection to the corporate network, processing of customer data or data of other data subjects, and the existence of subcontracting.

When the engagement involves the processing of personal data, the Data Protection Officer (DPO) is involved in the assessment, as set out in section 5.4.

### 5.2 SUPPLIER RISK CLASSIFICATION

Every supplier is classified into one of three risk categories — High, Medium, or Low — prior to contracting, based on the type of access to the Organization's assets, the volume and sensitivity of personal data processed, and the criticality of the service provided to PX.Center's operations. A supplier is classified as High Risk if it holds privileged access to systems or the corporate network, processes a significant volume of personal data or sensitive personal data, or if its service is critical to business continuity.

A Medium Risk supplier maintains limited access to internal information or processes personal data within a restricted scope, and a Low Risk supplier does not access personal data or critical assets. Suppliers classified as High Risk are subject to due diligence prior to contracting and to annual reassessment; Medium and Low Risk suppliers follow the proportional review frequency defined in section 5.8. The classification is recorded and reviewed at each contract renewal or relevant change in scope.

### 5.3 SELECTION AND DUE DILIGENCE

PX.Center's premise is to engage only third parties of unimpeachable reputation, sound conduct, and proven technical capability. The area responsible for procurement screens the supplier with the support of Information Security, verifying compliance with legal and regulatory requirements, relevant certifications (for example, ISO 27001, SOC 2, and LGPD compliance), history of security incidents, and market reputation.

When the engagement involves the processing of personal data, a prior assessment of the third party's technical capacity and security measures is conducted by means of FOR-17-001 (Supplier Due Diligence Questionnaire), whose responses are analyzed with the involvement of the DPO. The supplier is only approved after formal validation of the risk analysis. For third

parties already contracted prior to the publication of this policy, a compliance analysis is conducted to assess whether to maintain or terminate the contractual relationship.

5.4 THE DPO'S ROLE IN CONTRACTING DATA PROCESSORS

Whenever the engagement involves the processing of personal data by the third party on behalf of PX.Center — characterizing it as a processor under the LGPD — the Data Protection Officer (DPO) must be consulted prior to formalization. The DPO is responsible for defining, together with Legal, the personal data protection requirements applicable to the contract; evaluating the responses to FOR-17-001 to confirm compliance with the requirements; and conducting recurring due diligence to verify ongoing compliance.

If the third party does not meet the requirements, corrective measures are defined jointly with the DPO and implemented before proceeding with the engagement. The DPO is also consulted in case of questions regarding the contracting of processors, security incidents, or any personal data protection matter that may affect compliance with the LGPD.

5.5 CONTRACTUAL INFORMATION SECURITY REQUIREMENTS

The inclusion of information security contractual clauses is the responsibility of Legal, with technical support from Information Security. Contracts provide for, at a minimum: a non-disclosure agreement (NDA); responsibilities for the protection of information and data; minimum security requirements; penalties in case of non-compliance; and rules for the termination, return, or destruction of assets and information. The contract owner is the requesting area.

For engagements that do not involve a formal contractual instrument, a Commitment Agreement is executed establishing compliance with security requirements and the provisions of the LGPD.

5.6 PERSONAL DATA PROTECTION AND DATA PROCESSING AGREEMENT (DPA)

When the supplier acts as a personal data processor on behalf of PX.Center, the execution of a Data Processing Agreement (DPA) is mandatory, drafted by Legal together with the DPO, in compliance with ISO/IEC 27701:2019 (6.12) and the LGPD. The DPA expressly defines:

the roles of controller and processor; the purpose and categories of data processed; technical and organizational security measures; conditions for the use of sub-processors; rules for international transfers; the obligation to notify incidents; support for data subject rights; retention periods; return or deletion of data upon termination of the relationship; and PX.Center's right to audit. Contracts clearly define the duties and responsibilities of each party in the event of a personal data breach.

The personal data protection contractual clause to be incorporated into supplier contracts complies with the minimum content set out in Annex I of this policy.

5.7 SUBCONTRACTING

The supplier may not subcontract, in whole or in part, the contracted services involving access to PX.Center's information, systems, or data without PX.Center's prior formal written authorization. The requirement for such authorization is established in the contract. Once

subcontracting is authorized, the supplier remains fully responsible to PX.Center and must contractually pass on to the subcontractor all security and personal data protection requirements assumed under this policy, ensuring that the subcontractor's practices comply with this document.

For critical suppliers and cloud/SaaS providers, subcontractors, dependencies, and supply chain components are assessed and the supply chain is reviewed before significant changes, with mandatory notification of any changes.

### 5.8 MONITORING AND REVIEW

The requesting area, with the support of Information Security, monitors the supplier's performance against contractual security requirements. Compliance review is conducted at a minimum annually for High Risk suppliers, adjustable according to the supplier's criticality and classification. Reports, evidence, and internal audits may be required pursuant to the contract.

When personal data is processed, the DPO conducts periodic due diligence to confirm ongoing compliance; if a deficiency is identified in an already-contracted third party, a reasonable risk-based deadline for remediation is negotiated and, if not met, the DPO engages with the contract manager to propose replacement of the supplier.

### 5.9 TRAINING AND AWARENESS

Information Security provides awareness materials on information security to be presented to critical suppliers prior to service delivery. For internal employees, periodic training addresses outsourcing risks and best practices in partner relationships.

### 5.10 USE OF SOCIAL MEDIA IN THIRD-PARTY RELATIONSHIPS

The use of social media on behalf of PX.Center is permitted to business functions that depend on it, particularly Marketing and Commercial, subject to the prohibition on disclosing confidential information or personal data of the Organization, its clients, or its suppliers. All other employees are prohibited from personal use of social media during the performance of activities involving the Organization's information or assets.

Suppliers and service providers with access to PX.Center's information are subject to the same restriction and are prohibited from disclosing, on social media or external channels, any confidential information or personal data to which they have access by virtue of the contract.

### 5.11 REPORTING VIOLATIONS

Any suspected or actual violation of this policy, of security requirements, or of personal data protection obligations must be reported immediately through PX.Center's official channels. Matters relating to privacy and personal data protection are reported to the Data Protection Officer (DPO) at dpo@px.center; matters relating to information security are reported to the Information Security team at security@px.center.

Reports are handled diligently and confidentially and, upon confirmation of a violation, appropriate corrective and disciplinary measures are taken.

### 5.12 CONTRACT TERMINATION, ACCESS REVOCATION, AND RETURN OF ASSETS

The requesting area notifies Information Security of any change in scope or contract termination. Information Security assesses and updates the risks, documents the results, and forwards them to Compliance and Legal. The IT team, under the guidance of Information Security, ensures the revocation of access and the return of technological assets (laptops, tokens, credentials, and other resources) upon contract termination.

The return or destruction of shared information and personal data is confirmed and recorded upon termination of the relationship, ensuring that the supplier retains no form of access to the Organization's data or systems.

## 6. RESPONSIBILITIES

6.1 Manager of the requesting area (contract owner): requires third parties to comply with PX.Center's security and privacy rules and contractual provisions; provides FOR-17-001 to the supplier prior to contracting; submits responses to the DPO for analysis when personal data processing is involved; continuously monitors service delivery; and immediately notifies Information Security and the DPO of incidents and situations affecting compliance.

6.2 Information Security: identifies, classifies, and addresses supplier risks; defines security metrics and requirements in contracts prior to service delivery; guides third parties on the Information Security Policy; monitors the application of controls throughout the contract; and acts as the internal party responsible for investigating information security violations received through the security@px.center channel.

6.3 Legal: drafts, together with the DPO, contract templates, DPAs, and Commitment Agreements; and ensures the inclusion of security and personal data protection requirements in new contracts, revisions, and renewals.

6.4 Data Protection Officer (DPO): defines personal data protection requirements for contracts with processors together with Legal; evaluates FOR-17-001; conducts recurring due diligence; provides guidance on the application of this policy in personal data protection matters; and acts as the internal party responsible for investigating privacy and personal data protection violations received through the dpo@px.center channel.

6.5 IT Team: carries out access revocation and asset return upon contract termination, under the guidance of Information Security.

Approval: CISO / CTO.

## 7. RECORDS MANAGEMENT

Records related to suppliers — risk classifications, assessments, FOR-17-001 questionnaires, contracts and DPAs, monitoring reports, evidence of due diligence and asset returns — are stored in a secure repository managed by the responsible area, with access restricted on a need-to-know basis. PX.Center maintains a standard records control spreadsheet in

accordance with the Records Management Policy. Records are preserved with integrity and kept available for internal and external SGI audits.

## 8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on 23/06/2026 and remains valid for an indefinite period. It is reviewed annually or in response to a relevant change in the Organization's security strategy, in legislation or ANPD guidance, or in the need for technological adaptation. The document owner is the Information Security team, subject to approval by the CISO / CTO. Non-compliance with this policy by employees, contractors, or service providers subjects the offender to disciplinary measures set out in PX.Center's internal regulations, without prejudice to applicable legal and contractual sanctions.

## 9. ANNEXES

FOR-17-001 — Supplier Due Diligence Questionnaire: prior assessment instrument for the third party's technical capacity and security and personal data protection measures, applied during selection and periodic due diligence. Other operational records reside in the repositories indicated in the Records Management section.

ANNEX I — PERSONAL DATA PROTECTION CONTRACTUAL CLAUSE (LGPD)

Clause to be incorporated into contracts executed with suppliers that process personal data on behalf of PX.Center, with numbering adjusted to the respective contractual instrument.

Data Protection. The Parties declare to be aware of the provisions set forth in Law No. 13.709/2018 (Brazilian General Data Protection Law — LGPD), and undertake to comply fully therewith, as well as to obtain the authorizations of their respective clients and data subjects whenever the eventual sharing of data with third parties is required, releasing the other Party from liability in that regard or for any breach of said legislation.

The processing of personal data shall be carried out solely and exclusively for the purposes necessary for the performance of the contracted services, and its use for other purposes is prohibited without the express consent of the Contracting Party or the data subject, where required, subject to the joint liability of the Parties pursuant to the LGPD.

The Parties undertake to adopt all appropriate technical and organizational measures to protect personal data against unauthorized access, loss, destruction, leakage, or any form of incident or unlawful processing, using it solely for the performance of the contract.

The Parties undertake to notify each other, within 48 (forty-eight) hours of becoming aware, of the occurrence of any event constituting an information security incident with the potential to violate the privacy of personal data subjects. The notification, even if provisional, shall include at a minimum: the date and time the incident was identified; a description of the incident; the types of data potentially exposed; the volume of data subjects potentially affected; and the

measures taken to mitigate or remediate the impacts, under penalty of the sanctions provided for in the LGPD.

Upon termination of the contract, regardless of the reason, the Contracted Party shall delete all personal data obtained in its context, except where retention is legally permitted or required.

Non-compliance with this clause subjects the offending Party to liability for direct or indirect damages, whether moral, material, or regulatory, as well as to the application of the penalties set forth in the LGPD and other applicable legislation.

All rules regarding the processing of personal data carried out by the Contracting Party, including data subject rights, are set out in the Contracting Party's Privacy Notice, which the Contracted Party declares to have accessed, read, and agreed to.

## CHANGE HISTORY

| Version | Date | Author | Change Description |
|---|---|---|---|
| 00 | 09/06/2025 | IT and Cybersecurity Department - SI | Creation and Review |
| 01 | 24/06/2026 | SGI | Recoding to acronym |