Information Security Policy

Corporate guidelines for the protection of PX.Center's information assets and establishment of the ISMS

Code:	*POL-SIP-001*
Responsible area:	*Information Security*
Issue date:	*24/06/2026*
Approval authority:	*CISO / CTO*

1. PURPOSE/OBJECTIVE

PX.CENTER LTDA. (hereinafter referred to as "PX.Center" or "Organization") establishes this Information Security Policy (ISP) as the strategic and normative pillar for the protection of information assets owned by the Organization, as well as those held in custody by all its subsidiaries and controlled entities, across all business units and companies under its management.

Information security is understood by the Organization not merely as an operational control, but as a business-enabling asset and a mandatory resilience requirement, aimed at ensuring strict compliance with the principles of confidentiality, integrity, and availability of data.

The objective of this policy is to establish governance guidelines that direct the Information Security Management System (ISMS), in order to mitigate technological and human risks and ensure that the processing of personal and corporate data complies with Law 13.709/2018 (General Personal Data Protection Law, LGPD) and with international security standards.

The commitment of PX.Center's Senior Management to this regulatory body reflects the unceasing pursuit of reputational integrity and the fulfillment of contractual and regulatory obligations in force, with adherence to these standards being an inherent duty of all its stakeholders.

2. SCOPE/APPLICABILITY

This policy has corporate-wide scope and its application is mandatory and unrestricted to all business units, departments, and companies under PX.Center's management. The scope extends, without exception, to all stakeholders, including employees at any hierarchical level, interns, directors, board members, service providers, consultants, and commercial partners who, by virtue of their responsibilities, use the Organization's technological infrastructure or process information owned by the Organization.

Compliance with these guidelines encompasses all information assets, including software systems, databases, communication networks, physical devices, cloud computing environments, and documents. Compliance is an essential condition for the maintenance of the employment or contractual relationship with PX.Center, and access to the Organization's informational resources presupposes formal acceptance of the terms and obligations established herein.

All employees, interns, and third parties with access to PX.Center's information must sign a Confidentiality and Non-Disclosure Agreement (NDA) or equivalent document prior to commencing their activities, with a term that extends beyond the termination of the relationship for the period defined in supplementary technical standards, not less than two years for information classified as Restricted.

PX.Center must ensure that service providers, consultants, commercial partners, and other third parties with access to information assets are bound by specific contractual clauses on information security and data protection, commensurate with the risks of the activities

performed, and may be subject to risk assessments, audits, and additional control requirements.

Vendors and partners must be classified by risk level — High, Medium, or Low — based on the type of access to information assets, the volume of personal data processed, and the criticality of the services provided. High-Risk Vendors must be subject to a security assessment and due diligence prior to contracting and annually throughout the term of the contract.

Such third parties must notify PX.Center, within the maximum period contractually defined, not exceeding 30 (thirty) calendar days, of any security incident or data breach that may affect the Organization or the subjects of personal data.

3. USERS/TARGET AUDIENCE

Senior Management, the Information Security and Privacy Committee (CSIP), the Information Security Manager (CISO), the Data Protection Officer (DPO), area managers, owners of information assets, and all employees, interns, service providers, consultants, and commercial partners who use technological resources or process information on behalf of PX.Center.

4. REFERENCE DOCUMENTS

- Law 13.709/2018 (General Personal Data Protection Law, LGPD)
- Law 12.965/2014 (Brazilian Internet Civil Framework)
- ISO/IEC 27001:2022
- ISO/IEC 27701:2019
- PX.Center Code of Ethics and Conduct
- MAN-SGI-001 (SGI Manual)
- PLC-17-002 (ISMS Statement of Applicability)
- POL-SIP-016 (Access Control Technical Standard)
- POL-SIP-029 (Privacy and Personal Data Protection Policy)
- POL-SIP-027 (Privacy Governance Policy)
- POL-SIP-002 (Incident Management Policy)
- POL-SIP-017 (Training and Awareness Policy)
- POL-SGI-001 (Information Lifecycle Policy)
- POL-SIP-004 (Risk Management Methodology)
- POL-SGI-002 (Records Control Policy)
- Information Classification Policy
- Technical Standards for Asset Management, Backup, and Business Continuity

The possible absence of technical detail on a specific control in this policy does not exempt the individual from complying with the obligations contained in the supplementary technical standards. In the event of a conflict between this document and the specific standards, the guidelines of this ISP shall prevail, unless otherwise formally resolved by the Information Security and Privacy Committee.

5. GUIDELINES / RULES / CONTROLS

5.1 GOVERNANCE STRUCTURE

Information security governance is exercised centrally by PX.Center, which holds the authority to establish the guidelines and controls applicable to all companies under its management. Senior Management assumes responsibility for providing the necessary resources and for strategic support of the ISMS, and must ensure alignment between asset protection and business objectives.

The supervisory structure is composed of the Information Security and Privacy Committee (CSIP), a multidisciplinary collegiate body responsible for deliberating on investments, approving normative revisions, and monitoring the effectiveness of internal controls, with the authority to intervene in processes that present critical risks to operational continuity or legal compliance; the Information Security Manager (CISO), responsible for the technical implementation of the ISMS, for coordinating incident responses, and for auditing the logical and physical controls of all business units; and the Data Protection Officer (DPO), responsible for official communication with the National Data Protection Authority (ANPD) and for safeguarding the rights of data subjects, acting transversally to ensure compliance with the LGPD.

It is the duty of every employee and third party to observe the established standards of conduct, to maintain the confidentiality of information, and to immediately and mandatorily report any suspicious event through the Organization's official channels.

PX.Center must maintain and update a Statement of Applicability (SoA), formalized in PLC-17-002, which documents which controls from Annex A of ISO/IEC 27001:2022 are applicable to the Organization, with the respective justifications for inclusion or exclusion and the implementation status, in accordance with requirement §6.1.3 of the standard, constituting the basis for auditability and certifiability of the ISMS.

PX.Center's Senior Management must conduct a management review of the ISMS at least annually, with a minimum agenda defined in supplementary technical standards, covering indicator performance, audit results, risk treatment status, and improvement decisions, with results formally recorded in accordance with §9.3 of ISO/IEC 27001:2022.

PX.Center must define, document, and monitor measurable information security objectives, including performance indicators (KPIs) aligned with the business risk context, which must be reviewed at the management review conducted by Senior Management at least annually, in accordance with §6.2 of ISO/IEC 27001:2022.

PX.Center is committed to the continual improvement of its ISMS, and must promote periodic reviews of its objectives, indicators, and controls so as to adapt them to technological, regulatory, and business risk context changes. Senior Management must ensure that the results of assessments, audits, and incidents are taken into account when updating this policy and other related normative documents.

5.2 RISK MANAGEMENT AND INFORMATION CLASSIFICATION

PX.Center adopts a risk-based management methodology to prioritize the protection of its information assets, through periodic assessments that identify, analyze, and address threats that may compromise the continuity of operations or the privacy of data in its custody. The risk management methodology, the probability and impact scale, the acceptance threshold, and the Organization's risk appetite must be established in a supplementary document formally approved by the CSIP, with a minimum annual review, in accordance with §6.1.2 of ISO/IEC 27001:2022.

Every new project, system, or engagement of a critical vendor must be preceded by a security and privacy impact assessment, ensuring that preventive controls are integrated from the design phase (Privacy by Design). Significant changes in business processes, the creation of new digital products or services, and significant integrations with third-party systems must also be preceded by this assessment, whose results will guide the definition and implementation of additional controls necessary to mitigate the identified risks.

To ensure appropriate handling and access control, information within the Organization must be categorized according to its level of criticality and sensitivity. Public Information is information whose external access causes no negative impact on PX.Center or third parties. Internal Information corresponds to data for everyday operational use which, if improperly disclosed, may cause minor operational or administrative harm.

Confidential Information encompasses strategic data, trade secrets, or personal data, access to which is restricted exclusively to individuals with a functional need to know. Restricted Information comprises highly sensitive critical data, the leakage or loss of which may result in severe legal sanctions, irreparable reputational damage, or significant financial losses.

The protection of information also covers physical documents and non-digital storage media. Records containing Internal, Confidential, or Restricted information must be stored in appropriately protected locations, with physical access controlled and consistent with their level of criticality. The disposal of documents and media containing sensitive information must follow secure destruction procedures, such as shredding, disposal by a specialized company, or physical destruction of media, so as to prevent the unauthorized recovery of their content.

The assignment of classification level and the definition of access rights are the responsibility of the information owner, and the handling, storage, and disposal of assets must strictly follow the procedures established in PX.Center's supplementary standards.

Access logs, system usage records, and network traffic may be collected and analyzed by PX.Center for information security purposes, compliance with legal obligations, and protection of its assets, in accordance with applicable legislation. Users are hereby notified that they should have no expectation of privacy regarding the use of corporate technological resources and must use them in observance of the current internal regulations.

5.3 INFORMATION SECURITY AWARENESS PROGRAM

PX.Center must maintain a Corporate Information Security Awareness Program with mandatory participation for all employees and third parties with access to information assets,

with a minimum annual frequency and content updated in accordance with the current threat landscape, including social engineering, phishing, and the safe use of Artificial Intelligence.

Completion records must be maintained as evidence for audits, and phishing simulations and knowledge assessments may be applied periodically to gauge the effectiveness of the program, in accordance with Control A.6.3 of ISO/IEC 27001:2022.

5.4 ASSET MANAGEMENT AND PHYSICAL ACCESS

Access to PX.Center's physical premises is controlled by formal identification mechanisms, with badge use mandatory for all employees, interns, service providers, and visitors during their presence on the premises. Entry into internal areas, especially those classified as critical, requires authentication in access control systems, which may include badge validation and facial recognition, ensuring the traceability of all entries and exits.

Sharing of badges or granting access to unauthorized individuals is prohibited, and any loss, misplacement, or suspected misuse must be reported immediately through official channels. Every third party or visitor must have prior registration and be associated with an internal contact, with access conditional upon identity verification and the recording of entry and exit times. The Organization may establish access zones with different levels of physical restriction, aligned with the criticality of the assets and information present therein.

All equipment, mobile devices, storage media, and other technological resources provided by PX.Center are the exclusive property of the Organization and must be used strictly for professional purposes, with users responsible for the physical integrity and logical security of the assets in their care.

The Organization must maintain an up-to-date asset inventory, recording the responsible party, location, and status, with the installation of unauthorized software, the use of personal equipment in violation of internal standards, and the modification of security configurations without prior consent from the technology department being prohibited. In the event of termination, change of role, or end of contract, all assets and information owned by PX.Center must be returned immediately, in accordance with internal procedures for return and access revocation.

The use of personal devices to access corporate resources (BYOD) is permitted only when expressly authorized and subject to compliance with security requirements defined in specific technical standards, including malware protection mechanisms, encryption, and remote management capabilities. The use of removable media, such as USB drives and external disks, must be restricted, subject to technical protection controls, and replaced, wherever possible, by secure corporate file-sharing and storage solutions.

5.5 ACCESS CONTROL AND IDENTITY MANAGEMENT

Access to PX.Center's informational resources must be granted in a restrictive and controlled manner, based on the principles of least privilege (PoLP) and need to know. The Organization must ensure that each user has access strictly limited to the information and systems indispensable to the performance of their functional responsibilities.

The granting, modification, or revocation of such access must follow formal authorization processes, with periodic review of permissions being mandatory to ensure they remain aligned with the current activities of the employee or third party.

Authentication to PX.Center's systems and networks must be performed using individual and non-transferable credentials, with the sharing of passwords or the use of generic accounts for routine activities being prohibited. The Organization must implement multi-factor authentication (MFA) mechanisms and monitor access logs for audit and incident investigation purposes, ensuring the traceability of all actions performed on its technological infrastructure.

All access credentials, including passwords, tokens, API keys, and other authentication means, must be stored and transmitted securely, in accordance with encryption standards and using password vaults or equivalent corporate solutions, with annotation in insecure locations, storage in plain text, or transmission via unauthorized channels, such as personal email or messaging applications, being prohibited.

The creation, renewal, and recovery of passwords must follow established internal procedures, ensuring strong combinations, periodic rotation where applicable, and immediate change in the event of suspected compromise.

Accounts with administrative privileges must be managed by a Privileged Access Management (PAM) solution, with mandatory multi-factor authentication, auditable session recording, periodic credential rotation, and use exclusively for tasks requiring such privileges. Local administrator accounts on workstations must be disabled or managed by the corporate PAM solution, in accordance with Control A.8.2 of ISO/IEC 27001:2022.

The processes of creating, modifying, and revoking user accounts must follow formal identity management workflows, ensuring that new accesses are duly authorized, that role changes result in the immediate adjustment of profiles, and that access for terminated employees or disengaged third parties is revoked within a maximum of 15 (fifteen) business days. The maintenance of orphaned or unnecessary accounts is prohibited and must be periodically verified by the responsible areas in conjunction with the technology department.

5.6 USE OF THE INTERNET, SOCIAL MEDIA, AND ARTIFICIAL INTELLIGENCE

Internet access provided by the Organization is intended exclusively to support professional activities. PX.Center may implement content filters, monitor data traffic, and block access to websites that present security risks or are incompatible with its ethical guidelines.

The use of social media from corporate resources is permitted for employees whose business functions require it, particularly in the Marketing and Commercial areas, restricted to institutional purposes, with the disclosure of confidential information or personal data through those channels being prohibited. For all other roles, personal use of social media from corporate resources is prohibited.

Regarding the use of Artificial Intelligence tools, the entry of personal data, trade secrets, proprietary source code, or confidential organizational information into public generative AI tools without prior security evaluation and CISO approval is strictly prohibited. All AI-generated

output must be reviewed by a qualified professional before application, with final responsibility for the content or code resting entirely with the human user.

The use of AI for asset generation must respect intellectual property rights, with the infringement of third-party copyrights that could compromise PX.Center being prohibited.

5.7 SECURE SOFTWARE DEVELOPMENT

As technology is PX.Center's core business, the systems development lifecycle must integrate security controls at every phase (Security by Design), with security being a mandatory requirement from product conception. Logical and physical segregation between development, staging, and production environments is mandatory; under no circumstances may actual client data or personal data protected by the LGPD be used in development or test environments.

When data with a structure similar to production is required for testing purposes, masking, pseudonymization, or synthetic data generation techniques must be employed so as to preserve the format without exposing real personal information, in accordance with Control A.8.11 of ISO/IEC 27001:2022 and Art. 13 of the LGPD. All source code must undergo security analysis (SAST/DAST) prior to promotion to production, in order to identify and correct vulnerabilities before they can be exploited.

The use of third-party libraries or open-source components must be monitored to ensure the use of stable versions free from known vulnerabilities. Access to PX.Center's code repositories is restricted and auditable, and any modification to critical systems must go through a peer review (code review) process.

5.8 OPERATIONS AND NETWORK SECURITY

PX.Center must maintain technical and administrative controls to ensure the integrity of systems and the security of communications transmitted across its infrastructure. Network operations must be protected by perimeter defense mechanisms, encryption of data in transit, and continuous monitoring tools against intrusions and malicious code. Network and server configuration management is restricted to authorized professionals and must be documented to ensure traceability and compliance with the Organization's security standards.

Any significant change to the technological environment must follow a formal change management process aimed at mitigating negative impacts on system stability and information security.

PX.Center must implement Data Loss Prevention (DLP) controls to monitor and block the unauthorized transmission of information classified as Confidential or Restricted via channels such as email, non-corporate cloud storage, removable devices, and communication applications, with rules defined by the CISO and reviewed semi-annually, in accordance with Control A.8.12 of ISO/IEC 27001:2022.

PX.Center must conduct penetration tests (pentest) at least annually on its critical systems and infrastructure, conducted by a qualified internal team or an independent specialist third party, with results reported to the CISO and the CSIP. Incident response simulation exercises (tabletop exercises) must be conducted at least semi-annually to validate the effectiveness of response plans and team capabilities, in accordance with §5.29 of ISO/IEC 27001:2022.

Operational continuity must be ensured through rigorous backup processes and disaster recovery plans, with the Organization responsible for ensuring that critical data is stored securely and tested periodically to validate its availability in the event of failures or incidents. Backups are subject to retention and disposal policies aligned with applicable legal, contractual, and regulatory requirements, as well as the principles of data necessity and minimization.

Backups containing Confidential or Restricted information must receive the same level of protection as production databases, including with respect to access control, encryption, and secure disposal at the end of their lifecycle.

PX.Center must establish guidelines for vulnerability management, conducting systematic security scans and updates. It is the responsibility of each user to ensure the safe use of corporate email, to protect the contents of their inbox and outbox, to avoid storing sensitive information in unauthorized folders or services, and to strictly observe guidelines for preventing phishing attacks and other forms of social engineering.

The use of a corporate email address for registrations or purposes unrelated to professional activities is prohibited, as is the forwarding of corporate information to personal or unauthorized email accounts; any suspicious message, link, or potentially malicious attachment must be immediately reported through the official security channels.

Remote access to PX.Center's systems and information must be conducted exclusively through authorized corporate channels, such as virtual private networks (VPN/ZTNA) and strong authentication mechanisms, using duly managed and protected devices. Access to Confidential or Restricted information using public networks or unauthorized devices without proper cryptographic protection and the additional controls defined in the supplementary technical standards is prohibited.

5.9 INCIDENT MANAGEMENT AND BUSINESS CONTINUITY

PX.Center must maintain a dedicated structure for the detection, response, and remediation of information security incidents and events that may compromise the privacy of personal data. Every event identified as a real or potential threat to the confidentiality, integrity, or availability of the Organization's assets must be reported immediately through official communication channels; the official information security channel is security@px.center and the official channel for breaches involving privacy and personal data protection is dpo@px.center.

Incident management is coordinated by the Information Security Manager (CISO), who has the authority to activate the Incident Response Plan and mobilize the areas necessary for damage containment and root cause investigation. In the event of incidents involving personal data, the Organization must conduct a risk and impact analysis to fulfill notification obligations before the ANPD and the affected data subjects, in accordance with the deadlines and requirements established by current legislation and the Incident Management Policy (POL-SIP-002).

PX.Center must conduct post-incident investigations to identify control failures and implement preventive improvements, maintaining all incident records and actions taken securely for audit and legal evidence purposes. To ensure institutional resilience, the Organization must

establish formal Business Continuity guidelines and plans designed to keep critical activities operational in the face of serious failures or disasters, which must be periodically reviewed and tested.

Compliance with and cooperation in recovery protocols are mandatory for all departments, ensuring that the resumption of operations occurs in an orderly and secure manner.

5.10 COMPLIANCE, AUDIT, AND SANCTIONS

Compliance with the guidelines established in this policy is mandatory for all individuals associated with PX.Center, which must conduct an Internal ISMS Audit Program, executed at least annually by auditors independent of the audited area, in accordance with §9.2 of ISO/IEC 27001:2022, with results documented and reported to the CSIP and Senior Management, in addition to monitoring and other technical and administrative verifications designed to ensure compliance with security controls and applicable legislation.

Non-compliance with the standards of this ISP or its supplementary regulations may result in disciplinary and legal measures proportionate to the severity of the infringement. For employees, penalties may include a verbal or written warning, suspension, or termination of the employment contract for cause, without prejudice to applicable civil and criminal liability. In the case of service providers and commercial partners, the violation may result in immediate suspension of access, application of contractual penalties, or motivated termination of the commercial relationship with PX.Center.

6. RESPONSIBILITIES

Senior Management approves this policy, provides the necessary resources for the ISMS, conducts periodic management reviews of the system, and is accountable for the Organization's strategic commitment to information security and legal compliance.

The Information Security and Privacy Committee (CSIP) deliberates on investments, approves normative revisions, approves the Organization's risk methodology and criteria, arbitrates interpretation conflicts, decides on unaddressed cases, and monitors the effectiveness of internal controls, with the obligation to intervene in processes that present critical risks.

The Information Security Manager (CISO) is responsible for the technical implementation of the ISMS, for coordinating incident responses, for vulnerability management, for defining DLP rules, and for auditing logical and physical controls.

The Data Protection Officer (DPO) conducts official communication with the ANPD, safeguards the rights of data subjects, and acts transversally to ensure LGPD compliance in all personal data processing activities.

Area managers are responsible for applying this policy within their processes, ensuring the adequacy of their teams' access rights, and communicating relevant events and changes to the CISO and the DPO.

Information owners assign the classification level of assets under their responsibility and define the respective access rights.

Employees, interns, service providers, consultants, and commercial partners must observe the established standards of conduct, maintain the confidentiality of information, protect the credentials and assets in their care, and immediately report any suspicious event through official channels.

Failure to comply with the responsibilities described herein subjects the offender to applicable disciplinary and legal measures, in accordance with current legislation and PX.Center's employment or service contracts.

7. RECORDS MANAGEMENT

Records generated by the application of this policy reside in PX.Center's official governance repositories. Versions of this policy, CSIP minutes, the Statement of Applicability (PLC-17-002), ISMS management review records, impact assessments, and audit reports must be maintained in the SGI documentary repository. Security incident records and the respective treatment actions must be preserved in accordance with the Incident Management Policy (POL-SIP-002).

Access logs, system usage records, and network traffic must be retained for the periods defined in the SGI's supplementary technical standards, subject to at least annual review, and in applicable legislation. The asset inventory must be kept up to date by the technology department. It is mandatory to preserve the integrity of records, with access restricted on a need-to-know basis, and to keep them available for internal and external SGI audits.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on 24/06/2026 and is valid for an indefinite period, fully revoking any prior provisions, communications, or practices addressing the same subject matter within PX.Center. The CSIP must conduct ordinary annual reviews, or extraordinary reviews at any time, to ensure the document remains current in light of technological changes, new legislation, or changes in business risk. Approval of this policy and its revisions is the responsibility of the CISO / CTO, under resolution of the CSIP.

Unaddressed cases, exceptional situations, or ambiguous interpretations not covered by this policy must be submitted for analysis and resolution by the CSIP, and no exception to the rules established herein is permitted without the proper formalization and written approval by Senior Management, following a technical impact and risk assessment. It is the responsibility of all PX.Center members to remain up to date with the current version of this policy, which is permanently available for consultation in the official governance repositories.

The nullity or invalidity of any isolated item in this document does not affect the validity and effectiveness of the remaining provisions.

The application of this document does not exclude other obligations set forth in employment contracts, service agreements, or specific codes of conduct adopted by the Organization. The nullity or invalidity of any isolated item in this policy, as declared by a competent authority, does not affect the validity and effectiveness of the remaining provisions, which remain in full force for all legal purposes.

9. ANNEXES

There are no annexes. Operational records reside in the systems indicated in the Records Management section.

CHANGE HISTORY

Version	Date	Author	Change Description
00	14/01/2026	Cybersecurity Department	Creation and Review
01	26/01/2026	Legal	Review
02	24/06/2026	SGI	Recoding to acronym