Clean Desk and Clean Screen Policy

Protection of information at workstations, screens, and physical areas of PX.Center

Code:	*POL-SIP-010*
Responsible area:	*Information Security*
Issue date:	*24/06/2026*
Approval authority:	*CISO / CTO*

1. PURPOSE/OBJECTIVE

This policy establishes PX.Center's clean desk and clean screen guidelines, in accordance with control 7.7 (Clear desk and clear screen) of ISO/IEC 27001:2022, with the purpose of protecting sensitive information and information assets against unauthorized access, disclosure, loss, or damage resulting from exposure at workstations, screens, printers, boards, media, and other physical areas.

This document defines users' obligations regarding the storage of physical documents, screen locking, use of shared equipment, and reporting of violations, integrating the physical controls of the Information Security Management System (ISMS) established by POL-SIP-001.

2. SCOPE/APPLICABILITY

This policy applies to all physical workspaces, workstations, devices, and media that allow access, processing, display, or storage of PX.Center corporate information, in all units, meeting rooms, common areas, and remote work environments. PX.Center's designation as the reference entity encompasses the other CNPJs within the group, dispensing with the need for a specific document per entity.

These guidelines apply in conjunction with POL-SIP-001 (Information Security Policy) and with the information classification policy, which determines the level of protection required for each type of document or data.

3. USERS/TARGET AUDIENCE

All employees, interns, third parties, service providers, and any persons who have access to PX.Center facilities or information assets and who use physical workspaces or corporate devices.

4. REFERENCE DOCUMENTS

- ISO/IEC 27001:2022 (control 7.7, Clear desk and clear screen)
- Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD)
- POL-SIP-001: Information Security Policy
- POL-SIP-013: Acceptable Use Policy
- POL-SGI-001: Information Lifecycle Policy
- POL-SIP-002: Incident Management Policy

5. GUIDELINES / RULES / CONTROLS

5.1 GENERAL PRINCIPLE

The user is responsible for protecting information under their custody against improper exposure. Documents, screens, media, and printed materials containing information classified as internal, confidential, or restricted, as defined by the information classification policy, must remain protected from viewing or access by unauthorized persons. Workplace protection is the joint responsibility of Information Security, area leaders, and the user themselves.

5.2 CLEAN DESK

When leaving the workspace, even for brief periods, and at the end of each working day, the user must keep their desk free of confidential and sensitive documents. The following are mandatory:

- Store confidential and sensitive documents in locked drawers or cabinets with keys, so they are not visible when stepping away
- Do not leave contracts, spreadsheets, notes, post-its, badges, or devices containing organizational data exposed on the desk
- Collect personal items that may contain company data
- Keep the desk clear at the end of the working day, free of loose papers, unprotected electronic devices, or open documents
- Dispose of sensitive documents using a shredder; discarding them in general waste bins is prohibited.

5.3 CLEAN SCREEN

When stepping away from a computer or device, the user must prevent unauthorized access to the active session. The following are mandatory:

- Immediately lock the screen when stepping away (Windows+L or Ctrl+Alt+Del followed by Lock, or equivalent on the device in use)
- Never leave the system open or the session active and unattended
- Maintain automatic screen lock after a period of inactivity, set to 5 to 10 minutes, with password-protected resumption
- Do not write passwords in visible locations or leave them accessible at the workstation
- Log out of critical system sessions after use.

5.4 PRINTERS AND PRINTED DOCUMENTS

The user must immediately retrieve documents sent for printing from the printer, and must not leave printed materials unattended in the output tray. It is prohibited to abandon printed documents in shared printers, copiers, or scanning devices. Documents printed in error or that are no longer needed must be destroyed using a shredder.

5.5 WHITEBOARDS, FLIPCHARTS, AND MEETING ROOMS

At the end of meetings, the user must erase all sensitive or confidential information from whiteboards and flipcharts and collect any notes, printed materials, and media left in the room. Meeting rooms must be checked before leaving to ensure no corporate information remains exposed.

5.6 PHYSICAL DOCUMENTS AND MEDIA

Physical documents and media containing confidential or restricted information must be stored in locked drawers or cabinets when not in use. Removable storage devices, such as USB drives, external hard drives, and backup media, must be kept in a secure, protected location with access restricted on a need-to-know basis; leaving them exposed on desks or in circulation areas is prohibited.

5.7 SHARED EQUIPMENT AND WORKSTATIONS

Shared equipment, such as printers, self-service terminals, shared computers, and meeting rooms, must be used with attention to information protection. It is the user's responsibility to verify, upon finishing use, that no information has been left on the device, whether in printed documents, open files, or active sessions. Saving confidential data on public or shared devices is prohibited, and any information viewed on such devices must be removed immediately after use.

5.8 VIOLATION REPORTING

Any violation of this policy, improper exposure of information, or suspected unauthorized access must be reported immediately to Information Security via security@px.center. Incidents involving information compromise are handled in accordance with POL-SIP-002 (Incident Management Policy).

6. RESPONSIBILITIES

Information Technology (IT), through Information Security, is the area responsible for ensuring compliance with this policy, maintains the security@px.center channel for reporting violations, and is accountable for investigating breaches of its provisions. Management approves this policy and provides the resources necessary for its implementation, including lockable furniture, shredders, and automatic screen lock configuration.

Area leaders ensure the adoption of clean desk and clean screen practices by their teams and monitor compliance with the guidelines in their work environments. Users are responsible for protecting information under their custody, observe clean desk and clean screen obligations, check shared equipment after use, and report violations via security@px.center.

7. RECORDS MANAGEMENT

Records associated with this policy are maintained in the following repositories: - Versions of this policy and evidence of dissemination: SGI document repository. - Incidents and violations reported via security@px.center: handled in accordance with POL-SIP-002 and recorded in the corporate records tool. - Evidence of clean desk and clean screen awareness: in accordance with the ISMS training cycle. The integrity of records must be preserved, with access restricted on a need-to-know basis, and they must remain available for internal and external SGI audits.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy takes effect on 23/06/2026, with an indefinite validity period. Information Security reviews this document annually or in response to significant changes in legal or regulatory requirements, incidents related to non-compliance with this policy, or structural changes in the Organization that affect physical security controls. Non-compliance with this policy subjects the offender to the disciplinary measures set forth in PX.Center's internal regulations.

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