Information Lifecycle Policy

Classification, labeling, transfer, retention, and secure disposal of information at PX.Center

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

1. PURPOSE / OBJECTIVE

This policy establishes the mandatory guidelines for classification, labeling, transfer, retention, and secure disposal of information throughout its entire lifecycle at PX.Center, in compliance with controls A.5.9 through A.5.14, A.5.33, A.7.10, A.7.14, A.8.10, and A.8.12 of ISO/IEC 27001:2022, and in integration with POL-SEG-001 (Information Security Policy).

This document defines how the Organization classifies, labels, shares, retains, and eliminates information to preserve its confidentiality, integrity, and availability in any format or medium.

2. SCOPE / APPLICABILITY

This policy applies to information processed by PX.Center in any format or medium — whether physical, digital, or oral — and to every person who accesses or uses it: employees, interns, service providers, consultants, and partners.

The definition of PX.Center as the reference entity covers the other CNPJs (legal entities) within the group, eliminating the need for a document specific to each entity. The provisions set forth herein are observed together with POL-SEG-001 and with the other security, privacy, and access control regulations.

3. TARGET AUDIENCE

Executive leadership, CISO, CTO, Information Security Leader, area managers acting as information owners, Legal and Privacy departments, and all employees, service providers, and third parties who process the Organization's information.

4. REFERENCE DOCUMENTS

- ISO/IEC 27001:2022 (controls A.5.9 through A.5.14, A.5.33, A.7.10, A.7.14, A.8.10, A.8.12)
- Law 13,709/2018 — Brazilian General Data Protection Law (LGPD)
- Law 12,965/2014 — Brazilian Internet Civil Rights Framework (Marco Civil da Internet)
- POL-SEG-001: Information Security Policy
- POL-SEG-006: Cryptographic Controls Policy
- POL-SEG-016: Access Control Policy
- POL-SGI-002: Records Management Policy
- POL-SEG-005: Disposal and Destruction Policy
- POL-SEG-003: Backup Policy
- POL-SEG-002: Incident Management Policy
- POL-SEG-029: Privacy and Personal Data Protection Policy
- INT-SEG-001: Information Classification Instruction
- POL-SEG-011: Supplier Security Policy

5. GUIDELINES / RULES / CONTROLS

5.1 Information Classification

All PX.Center information is classified according to its sensitivity and criticality. It is the duty of the manager who originates or uses the information to assign the classification, with support from Information Security. Four levels are mandatory:

- **Public:** Information whose external disclosure causes no harm, such as institutional material already published.
- **Internal:** Information restricted to the Organization's staff, such as communications and work instructions.
- **Restricted:** Information whose access is limited to specific areas or functions, such as financial reports and project data.
- **Confidential:** Highly critical information — including sensitive personal data, trade secrets, proprietary source code, and credentials — whose disclosure causes material legal, financial, or reputational harm.

5.2 Information Labeling

Labeling is mandatory for information classified as Internal, Restricted, or Confidential. In physical media, the indication appears as a stamp, label, header, or footer. In digital media, corporate sensitivity labels are applied in accordance with INT-SEG-001. For oral communications dealing with Restricted or Confidential matters, the person responsible signals the sensitive nature at the outset and limits participation to the individuals involved.

5.3 Transfer and Sharing

Information transfer takes place only through approved corporate channels: corporate email, corporate collaboration tools, and corporate repositories. Sharing information without a legitimate purpose and without the recipient's need to know is prohibited. Restricted or Confidential information must be transmitted with recipient access control and encryption, in accordance with POL-SEG-006. The integrated corporate messaging application is restricted to customer service and is prohibited for Restricted or Confidential data.

5.4 Relationship with Third Parties and Confidentiality Agreements

Sharing classified information with third parties is contingent upon the signing of a non-disclosure agreement (NDA) and contractual clauses covering confidentiality, minimum security controls, incident notification, and return or secure disposal upon termination of the relationship. Security requirements applicable to suppliers and third parties follow POL-SEG-011 (Supplier Security Policy); where personal data processing is involved, the LGPD and POL-SEG-029 must also be observed.

5.5 Information Retention

Retention observes the periods required by law, regulation, or contract, as well as the Organization's operational needs. Retaining information beyond the necessary period is prohibited. Backups follow POL-SEG-003 and records follow POL-SGI-002. Once the retention period expires, information is eliminated, anonymized, or retained only with documented justification.

5.6 Secure Disposal and Destruction

At the end of the retention period, information and the media on which it is stored are disposed of irreversibly and in proportion to the classification. Disposal and secure destruction procedures — such as shredding, overwriting, physical destruction, and disposal logging — follow POL-SEG-005 (Disposal and Destruction Policy).

5.7 Exceptions

Every exception to this policy must be prior, substantiated, time-limited, and accompanied by compensatory measures. Information Security evaluates and approves the exception and records the justification, scope, term, and additional controls, with periodic review until return to the standard guideline.

6. RESPONSIBILITIES

Executive leadership approves this policy and provides the resources necessary for its execution. The CISO and CTO define information lifecycle controls and are accountable for their maintenance. The Information Security Leader coordinates policy implementation, evaluates exceptions, and leads incident response in accordance with POL-SEG-002. Area managers, acting as information owners, classify the information under their responsibility and ensure their teams comply with this policy. The Legal department reviews NDAs and contractual confidentiality clauses.

Users protect information under their custody, observe classification and labeling, and report incidents through the channel security@px.center; privacy and LGPD matters are directed to dpo@px.center.

7. RECORDS MANAGEMENT

Records under this policy include classification records, approved exceptions, and disposal evidence for sensitive information. Sensitivity labels reside in the corporate classification solution. Versions of this policy reside in the ISMS document repository. It is mandatory to preserve the integrity of records, with access restricted by need-to-know, and to keep them available for internal and external ISMS audits. Incidents involving information follow the treatment established in POL-SEG-002.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on June 24, 2026, and remains valid for an indefinite period. Information Security reviews the document annually or in response to a legal or regulatory change, a relevant incident, or the adoption of new technology that affects the controls defined herein. Non-compliance with this policy subjects the offender to the disciplinary measures set forth in PX.Center's internal regulations.

9. ANNEXES

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

CHANGE HISTORY

Version	Date	Author	Description
00	Feb 9, 2026	Cybersecurity Department	Creation and review
01	Jun 24, 2026	SGI	Recoding to acronym-based numbering