Physical Protection of Premises Policy

PxP Shape sp. z o.o.

1. **Purpose**

The purpose of this procedure is to establish guidelines and controls to protect the physical premises where services are performed, ensuring the safety of personnel, safeguarding company assets, and maintaining the confidentiality, integrity, and availability of information, both on-site and remotely.

2. **Scope**

This procedure applies to all employees, contractors, visitors, and any other individuals accessing company premises. It covers all physical locations where services are performed, including offices, and remote work environments.

3. Physical Security Controls for Office Locations

A. Access Control

- Office Badge: All employees, contractors, and visitors must wear office-issued identification badges at all times while on premises.
- Access Levels: Access to different areas of the premises shall be restricted based on necessity. Higher security areas require additional authorization.
- Visitor Management: Visitors must check-in at the reception, be escorted by authorized personnel, and wear visitor badges at all times.
- Audit: All accesses to the premises are registered and logged accordingly.

B. Physical Barriers

- Perimeter Security: Locked doors are installed around the premises to prevent unauthorized entry.
- Secure Doors: Entry points are equipped with badge-based electronic access control systems.

4. Physical Security Controls for Remote Work

A. Secure Workspace

- Designated Workspace: Employees and contractors should establish a secure, designated workspace at home to perform their duties. The designated workspace should be used exclusively for work-related activities, where feasible.
- Physical Access: Ensure that unauthorized individuals do not have physical access to company-issued devices and confidential information. Employees must ensure that unauthorized household members or visitors do not have access to confidential company information or devices.

B. Device Security

- Device Locking: All devices must be locked when not in use. Use strong passwords and enable automatic locking features, according to Device and Password Policy adopted by the Company,
- Encryption: Ensure that all company-issued devices and sensitive data are encrypted.
- For more detailed information please check the Device and Password Policy.

C. Data Handling

- Document Security: Store physical documents securely and dispose of them properly using shredders when no longer needed.

5. **Training and Awareness**
    - Employee Training: Conduct regular training sessions for employees.
6. **List of covered locations:**
    - Kamienna 21, 31-403 Kraków
7. **Document Control**

Document Details

Document Type	Policy
Owner	Bruno Pimenta
Approvers	See below
Date First Published	02/08/2024
Date of Next Planned Review	31/12/2025

Version History

Version	**Date**	**Description of Change**	**Edited By**	**Reviewed and Approved? (Y/N) / Approver**
1.0	02/08/2024	Document created	Bruno Pimenta	Yes / Arthur Pfister
1.1	19/03/2025	Document updated	Bruno Pimenta	Yes / Arthur Pfister
1.2	24/06/2025	Document updated	Bruno Pimenta	Yes / Maria Pfister