Device and Password Policy

PxP Shape sp. z o.o.

1. Purpose

The purpose of this policy is to define the responsibilities and requirements that Organization's Employees and Contractors are subject to in relation to using, processing, storing, transferring internal and confidential information on personal or corporate devices.

2. Definitions

For the purposes of this document, the terms defined in **Personal Data Protection Policy** document are used.

3. Scope

This policy applies to all Employees and Contractors of the Organization regardless of their position, role or location which are using any kind of personal or corporate device (mobile phone, laptop, tablet, etc.) during their contractual relationship with the Organization.

4. Policy Statement

4.1. Device Management

All Employees and Contractors of Organization are under the obligation to perform the agreed activities using devices for the corporate duties with the following considerations:

- Devices (laptops, mobile phones, tablets, etc.) shall be used **solely** by the Employee/Contractor.
- Devices shall not be left unattended at any moment and secured appropriately.
- Whenever possible, Organization information shall be logically segregated on the device from the rest of existing information.
- Laptops are required to have antivirus software installed, updated and active at all times.
- All devices must lock themselves with password, PIN or Face recognition if it's idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden for performing Organization's agreed activities.
- The Employee/Contractor must ensure that no illegal software is used.
- Each Employee/Contractor using a laptop computer must be familiar with this Policy and obliges to comply with it,
- Personal data should be stored on an encrypted disk mutually in accordance with the rules described in this Policy,
- in case of theft or loss of a portable computer, the User shall immediately notify Data Protection Officer (e-mail: dataprotection@pxpshape.com) at the Organization, providing information about the type of data processed on the carrier and the circumstances of loss/theft of the carrier,
- The Employee/Contractor shall secure the portable computer during transportation, in particular by: (i) not leaving the portable computer in the car

while parked in a public place unattended; (ii) and avoid leaving it in the vehicle unattended, even when hidden.

- All user-level and system-level passwords must conform to the following:
    - Contain at least 8 alphanumeric characters, up to a maximum of 256.
    - Contain 3 out of 4 of the following conditions: contain both upper- and lower-case letters, contain at least one number (for example, 0-9), contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).
    - Cannot contain the username.
    - When available, multi-factor Authentication (MFA) shall be enabled for all critical systems.
    - Passwords shall expire every 40 days.
    - If there is any indicator that the password has been compromised, change must be done immediately.
    - In case of home routers, printers and other devices connected to the network, we strongly recommend changing default admin user/passwords and to keep them updated at all times.
    - The use of a password management program like LastPass, Keeper, Password Safe or Apple Passwords to store passwords in a central encrypted database secured by a master password (which is subject to the same guidelines described in this Policy) is required.

4.2. Risk and Incident Management

Lost, stolen, or compromised (i.e. malware, virus or similar attacks) devices must be reported to Organization within 12 hours to security@pxpshape.com. Employees and/or Contractors are responsible for notifying their mobile carrier immediately upon the loss of a device. The Employee and/or Contractor is expected to always use the devices in an ethical manner and adhere to the standards presented on this document.

Upon Contract Termination, the Employee or Contractor shall return to the Organization all corporate devices and, if any, information stored on personal devices should be wiped.

5. Encryption/Security Media:

a) Data processed on portable computers should be encrypted using encryption software (bitlocker/veracrypt/FileVault),

b) Encryption of mobile computer drives is carried out before the computer is issued to the User for use,

c) Passwords for encrypted drives are stored in a suitable application for secure storage and editing

d) Cell phones (smartphones, tablets) should be secured with an authentication mechanism,

6. Policy Compliance

6.1. Compliance Measurement

Executive Management ensure, that each member of the Staff shall be acquainted with this Policy prior starting to cooperate with the Organization, on whatever basis.

Organization shall verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, monitoring, business tool reports, internal and external audits, and feedback.

6.2. Exceptions

Any exception to the policy must be approved by the Executive Management in advance.

6.3. Non-Compliance

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7. Document Control

Document Details

Document Type	Policy
Owner	Bruno Pimenta
Approvers	See below
Date First Published	02/01/2023
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	02/01/2023	Document created	Bruno Pimenta	Yes / Arthur Pfister
1.1	22/06/2023	Password rules updated	Bruno Pimenta	Yes / Arthur Pfister
1.2	09/07/2024	Password rules updated	Bruno Pimenta	Yes / Arthur Pfister
1.3	13/02/2025	Password rules updated	Bruno Pimenta	Yes / Arthur Pfister
1.4	24/06/2025	Password rules updated	Bruno Pimenta	Yes / Maria Pfister