Clean Desk and Clear Screen Policy

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

Code	POL-SEG-010
Responsible Area	Information Security
Issue Date	June 24, 2026
Approval Authority	CISO / CTO

1. PURPOSE / OBJECTIVE

This policy establishes PX.Center's clean desk and clear 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, whiteboards, media, and other physical areas.

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

2. SCOPE / APPLICABILITY

This policy applies to all physical workspaces, workstations, devices, and media that allow access to, processing, display, or storage of PX.Center's corporate information, across all facilities, meeting rooms, common areas, and remote working environments. PX.Center's designation as the reference entity covers the other CNPJs (Brazilian tax registration numbers) of the group, making a separate document per entity unnecessary.

The guidelines apply in conjunction with POL-SEG-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's 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)
- Law No. 13,709/2018 (Brazilian General Data Protection Law — LGPD)
- POL-SEG-001: Information Security Policy
- POL-SEG-013: Acceptable Use Policy
- POL-SGI-001: Information Lifecycle Policy
- POL-SEG-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 printouts containing information classified as internal, confidential, or restricted — in accordance with the information classification policy — must remain protected from

viewing or access by unauthorized persons. Workplace protection is a shared responsibility of Information Security, the leadership of each department, and the user themselves.

5.2 Clean Desk

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

- Store confidential and sensitive documents in locked drawers or cabinets so they are not visible when stepping away.
- Do not leave contracts, spreadsheets, notes, sticky notes, ID badges, or devices containing organizational data exposed on the desk.
- Collect personal items that may contain company data.
- Keep the desk clean at the end of the working day, with no loose papers, unprotected electronic devices, or open documents.
- Dispose of sensitive documents using a shredder; disposal in regular waste bins is prohibited.

5.3 Clear Screen

When leaving a computer or device, users must prevent unauthorized access to the active session. The following are mandatory:

- Lock the screen immediately when stepping away (Windows+L or Ctrl+Alt+Del followed by Lock, or the equivalent on the device being used).
- Never leave the system open or the session active without supervision.
- Maintain automatic screen lock after a period of inactivity, set to between 5 and 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

Users must immediately retrieve documents sent to the printer from the output tray and must not leave printouts unattended. It is prohibited to abandon printed documents at shared printers, copiers, or scanning devices. Documents printed in error or discarded must be shredded.

5.5 Whiteboards, Flipcharts, and Meeting Rooms

At the end of meetings, users must erase all sensitive or confidential information from whiteboards and flipcharts and collect 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 kiosks, shared computers, and meeting rooms — must be used with attention to information protection. It is each user's responsibility to verify, upon completion of use, that no information has remained 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 there must be removed immediately after use.

5.8 Reporting Violations

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

6. RESPONSIBILITIES

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

The leadership of each department ensures adoption of clean desk and clear screen practices by their teams and monitors compliance with these guidelines within their work environments. Users are responsible for protecting information under their custody, observing clean desk and clear screen obligations, verifying shared equipment after use, and reporting violations via **security@px.center**.

7. RECORDS MANAGEMENT

Records associated with this policy reside in the following repositories:

- Versions of this policy and disclosure evidence: the ISMS document repository.
- Incidents and violations reported via security@px.center: handled in accordance with POL-SEG-002 and recorded in the corporate records management tool.
- Clean desk and clear screen awareness evidence: in accordance with the ISMS training cycle.

The integrity of records must be preserved, with access restricted on a need-to-know basis, and records must be kept available for internal and external ISMS audits.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy takes effect on June 23, 2026, with indefinite validity. Information Security reviews this document annually or upon any significant change 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

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

CHANGE HISTORY

Version	Date	Author	Description of Changes
00	June 9, 2025	IT and Cybersecurity Department — IS	Creation and Review
01	June 24, 2026	ISMS (SGI)	Recoded to acronym-based identifier