Information Security Policy

Corporate guidelines for protecting PX.Center's information assets and establishing the Information Security Management System (ISMS)

Code	POL-SEG-001
Responsible Area	Information Security
Issue Date	June 24, 2026
Approval Authority	CISO / CTO

1. PURPOSE / OBJECTIVE

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

Information security is understood by the Organization not merely as an operational control, but as a business enablement asset and a mandatory resilience requirement, aimed at ensuring strict observance of 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), so as to mitigate technological and human risks and ensure that the processing of personal and corporate data complies with Law 13.709/2018 (Brazilian General Data Protection Law — LGPD) and with international security standards.

The commitment of PX.Center's Senior Management to this normative body reflects its relentless pursuit of reputational integrity and compliance with existing contractual and regulatory obligations, with adherence to these standards being an inherent duty of all its stakeholders.

2. SCOPE / APPLICABILITY

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

Compliance with these guidelines covers all information assets, including software systems, databases, communication networks, physical devices, cloud computing environments, and documents. Compliance is an essential condition for maintaining an employment or contractual relationship with PX.Center, and access to the Organization's informational resources presupposes the 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 Non-Disclosure Agreement (NDA) or equivalent document before commencing their activities, with a term that extends beyond the termination of the relationship for a period defined in complementary technical standards, no 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, compatible with the risks of the activities performed, and may be subject to risk assessments, audits, and additional control requirements.

Suppliers 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 Suppliers must undergo a security assessment and due diligence before contracting and annually during the term of the contract.

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

3. TARGET USERS / AUDIENCE

Senior Management, Information Security and Privacy Committee (ISPC), Chief Information Security Officer (CISO), Data Protection Officer (DPO), department managers, information asset owners, and all employees, interns, service providers, consultants, and business partners who use technological resources or process information on behalf of PX.Center.

4. REFERENCE DOCUMENTS

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

The absence of detailed technical guidance on a specific control in this policy does not exempt any individual from complying with the obligations contained in the complementary technical standards. In the event of conflict between this document and 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 guidelines and controls applicable to all entities under its management. Senior Management

assumes responsibility for providing the necessary resources and strategic support to the ISMS, ensuring alignment between asset protection and business objectives.

The supervisory structure is composed of:

- The **Information Security and Privacy Committee (ISPC)** — a multidisciplinary collegiate body responsible for deliberating on investments, approving normative revisions, and monitoring the effectiveness of internal controls, with authority to intervene in processes presenting critical risks to operational continuity or legal compliance.
- The **Chief Information Security Officer (CISO)** — responsible for the technical implementation of the ISMS, coordination of incident responses, and auditing of logical and physical controls across all business units.
- The **Data Protection Officer (DPO)** — responsible for official communication with the National Data Protection Authority (ANPD) and for safeguarding the rights of data subjects, operating transversally to ensure compliance with the LGPD.

Every employee and third party has a duty to observe the established conduct standards, safeguard the confidentiality of information, and 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, documenting which controls in Annex A of ISO/IEC 27001:2022 are applicable to the Organization, with the respective justifications for inclusion or exclusion and the implementation status, pursuant to requirement §6.1.3 of the standard, constituting the basis for ISMS auditability and certifiability.

PX.Center's Senior Management must conduct a management review of the ISMS at least annually, with a minimum agenda defined in complementary technical standards, covering performance indicators, audit results, risk treatment status, and improvement decisions, with results formally recorded pursuant to §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 in the management review conducted by Senior Management at least annually, pursuant to §6.2 of ISO/IEC 27001:2022.

PX.Center is committed to the continuous improvement of its ISMS, conducting periodic reviews of its objectives, indicators, and controls, to adapt them to technological, regulatory, and business risk context changes. Senior Management must ensure that the results of assessments, audits, and incidents are considered in the update of this policy and related regulations.

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 treat threats that could compromise operational continuity or the privacy of data under 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 complementary document formally approved by the ISPC, with a minimum annual review, pursuant to §6.1.2 of ISO/IEC 27001:2022.

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

To ensure appropriate handling and access control, information in the Organization must be categorized according to its level of criticality and sensitivity:

- **Public Information:** Information whose external access does not generate a negative impact on PX.Center or third parties.
- **Internal Information:** Data for routine operational use that, if improperly disclosed, may cause minor operational or administrative damage.
- **Confidential Information:** Strategic data, trade secrets, or personal data, access to which is restricted exclusively to individuals with a functional need to know.
- **Restricted Information:** Critical, highly sensitive data whose leak or loss may result in severe legal sanctions, irreparable reputational damage, or serious financial harm.

The protection of information also encompasses physical documents and non-digital storage media. Records containing Internal, Confidential, or Restricted information must be stored in adequately protected locations, with physical access controlled and compatible 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 — to prevent 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 complementary 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 informed that they should have no expectation of privacy regarding the use of corporate technological resources and must use them in observance of 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 to reflect 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 program's effectiveness, 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 facilities is controlled by formal identification mechanisms, with mandatory use of identification badges by all employees, interns, service providers, and visitors during their stay on the premises. Entry into internal areas, especially those classified as critical, requires authentication via access control systems, which may include badge validation and facial recognition, ensuring the traceability of all entries and exits.

Sharing of badges or allowing entry of unauthorized persons is prohibited; any loss, misplacement, or suspected misuse must be immediately reported through official channels. Every third party or visitor must have prior registration and be linked to an internal sponsor, with access conditional on identity verification and 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 the user responsible for the physical integrity and logical security of the assets under their care.

The Organization must maintain an updated asset inventory with records of the responsible party, location, and status. The installation of unauthorized software, the use of personal equipment in violation of internal regulations, and the modification of security configurations without prior approval from the technology department are prohibited. Upon dismissal, change of role, or termination of contract, all assets and information belonging to PX.Center must be immediately returned, in accordance with internal return and access revocation procedures.

The use of personal devices to access corporate resources (BYOD) is only permitted when expressly authorized and conditional on meeting the security requirements defined in specific technical standards, including anti-malware protection mechanisms, encryption, and remote management capability. 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 information 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 essential to the performance of their functional duties.

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

Authentication in PX.Center's systems and networks must be performed using individual, non-transferable credentials. Sharing of passwords or use of generic accounts for routine activities is 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, observing encryption standards and the use of password vaults or equivalent corporate solutions. Noting credentials in insecure locations, storing them in plain text, or transmitting them via unauthorized channels such as personal email or messaging applications is prohibited.

Password definition, renewal, and recovery must follow established internal procedures, ensuring strong combinations, periodic rotation where applicable, and immediate change upon suspicion of 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 exclusive use 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 permissions, and that accesses of dismissed employees or disengaged third parties are 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 together with the technology department.

5.6 Internet Use, 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 Marketing and Sales areas, restricted to institutional purposes, with the disclosure of confidential information or personal data through these channels being prohibited. For all other roles, personal use of social media from corporate resources is prohibited.

Regarding the use of Artificial Intelligence tools, it is strictly prohibited to insert personal data, trade secrets, proprietary source code, or the Organization's confidential information into public generative AI tools without prior security assessment and CISO approval. All AI-generated results must be reviewed by a qualified professional before application, with full responsibility for the content or code resting with the human user.

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

5.7 Secure Software Development

As technology is PX.Center's core business activity, the system development lifecycle must integrate security controls across all phases (Security by Design), with security being a mandatory requirement

from the conception of the product. Logical and physical segregation between development, staging, and production environments is mandatory; under no circumstances may real customer data or personal data protected under the LGPD be used in development or test environments.

When data with production-like structure is required for testing purposes, techniques of data masking, pseudonymization, or synthetic data generation must be employed, so as to preserve the format without exposing real personal information, pursuant to Control A.8.11 of ISO/IEC 27001:2022 and Art. 13 of the LGPD. All source code must undergo security analysis (SAST/DAST) before promotion to production, to identify and correct flaws 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 change 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 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. The management of network and server configurations 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, pursuant to Control A.8.12 of ISO/IEC 27001:2022.

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

Operational continuity must be ensured by rigorous backup processes and disaster recovery plans, with the Organization being responsible for ensuring that critical data is stored securely and tested periodically to validate 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 with the principles of data minimization.

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

PX.Center must establish vulnerability management guidelines, conducting systemic security scanning and updates. Every user is responsible for the safe use of corporate email, protecting the contents of

their inboxes and outboxes, avoiding the storage of sensitive information in unauthorized folders or services, and strictly following guidance on preventing phishing attacks and other forms of social engineering.

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

Remote access to PX.Center's systems and information must be carried out exclusively via authorized corporate channels, such as virtual private networks (VPN/ZTNA) and strong authentication mechanisms, using appropriately managed and protected devices. Accessing Confidential or Restricted information using public networks or unauthorized devices without adequate cryptographic protection and the additional controls defined in complementary 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 immediately reported through official communication channels. The official information security channel is security@px.center and the official channel for violations involving privacy and personal data protection is dpo@px.center.

Incident management is coordinated by the Chief Information Security Officer (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 its notification obligations before the ANPD and the affected data subjects, in accordance with the deadlines and requirements established by applicable legislation and the Incident Management Policy (POL-SEG-002).

PX.Center must conduct post-incident investigations to identify control failures and implement preventive improvements, maintaining all records of incidents and actions taken securely for audit and legal evidence purposes. To ensure institutional resilience, the Organization must establish formal guidelines and Business Continuity Plans designed to keep critical activities operational in the face of serious failures or disasters, which must be periodically reviewed and tested.

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

5.10 Compliance, Auditing, and Sanctions

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

Non-compliance with the standards of this ISP or its complementary regulations may result in disciplinary and legal measures proportional to the severity of the infringement. For employees, penalties may include verbal or written warnings, suspension, or termination of the employment contract for cause, without prejudice to applicable civil and criminal liabilities. For service providers and business partners, the violation may result in immediate suspension of access, application of contractual fines, or justified termination of the commercial relationship with PX.Center.

6. RESPONSIBILITIES

Senior Management approves this policy, provides the resources necessary 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 (ISPC)** deliberates on investments, approves normative revisions, approves the Organization's risk methodology and criteria, arbitrates interpretation conflicts, decides on omitted cases, and monitors the effectiveness of internal controls, intervening in processes that present critical risks.

The **Chief Information Security Officer (CISO)** is responsible for the technical implementation of the ISMS, coordination of incident responses, vulnerability management, definition of DLP rules, and auditing of 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.

Department managers are responsible for applying this policy in their processes, ensuring appropriate access controls for their teams, and communicating relevant events and changes to the CISO and DPO.

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

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

Failure to fulfill the described responsibilities subjects the offender to the applicable disciplinary and legal measures, pursuant to 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. The versions of this policy, ISPC meeting minutes, the Statement of Applicability (PLC-17-002), ISMS management review records, impact assessments, and audit reports must be maintained in the ISMS document repository. Security incident records and the respective response actions must be preserved in accordance with the Incident Management Policy (POL-SEG-002).

Access logs, system usage records, and network traffic must be retained for the periods defined in the ISMS's complementary technical standards, with a minimum annual review, and in accordance with

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 ISMS audits.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on June 24, 2026, and remains valid indefinitely, fully revoking any prior provisions, communications, or practices addressing the same subject matter within PX.Center. The ISPC must conduct ordinary annual reviews, or extraordinary reviews at any time, to ensure the document's currency in light of technological changes, new legislation, or changes in business risks. The approval of this policy and its revisions is the responsibility of the CISO / CTO, under ISPC deliberation.

Omitted cases, exceptional situations, or ambiguous interpretations not addressed in this policy must be submitted for ISPC analysis and deliberation, and no exception to the rules established herein is permitted without proper formalization and written approval by Senior Management, after a technical impact and risk assessment. It is the responsibility of all PX.Center members to keep themselves updated on the current version of this policy, permanently available for consultation in the official governance repositories.

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

The application of this document does not exclude other obligations set forth in employment contracts, service contracts, or specific codes of conduct adopted by the Organization. The nullity or invalidity of any isolated item of this policy, as declared by a competent authority, does not impair 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.

REVISION HISTORY

Version	Date	Author	Description
00	January 14, 2026	Cybersecurity Department	Creation and Review
01	January 26, 2026	Legal	Review
02	June 24, 2026	ISMS	Recodification to acronym-based code