Acceptable Use Policy

Defines the mandatory rules for the secure and appropriate use of PX.Center information assets (corporate systems, email, internet, devices, and social media), in compliance with ISO/IEC 27001:2022 and LGPD.

Code:	*POL-SIP-013*
Responsible area:	*Information Security*
Issue date:	*24/06/2026*
Approval authority:	*CISO / CTO*

1. PURPOSE/OBJECTIVE

This policy establishes the mandatory rules for the secure and appropriate use of PX.Center information assets, preventing risks to the confidentiality, integrity, and availability of information, in integration with POL-SIP-001 (Information Security Policy), from which it derives, and in compliance with ISO/IEC 27001:2022. The standard 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 information assets is required to operate in compliance 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 information assets, regardless of their physical location or the work arrangement adopted. The standard covers:

a) physical, logical, and human information assets that support the processing, storage, or transmission of corporate information; b) corporate systems, email and other messaging channels, the corporate internet, networks, and fixed and mobile devices; c) in-person and remote work, in any unit or technological environment of the Organization. It applies in conjunction with POL-SIP-001 (Information Security Policy), to which this policy is subordinate.

3. USERS/TARGET AUDIENCE

All employees, interns, suppliers, service providers, partners, and third parties with access to PX.Center 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 standard.

4. REFERENCE DOCUMENTS

- ISO/IEC 27001:2022 (Information Security Management System)
- Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD)
- POL-SIP-001: Information Security Policy (ISP)
- POL-SIP-029: Privacy and Personal Data Protection Policy
- POL-SGI-001: Information Lifecycle Policy
- POL-SIP-008: Mobile Device and Remote Work Policy
- POL-SIP-012: Bring Your Own Device Policy (BYOD)
- POL-SIP-010: Clean Desk and Clear Screen Policy
- POL-SIP-003: Backup Policy

- POL-SIP-002: Incident Management Policy
- POL-SGI-002: Records Control Policy
- POL-SIP-016: Access Control Policy
- POL-SIP-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 evidence for auditing purposes. 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; and running cryptocurrency mining, work-unrelated games, 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 equipment 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 offboarding, except in cases where the employee works remotely at a distance from the main office; the IT department must perform a secure data wipe and the area manager must confirm the return and record it in the inventory.

5.3 ANTIVIRUS PROTECTION

The corporate antivirus and EDR are kept active on all equipment. Users are prohibited from disabling, removing, circumventing, or altering the configuration of security agents (EDR, DLP, MDM). The management, updating, and monitoring of malware protection follow POL-SIP-022 (Malware Protection Policy).

5.4 ACCOUNT AUTHORIZATION AND RESPONSIBILITIES

The account is personal, individual, and non-transferable: sharing username, password, tokens, verification codes, or MFA devices with any person — including managers, colleagues, third parties, or vendors — is prohibited. The user is responsible for all actions performed with their account until formal reporting of a suspected compromise, must use MFA on systems that require it, and must approve push requests only when they themselves initiate the access.

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

5.5 CLEAN DESK AND CLEAR SCREEN

Users must keep their desk free of sensitive information when away from it 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-SIP-010 (Clean Desk and Clear Screen Policy).

5.6 INTERNET USE

Use of the corporate internet is permitted exclusively for professional purposes. Accessing sites with illegal, pornographic, discriminatory, violent, or gambling content, or content that encourages inappropriate or illegal conduct, is prohibited. Downloading software, executables, or any content without prior authorization from the IT department is prohibited. Using proxy, non-corporate VPN, or any other method to circumvent the Organization's access restrictions is prohibited.

Using the 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 is prohibited. External communication applications (e.g., non-approved external communication applications) must follow the Organization's guidelines and may not be used for transferring 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

Use of the corporate email and other PX.Center digital channels (instant messaging, corporate chats, collaboration platforms, and videoconferencing) 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 to handle 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 complies with LGPD and the Information Classification Policy. Automatic forwarding of corporate emails to personal or third-party accounts and opening attachments or links from suspicious senders are prohibited. Suspicious messages (phishing, malware, social engineering) must be reported immediately to security@px.center.

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

5.8 COPYRIGHT AND INTELLECTUAL PROPERTY

Reproduction, copying, modification, distribution, or use of materials, software, documents, and content without proper formal authorization is prohibited. All material developed in the scope of corporate activities — including source code, technical documentation, presentations, and databases — constitutes intellectual property of PX.Center, unless otherwise stipulated by contract.

Only software licensed and authorized by the IT department may be installed and used on corporate equipment; the use of pirated software, unauthorized versions, or applications that infringe 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, and is prohibited in any context that damages the Organization's reputation.

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-SIP-008 (Mobile Device and Remote Work Policy); the use of personal devices follows POL-SIP-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 equipment and devices is authorized exclusively to business functions responsible for that activity — particularly Marketing and Sales — using corporate accounts and for institutional promotion and communication purposes. Such use is subject to content restrictions: publishing or sharing confidential, restricted, or personal data is prohibited. For all other functions, 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 management.

5.11 MONITORING, INCIDENTS, AND CONSEQUENCES

All activities carried out on PX.Center systems, networks, and communication channels may be recorded, monitored, and audited on a continuous and proportionate basis, in compliance with LGPD. Users are prohibited from attempting to disable, circumvent, or interfere with monitoring mechanisms. Every user is informed, at the time of hiring or upon adherence to this policy, of the existence and purpose of monitoring.

Every security incident — such as unauthorized access, data leakage, system unavailability, malware infection, loss or theft of devices, 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 are additionally reported to dpo@px.center, in accordance with POL-SIP-029. Failure to report in a timely manner constitutes a violation of this policy.

The user acknowledges and agrees to access monitoring and auditing at the time of onboarding and at each relevant update of this standard.

6. RESPONSIBILITIES

The CISO and CTO approve this policy, define security requirements, provide the necessary resources, and oversee acceptable use compliance 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 oversees records 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 the assets under their responsibility.

Area managers approve access and remote work for their teams, confirm asset return upon offboarding, and support the application of monitoring measures. The Data Protection Officer (DPO) handles incidents involving personal data through the dpo@px.center channel, in accordance with POL-SIP-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 PX.Center's Records Control Policy. Records include access logs, use authorization evidence, incident reports, semi-annual access reviews, and training evidence, and are stored in electronic files (PDF, DOCX, XLSX), in corporate systems, or in physical copies where applicable. Control is performed through the Records Management Spreadsheet, with the following mandatory fields:

record type, creation date, responsible party, retention period, storage location, and status. The record owner ensures its creation, updating, and maintenance; the Information Security team oversees compliance; and the IT department ensures the protection, backup, and availability of electronic records. Records are retained for the minimum period defined in the Records Control Policy, or for a longer period when required by law, contract, or regulation, and their disposal occurs through complete and irrecoverable deletion of the information.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy comes into effect on 23/06/2026 on the SGI Portal, with indefinite validity, and is reviewed annually or whenever there are changes to legal and regulatory requirements, relevant security incidents, technology updates, or process changes. Non-compliance with this policy subjects the offender to applicable disciplinary measures — such as warning, suspension, blocking or revocation of access, and contract termination — in accordance with the severity of the infraction, applicable labor law, and the applicable contract, without prejudice to civil and criminal liability under applicable legislation.

9. ANNEXES

No annexes. Operational records reside in the systems indicated in the Records Management section.

CHANGE HISTORY

Version	Date	Author	Change Description
00	09/06/2025	IT and Cybersecurity Department - IS	Creation and Review
01	24/06/2026	SGI	Recoding to acronym