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:	*24/06/2026*
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 conformance 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-SIP-001 (Information Security Policy).

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

2. SCOPE/APPLICABILITY

This policy applies to information handled by PX.Center in any format or medium — 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 within the group, eliminating the need for entity-specific documents. The provisions established herein are to be observed in conjunction with POL-SIP-001 and the other applicable security, privacy, and access-control policies.

3. USERS/TARGET AUDIENCE

Executive leadership, CISO, CTO, Information Security Lead, area managers in their capacity as information owners, Legal and Privacy teams, 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)
- Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD)
- Lei 12.965/2014 (Marco Civil da Internet)
- POL-SIP-001: Information Security Policy
- POL-SIP-006: Cryptographic Controls and Usage Policy
- POL-SIP-016: Access Control Policy
- POL-SGI-002: Records Control Policy
- POL-SIP-005: Disposal and Destruction Policy
- POL-SIP-003: Backup Policy
- POL-SIP-002: Incident Management Policy
- POL-SIP-029: Privacy and Personal Data Protection Policy
- INT-SIP-005: Information Classification
- POL-SIP-011: Supplier Security Policy

5. GUIDELINES / RULES / CONTROLS

5.1 INFORMATION CLASSIFICATION

All information at PX.Center is classified according to its sensitivity and criticality. It is the responsibility 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 already-published institutional material. Internal: information restricted to the Organization's workforce, such as internal communications and work instructions. Restricted: information whose access is limited to specific departments or roles, such as financial reports and project data. Confidential:

high-criticality information, such as sensitive personal data, trade secrets, proprietary source code, and credentials, whose disclosure causes significant legal, financial, or reputational harm.

5.2 INFORMATION LABELING

Labeling is mandatory for information classified as Internal, Restricted, or Confidential. In physical media, the designation appears as a stamp, label, header, or footer. In digital media, corporate sensitivity labels are applied in accordance with INT-SIP-005. In oral communications involving Restricted or Confidential matters, the responsible party signals the sensitive nature at the outset and limits participation to the individuals directly involved.

5.3 TRANSFER AND SHARING

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

5.4 THIRD-PARTY RELATIONSHIPS AND CONFIDENTIALITY AGREEMENTS

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

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-SIP-003 and records follow POL-SGI-002. Once the retention

period expires, information is disposed of, anonymized, or retained only upon documented justification.

5.6 SECURE DISPOSAL AND DESTRUCTION

Upon expiry of the retention period, information and the media on which it is stored are disposed of in an irreversible manner proportionate to the classification level. Secure disposal and destruction procedures — including shredding, overwriting, physical destruction, and disposal records — follow POL-SIP-005 (Disposal and Destruction Policy).

5.7 EXCEPTIONS

Any exception to this policy must be prior, substantiated, time-limited, and accompanied by compensating controls. Information Security evaluates and approves the exception and records the justification, scope, duration, and additional controls, with periodic review until reversion to the standard guideline.

6. RESPONSIBILITIES

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

Users protect the information in their custody, observe classification and labeling requirements, 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 SGI document repository. Maintaining the integrity of records is mandatory, with access restricted on a need-to-know basis, and records must remain available for internal and external SGI audits. Incidents involving information follow the response procedures of POL-SIP-002.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on 24/06/2026 and remains valid for an indefinite term. Information Security reviews the document annually or upon any legal or regulatory change, significant

incident, or adoption of new technology that affects the controls defined herein. Non-compliance with this policy subjects the offender to the disciplinary measures set out in PX.Center's internal regulations.

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	09/02/2026	Cybersecurity Department	Creation and Review
01	24/06/2026	SGI	Recoded to acronym-based identifier