Supplier Security Policy

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

Code	POL-SEG-011
Responsible Area	Information Security
Issue Date	June 24, 2026
Approval Authority	CISO / CTO

1. PURPOSE / OBJECTIVE

This policy establishes the guidelines for managing information security in PX.Center's relationships with suppliers, partners, and service providers, ensuring that third-party services 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 under Law No. 13,709/2018 (Brazilian General Data Protection Law — LGPD). This policy derives from the Information Security Policy (POL-SEG-001) and details its requirements in the domain of supplier relationships and supply chain management.

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 PX.Center's personal data, as well as to internal employees responsible for contracting, managing, and supervising these services. It covers the entire lifecycle of the third-party relationship: risk identification, classification, selection, contractual formalization, execution, monitoring, and termination.

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

3. USERS / TARGET AUDIENCE

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

4. REFERENCE DOCUMENTS

- Law No. 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-SEG-001: Information Security Policy
- POL-SEG-029: Privacy and Personal Data Protection Policy
- POL-SGI-001: Information Lifecycle Policy
- POL-SEG-016: Access Control Policy
- POL-SEG-004: Risk Assessment and Treatment Methodology

- POL-SEG-002: Incident Management Policy
- POL-SGI-002: Records Control Policy
- FOR-17-001: Supplier Due Diligence Questionnaire

5. GUIDELINES / RULES / CONTROLS

5.1 Risk Identification and Assessment

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

When contracting involves the processing of personal data, the Data Protection Officer (DPO) is included in the assessment, in accordance with 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 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 provides a service that is critical to business continuity.

A Medium Risk supplier maintains limited access to internal information or processes personal data within a restricted scope, while 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 a proportional review schedule as defined in section 5.8. Classifications are recorded and reviewed at each contract renewal or upon any significant change in scope.

5.3 Selection and Due Diligence

PX.Center's premise is to engage only third parties with an unblemished reputation, sound conduct, and demonstrated technical capability. The department responsible for contracting performs supplier screening with the support of Information Security, verifying compliance with legal and regulatory requirements, relevant certifications (e.g., ISO 27001, SOC 2, and LGPD compliance), the history of security incidents, and market reputation.

When the contracting arrangement involves the processing of personal data, a prior assessment of the third party's technical capability and security measures is conducted using FOR-17-001 (Supplier Due Diligence Questionnaire), the responses to which are analyzed with the DPO's involvement. The supplier is approved only after formal validation of the risk analysis. For third parties already engaged before this policy was published, a compliance analysis is performed to assess whether to maintain or terminate the contractual relationship.

5.4 The DPO's Role in Contracting Data Processors

Whenever contracting involves the processing of personal data by a third party on behalf of PX.Center — thereby characterizing it as a data processor under the LGPD — the Data Protection Officer (DPO) must be consulted before 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 that requirements are met.
- Conducting recurring due diligence to verify the maintenance of compliance.

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

5.5 Contractual Information Security Requirements

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

For engagements that do not involve a formal contractual instrument, a Letter of Commitment is signed establishing compliance with the 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. This agreement is prepared by Legal together with the DPO, in compliance with ISO/IEC 27701:2019 (6.12) and the LGPD. The DPA expressly sets out:

- The roles of controller and processor.
- The purposes and categories of data processed.
- Technical and organizational security measures.
- Conditions for the use of sub-processors.
- Rules for international data transfers.
- The obligation to notify incidents.
- Support for fulfilling data subjects' rights.
- Retention periods.
- Return or deletion of data upon termination of the relationship.
- 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 observes 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 that involve access to PX.Center's information, systems, or data without prior, formal, written authorization from PX.Center. The requirement for such authorization is established in the contract. If 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, sub-processors, dependencies, and supply chain components are evaluated; the supply chain is reassessed before significant changes, and mandatory notification of any alterations is required.

5.8 Monitoring and Review

The requesting department, with the support of Information Security, monitors supplier performance against contractual security requirements. Compliance reviews are conducted at a minimum annual frequency for High Risk suppliers, adjustable according to supplier criticality and classification. Reports, evidence, and internal audits may be required as stipulated in the contract.

When personal data processing is involved, the DPO conducts periodic due diligence to confirm ongoing compliance. If inadequacy is identified in a supplier already engaged, a reasonable timeline — determined based on risk — is negotiated for remediation. If the timeline is not met, the DPO works with the contract manager to propose supplier replacement.

5.9 Training and Awareness

Information Security provides information security awareness materials to be presented to critical suppliers prior to the commencement of services. 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 for business functions that depend on it, especially Marketing and Sales, subject to the prohibition on disclosing confidential information or personal data belonging to the Organization, its customers, or its suppliers. All other employees are prohibited from personal use of social media during 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 exposing, on social media or external channels, any confidential information or personal data accessed 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 immediately reported through PX.Center's official channels. Privacy and personal data protection matters are reported to the Data Protection Officer (DPO) at **dpo@px.center**; information security matters are reported to the Information Security area at **security@px.center**.

Reports are handled diligently and confidentially. Once a violation is confirmed, appropriate corrective and disciplinary measures are taken.

5.12 Contract Termination, Access Revocation, and Asset Return

The requesting department notifies Information Security of any change in scope or contract termination. Information Security assesses and updates risks, documents the results, and forwards them to Compliance and Legal. The IT team, under the direction 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 at the close of the relationship, ensuring that the supplier retains no form of access to the Organization's data or systems.

6. RESPONSIBILITIES

6.1 Requesting Department Manager (Contract Owner)

Requires that third parties follow PX.Center's security and privacy rules and contractual provisions; submits FOR-17-001 to the supplier prior to contracting; forwards 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 manages supplier risks; defines security metrics and requirements in contracts prior to service delivery; advises third parties on the Information Security Policy (ISP); monitors the application of controls throughout the contract; and serves as the internal authority for investigating information security violations received via **security@px.center**.

6.3 Legal

Prepares, together with the DPO, contract templates, DPAs, and Letters of Commitment; and ensures the inclusion of security and personal data protection requirements in new contracts, revisions, and renewals.

6.4 Data Protection Officer (DPO)

Defines with Legal the personal data protection requirements in contracts with processors; evaluates FOR-17-001; conducts recurring due diligence; provides guidance on the application of this policy in personal data protection matters; and serves as the internal authority for investigating privacy and personal data protection violations received via **dpo@px.center**.

6.5 IT Team

Executes access revocation and asset return upon contract termination, under the direction 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, due diligence evidence, and asset return records — are stored in a secure repository controlled 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 ISMS audits.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy takes effect on June 23, 2026, with indefinite validity. It is reviewed annually or upon any significant change in the Organization's security strategy, in legislation or ANPD (Brazilian National Data Protection Authority) guidance, or when technological adjustments are required. The document owner is the Information Security area, under the approval of the CISO / CTO. Non-compliance with this policy by employees, contractors, or service providers subjects the offender to the disciplinary measures set forth in PX.Center's internal regulations, without prejudice to applicable legal and contractual sanctions.

9. ANNEXES

FOR-17-001 — Supplier Due Diligence Questionnaire: an instrument for prior assessment of the third party's technical capability 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 — Contractual Clause on Personal Data Protection (LGPD)

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

Data Protection. The Parties acknowledge their awareness of the provisions of Law No. 13,709/2018 (Brazilian General Data Protection Law — LGPD) and assume full responsibility for compliance, as well as for obtaining the necessary authorizations from their respective customers and data subjects when any disclosure of data to third parties is required, releasing the other Party from liability in this regard or for any non-compliance with said legislation.

Personal data processing is carried out solely and exclusively for the purposes necessary for the performance of the contracted services; use for other purposes without the express consent of the Contracting Party or of the data subject, where required, is prohibited, subject to the joint and several liability of the Parties under the LGPD.

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

The Parties undertake to notify each other within 48 (forty-eight) hours of becoming aware of any event constituting a security incident with potential privacy impact on personal data subjects. The notification, even if preliminary, must include at minimum: the date and time the incident was discovered; a description of the incident; the types of data potentially exposed; the number of data subjects potentially

affected; and the measures taken to mitigate or remediate the impacts, under penalty of the sanctions set forth in the LGPD.

Upon termination of the contract, regardless of the reason, the Contracted Party must delete all personal data obtained in its context, unless 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 sanctions provided for in the LGPD and other applicable legislation.

All rules regarding personal data processing carried out by the Contracting Party, including data subjects' 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	Description of Changes
00	June 9, 2025	IT and Cybersecurity Department — IS	Creation and Review
01	June 24, 2026	ISMS (SGI)	Recoded to acronym-based identifier