Acceptable Use Policy

Defines the mandatory rules for the safe and appropriate use of PX.Center's information assets (corporate systems, email, internet, devices, and social media), in compliance with ISO/IEC 27001:2022 and the Brazilian General Data Protection Law (LGPD).

Code	POL-SEG-013
Responsible Area	Information Security
Issue Date	June 24, 2026
Approval Authority	CISO / CTO

1. PURPOSE / OBJECTIVE

This policy establishes the mandatory rules for the safe and appropriate use of PX.Center's information assets, preventing risks to the confidentiality, integrity, and availability of information. It integrates with POL-SEG-001 (Information Security Policy), from which it derives, and complies with ISO/IEC 27001:2022. The policy defines the acceptable use of corporate systems, email and messaging, internet, devices, and mobile computing, remote work, and social media, as well as the responsibilities of each party and the consequences of non-compliance.

Every user with direct or indirect access to PX.Center's information assets is required to operate in accordance with the controls defined herein.

2. SCOPE / APPLICABILITY

This policy applies to all employees, interns, suppliers, service providers, partners, and third parties who have direct or indirect access to PX.Center's information assets, regardless of their physical location or work modality. The policy covers:

- Physical, logical, and human information assets that support the processing, storage, or transmission of corporate information;
- Corporate systems, email and other messaging channels, corporate internet, networks, and fixed and mobile devices;
- On-site and remote work, in any organizational unit or technology environment.

This policy applies in conjunction with POL-SEG-001 (Information Security Policy), to which it is subordinate.

3. TARGET AUDIENCE

All employees, interns, suppliers, service providers, partners, and third parties with access to PX.Center's information assets; asset owners; area managers; the IAM (Identity & Access Management) Team; the IT department; the CISO / CTO; and the Information Security team responsible for governing this policy.

4. REFERENCE DOCUMENTS

- ISO/IEC 27001:2022 (Information Security Management System)
- Law 13,709/2018 (Brazilian General Data Protection Law — LGPD)
- POL-SEG-001: Information Security Policy (ISP)
- POL-SEG-029: Privacy and Personal Data Protection Policy
- POL-SGI-001: Information Lifecycle Policy
- POL-SEG-008: Mobile Device and Remote Work Policy
- POL-SEG-012: Bring Your Own Device (BYOD) Policy

- POL-SEG-010: Clean Desk and Clear Screen Policy
- POL-SEG-003: Backup and Recovery Policy
- POL-SEG-002: Incident Management Policy
- POL-SGI-002: Records Control Policy
- POL-SEG-016: Access Control Policy
- POL-SEG-022: Malware Protection Policy

5. GUIDELINES / RULES / CONTROLS

5.1 Acceptable Use of Assets

Information assets must be used exclusively for purposes related to approved corporate activities. Access must always be tied to the role profile and approved by the responsible manager and the IT department. Use must comply with Brazilian legislation, internal standards, and contractual obligations. Access logs, firewall reports, and authorization records constitute audit evidence. The following are strictly prohibited:

- Using assets for illegal, offensive, or discriminatory activities;
- Installing or running unauthorized software;
- Sharing credentials or accessing third-party accounts;
- Copying, transferring, or disclosing information without authorization;
- Cryptocurrency mining, work-unrelated gaming, or excessive use of resources for personal purposes.

5.2 Asset Responsibility

Asset owners must ensure the implementation of appropriate security controls. Users must protect assets against unauthorized access, loss, theft, or damage. The IT department must maintain an up-to-date and protected asset inventory. Removing assets from the organization's premises requires formal management authorization; mobile devices containing sensitive data must have disk encryption enabled, and transport must follow the secure asset transport procedure.

Upon contract termination, all assets must be returned within 48 hours of departure, except in cases where the employee is working remotely far from the main office. The IT department must perform a secure data wipe, and the responsible manager must confirm the return and record it in the inventory.

5.3 Antivirus Protection

Corporate antivirus and EDR (Endpoint Detection and Response) solutions are kept active on all devices. Users are prohibited from disabling, removing, bypassing, or altering the configuration of security agents (EDR, DLP, MDM). The management, updating, and monitoring of malware protection follow POL-SEG-022 (Malware Protection Policy).

5.4 Account Authorization and Responsibilities

Each account is personal, individual, and non-transferable. Sharing usernames, passwords, tokens, verification codes, or MFA devices with any person — including managers, colleagues, third parties, or suppliers — is strictly prohibited. The user is responsible for all actions performed under their account

until the formal reporting of a suspected compromise, must use MFA in systems that require it, and must only approve push authentication requests when they themselves initiate the access.

Loss, theft, or suspected compromise of credentials or an MFA device must be reported immediately to security@px.center. The granting, review, and deprovisioning of access, password requirements, and secrets management follow POL-SEG-016 (Access Control Policy).

5.5 Clean Desk and Clear Screen

Users must keep their desks free of sensitive information when away and at the end of the workday, and must lock their screen whenever they leave their workstation. Clean desk and clear screen guidelines are defined in POL-SEG-010 (Clean Desk and Clear Screen Policy).

5.6 Internet Use

Corporate internet use is permitted exclusively for professional purposes. The following are prohibited:

- Accessing websites with illegal, pornographic, discriminatory, violent, gambling, or inappropriate content;
- Downloading software, executables, or any content without prior IT department authorization;
- Using a proxy, non-corporate VPN, or any other method to bypass the organization's access restrictions;
- Using corporate internet for personal purposes, external commercial activities, sending spam, participating in forums with controversial personal positions, or any activity that compromises PX.Center's image, resources, or security.

External communication applications must follow the organization's guidelines and may not be used to transfer corporate files without approval. Internet traffic is monitored and audited by the responsible department; inappropriate use subjects the offender to the measures set out in section 5.11.

5.7 Email and Messaging

The use of corporate email and other PX.Center digital channels (instant messaging, corporate chats, collaboration platforms, and video conferencing) is permitted exclusively for professional purposes. Only corporate accounts and channels authorized by the IT department may be used for work activities. The use of personal email, unauthorized messaging applications, or social media for corporate matters is prohibited.

Information classified as Confidential or Sensitive must be transmitted only through protected corporate channels, with encryption or password-protected attachments; the sending of personal data observes the LGPD and the Information Classification Policy. Automatic forwarding of corporate emails to personal or third-party accounts is prohibited, as is opening attachments or links from suspicious senders. Suspicious messages (phishing, malware, social engineering) must be reported immediately to security@px.center.

Attempting to disable or bypass antispam and antivirus filters is prohibited. Sending offensive, discriminatory, illegal, or reputation-damaging content is forbidden; communications must maintain a professional, clear, and objective standard. Corporate communications may be monitored, recorded, and audited.

5.8 Copyright and Intellectual Property

Reproducing, copying, modifying, distributing, or using materials, software, documents, and content without proper formal authorization is prohibited. All material developed in the course of corporate activities — including source code, technical documentation, presentations, and databases — constitutes PX.Center's intellectual property, unless otherwise stipulated by contract.

Only licensed and IT-authorized software may be installed and used on corporate equipment; the use of pirated software, unauthorized versions, or applications that violate intellectual property rights is prohibited. The assignment of rights for external use requires formal management approval. Use of the PX.Center brand, logo, and visual identity is permitted only in materials and publications authorized by management; use in contexts that damage the organization's reputation is prohibited.

5.9 Mobile Computing and Remote Work

The use of mobile devices and remote work to access PX.Center resources and information follows the guidelines of POL-SEG-008 (Mobile Device and Remote Work Policy); the use of personal devices follows POL-SEG-012 (BYOD Policy). Storing corporate information on unauthorized personal devices, media, or cloud services is prohibited.

5.10 Social Media

The use of social media and messaging applications on PX.Center's equipment and devices is authorized exclusively to the business functions responsible for this activity — in particular Marketing and Commercial — using corporate accounts and for promotional and institutional dissemination purposes. Such use is subject to content restrictions: publishing or sharing confidential, restricted, or personal data is prohibited.

For all other roles, personal use of social media and messaging applications on the organization's equipment and devices is prohibited. No employee is authorized to speak on behalf of PX.Center or about internal, restricted, or confidential matters on social media, unless expressly authorized by the Board.

5.11 Monitoring, Incidents, and Consequences

All activities performed on PX.Center's systems, networks, and communication channels may be recorded, monitored, and audited on a continuous and proportionate basis, in compliance with the LGPD. Users are prohibited from attempting to disable, bypass, or interfere with monitoring mechanisms. All users are informed, at the time of hiring or upon adhering to this policy, of the existence and purpose of monitoring.

Every security incident — such as unauthorized access, data leakage, system unavailability, malware infection, device loss or theft, malicious emails, or configuration failures — must be reported immediately to security@px.center and handled in accordance with the Incident Management Policy. Incidents involving personal data must additionally be reported to dpo@px.center, in accordance with POL-SEG-029. Failure to report in a timely manner constitutes a violation of this policy.

Users acknowledge and agree to access monitoring and auditing at the time of onboarding and at each relevant update of this policy.

6. RESPONSIBILITIES

The **CISO and CTO** approve this policy, define security requirements, provide the necessary resources, and oversee compliance with acceptable use at PX.Center. The **Information Security team** implements, manages, and reviews monitoring mechanisms; operates the security@px.center channel; conducts incident investigation and response; and supervises record compliance with ISO/IEC 27001.

The **IT department** maintains the asset inventory, monitoring tools, network filters, and antivirus; provides and maintains secure remote access resources; and ensures the protection, backup, and availability of electronic records. The **IAM Team** creates, modifies, and deprovisions accounts and credentials; authorizes functional accounts; and conducts semi-annual access reviews. **Asset owners** ensure the implementation of appropriate security controls for assets under their responsibility.

Area managers approve access and remote work for their teams, confirm asset return upon departure, and support the application of monitoring measures. The **Data Protection Officer (DPO)** handles incidents involving personal data via dpo@px.center, in accordance with POL-SEG-029. **Users and third parties** use assets exclusively for authorized corporate purposes, protect their credentials and the assets in their custody, and immediately report any incident or suspicion to security@px.center.

7. RECORDS MANAGEMENT

All records generated by the application of this policy are documented, maintained, and controlled in accordance with the PX.Center Records Control Policy. Records include access logs, use authorization evidence, incident reports, semi-annual access reviews, and training evidence; they are stored in electronic files (PDF, DOCX, XLSX), in corporate systems, or in physical copies where applicable.

Control is performed via the Records Management Spreadsheet, with mandatory fields: record type, creation date, responsible party, retention period, storage location, and status. The record owner ensures creation, updating, and maintenance; the Information Security team supervises compliance; and the IT department ensures the protection, backup, and availability of electronic records. Records are kept for the minimum period defined in the Records Control Policy, or for a longer period when required by law, contract, or regulation; disposal occurs through complete and irrecoverable deletion of information.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on June 23, 2026, in the ISMS (Information Security Management System) Portal, with indefinite validity. It is reviewed annually or whenever there are changes to legal and regulatory requirements, relevant security incidents, technological updates, or process changes. Non-compliance with this policy subjects the offender to applicable disciplinary measures — including warning, suspension, access blocking or revocation, and contract termination — commensurate with the severity of the violation, the Brazilian Labor Code (CLT), and the applicable contract, without prejudice to civil and criminal liability under applicable law.

9. ANNEXES

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

CHANGE HISTORY

Version	Date	Author	Description
00	Jun 9, 2025	IT and Cybersecurity Department — IS	Document creation and review
01	Jun 24, 2026	ISMS (SGI)	Recodification to acronym-based code