Mobile Device and Remote Work Policy

Secure use of mobile devices and remote access at PX.Center

Code	POL-SEG-008
Responsible Area	Information Security
Issue Date	June 24, 2026
Approval Authority	CISO / CTO

1. PURPOSE / OBJECTIVE

This policy establishes the mandatory guidelines for the secure use of mobile devices and remote work practices at PX.Center, in compliance with control 6.7 of ISO/IEC 27001:2022 (remote work), controls 7.9 (security of off-premises assets) and 8.1 (user endpoint devices), and in integration with POL-SEG-001 (Information Security Policy).

This document defines the protection rules applicable to notebooks, smartphones, tablets, and other assets that access the Organization's information outside its physical premises, in order to preserve the confidentiality, integrity, and availability of information even in remote environments and connections outside the corporate perimeter.

2. SCOPE / APPLICABILITY

This policy applies to all employees, service providers, and third parties who access PX.Center's information assets outside the Organization's physical premises, on any authorized corporate or personal device. PX.Center's designation as the reference entity covers the other CNPJs (tax registration numbers) of the group, eliminating the need for a specific document per entity.

The policy covers mobile computing devices such as notebooks, smartphones, tablets, corporate USB media, and IoT devices with external connectivity, as well as all remote access to systems, cloud services, and internal data of the Organization. The use of personal devices (BYOD) is governed by the specific rules of POL-SEG-012. The provisions apply jointly with POL-SEG-001 (Information Security Policy), to which this policy is subordinate.

3. TARGET USERS / AUDIENCE

Senior Management, CISO, CTO, Information Security Lead, IT Infrastructure team, department managers, and all employees, service providers, and third parties authorized to use mobile devices or to remotely access PX.Center's information assets.

4. REFERENCE DOCUMENTS

- ISO/IEC 27001:2022 (controls 6.7, 7.9, and 8.1)
- POL-SEG-001: Information Security Policy
- POL-SEG-012: BYOD Policy (use of personal devices)
- POL-SEG-002: Incident Management Policy
- POL-SEG-016: Access Control Policy
- POL-SGI-001: Information Lifecycle Policy
- POL-SEG-013: Acceptable Use Policy

5. GUIDELINES / RULES / CONTROLS

5.1 Mobile Device Provisioning and Management

Mobile computing devices are considered to include notebooks, smartphones, tablets, corporate USB media, IoT devices with external connectivity, and any other asset capable of accessing PX.Center's systems or information outside the Organization's premises. The provision of corporate devices is the responsibility of the Information Technology area, subject to the approval of the employee's direct manager.

The inventory, management, and monitoring of provided devices are conducted by the IT Infrastructure team via the corporate endpoint management solution (UEM), and endpoint protection is ensured by the corporate Endpoint Detection and Response (EDR) solution. Accessing the Organization's information on a device not inventoried by IT is prohibited.

5.2 Secure Device Configuration

Every corporate mobile device must maintain active and up-to-date endpoint protection (EDR), enabled disk encryption, strong authentication, and automatic screen lock. Automatic screen lock is mandatory and must activate after no more than 5 minutes of inactivity, with unlock protected by password, PIN, or biometrics. Operating systems and applications must be kept up to date in accordance with IT's patch management policy. The installation of software not authorized or not previously assessed by IT is prohibited.

5.3 Use in Transit and Protection of Off-Premises Assets

In accordance with control 7.9 of ISO/IEC 27001:2022, the removal and transport of corporate devices requires authorization and registration in the IT inventory. Equipment must be kept in a physically secure location, must not be left unattended in public places, and must not be used by third parties. Employees must prevent information from being viewed by unauthorized persons in public environments, and sharing the device with unauthorized individuals is prohibited.

Off-premises maintenance of the device is authorized and controlled by IT, and the return of the asset is recorded with the corresponding entry removal from the inventory.

5.4 Remote Access and Remote Work

In accordance with control 6.7 of ISO/IEC 27001:2022, remote access to PX.Center's internal systems must occur exclusively through secure channels, with mandatory use of corporate VPN combined with multi-factor authentication (MFA). Accessing internal systems via direct connections that do not route through the corporate VPN is prohibited. Authorization for remote work is the responsibility of the employee's direct manager, and the technical enablement of access is managed by the IT team.

Employees must ensure a private and secure physical environment with adequate connectivity, and the use of third-party devices to access the Organization's data is prohibited.

5.5 Data Protection and Storage

Sensitive or confidential data must not be stored locally on the device without encryption and without approval from the responsible area. Storing the Organization's documents on unauthorized devices or

non-corporate external media is prohibited. Upon replacement or disposal of the device, the equipment must be returned to IT for secure formatting and removal from the inventory.

5.6 Reporting Loss, Theft, or Incident

The loss or theft of a mobile device must be immediately reported to security@px.center. Information Security will activate the remote lock or wipe of the device through the corporate endpoint management and EDR solutions. Incidents involving mobile devices or remote access are handled in accordance with the procedures defined in POL-SEG-002; when personal data is involved, dpo@px.center is also notified for assessment of LGPD obligations.

5.7 Use of Personal Devices (BYOD)

The use of personal devices to access PX.Center's information assets is governed by the specific rules of POL-SEG-012. In the absence of authorization and enrollment under the controls of that standard, accessing the Organization's systems and data through personal devices is prohibited.

6. RESPONSIBILITIES

Information Technology (IT) is the area responsible for ensuring compliance with this policy and is accountable for investigating violations of its provisions. The security contact is security@px.center for information security matters and dpo@px.center for privacy and LGPD matters. **Senior Management** approves this policy and provides the resources necessary for its execution. The **CISO and CTO** approve this policy, define the controls applicable to mobile devices and remote access, and are responsible for its maintenance.

The **IT Infrastructure team** provisions corporate devices, maintains the inventory, management, and monitoring through the corporate endpoint management solution (UEM), and enables remote access via VPN with MFA. The **Information Security Lead** receives reports of loss, theft, and incidents, activates remote lock or wipe, and manages incident response in accordance with POL-SEG-002.

Department managers authorize remote work for their teams, validate the need for device provision, and ensure the compliance of employees under their management with this policy. **Employees, service providers, and third parties** comply with the rules of this policy, physically protect the devices under their care, and immediately report any loss, theft, or incident.

7. RECORDS MANAGEMENT

Records maintained in accordance with this document reside in the following repositories:

- Inventory of corporate mobile devices, with history of provision, revocation, maintenance, and disposal: corporate endpoint management solution (UEM).
- Registry of authorized remote accesses: under the custody of the IT Infrastructure team.
- Endpoint protection events and remote lock/wipe actions: corporate EDR and endpoint management solution.
- Incidents involving mobile devices or remote access: in accordance with POL-SEG-002.
- Versions of this policy: ISMS document repository.

It is mandatory to preserve the integrity of records, with access restricted on a need-to-know basis, and to keep them available for internal and external ISMS audits.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on June 23, 2026, and remains valid indefinitely. The document is reviewed annually or in the event of a relevant incident involving mobile devices or remote work, a regulatory or compliance change, or the adoption of a new technology that impacts the controls defined herein. Non-compliance with this policy subjects the offender to the disciplinary measures provided for in PX.Center's internal regulations.

9. ANNEXES

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

REVISION HISTORY

Version	Date	Author	Description
00	June 23, 2025	IT and Cybersecurity Department — IS	Creation and Review
01	June 24, 2026	ISMS	Recodification to acronym-based code