| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insert Registered Legal Entity Name Here | | | | | | | |
| Document number:<br>P34S | | | | | Document Title:<br>**Mobile Device and BYOD Policy** | | | | | | | |
| Version:<br>1.0 | | Effective Date:<br>01.01.2025 | | | Document Owner: | | | | | | | |
| X | Policy | | Standard | | Procedure | | Form | | Register | | Other | |

| **Revision history** | | | | |
|---|---|---|---|---|
| **Revision number** | **Revision Date** | **Changes** | **Reviewed by** | **Process owner** |
| | | | | |
| | | | | |

| **Approvals** | | | |
|---|---|---|---|
| **Name** | **Title** | **Date** | **Signature** |
| | | | |
| | | | |

Aligned with standards and regulations

| Standard/Regulation | Clause/Article | Comment |
|---|---|---|
| ISO/IEC 27001:2022 | Clauses 5.1, 5.2, 6.1, 6.2, 8 | General ISMS and mobile/BYOD control requirements |
| ISO/IEC 27002:2022 | Controls 5.10–5.13 | Detailed controls for mobile/BYOD and remote access |
| NIST SP 800-53 Rev.5 | AC-19, AC-20, CM-6, MP-7 | Federal device, media, and configuration controls |
| EU GDPR | Article 5(1)(f) | Personal data and mobile endpoint protection |
| EU NIS2 | Article 21(2)(d) | Protection of business-critical devices (including BYOD) |
| EU DORA | Articles 9, 10 | ICT risk and continuity requirements for mobile endpoints |
| COBIT 2019 | APO13, DSS01, DSS05 | IT governance, operations, and security service controls |

## 1. Purpose

1.1. This policy defines the mandatory security requirements for the use of mobile devices, including smartphones, tablets, and laptops, when accessing company information, systems, or services.

1.2. It also governs Bring Your Own Device (BYOD) use to ensure that customer and business data is protected, regardless of device ownership.

1.3. This policy enforces consistent protections for mobile access, supports ISO/IEC 27001 certification objectives, and prevents data loss or compromise arising from lost, stolen, or misused mobile endpoints.

1.4. It ensures that both technical controls and procedural safeguards are applied to mobile use in SMEs without dedicated IT teams, including remote work environments and cloud-based services.

## 2. Scope

**2.1. This policy applies to all employees, contractors, interns, and service providers who:**

2.1.1. Use a mobile device to access, process, or store company data or systems

2.1.2. Connect to company services, including email, shared folders, cloud applications, or internal systems, via the corporate VPN

**2.2. It covers:**

2.2.1. All mobile devices: smartphones, tablets, and laptops (company-issued devices and personal BYOD devices)

2.2.2. All operating systems (e.g., iOS, Android, Windows, macOS)

2.2.3. All locations (office, home, remote locations, and public spaces)

2.3. This policy applies across all work environments and must be enforced regardless of device ownership.

## 3. Objectives

3.1. Prevent Data Loss: Ensure that mobile device use does not expose sensitive company or customer data to unauthorized access, theft, or misuse.

3.2. Define Clear Rules for BYOD: Establish enforceable conditions for the use of personal devices for business purposes, including legal and technical safeguards.

3.3. Support Regulatory Compliance: Meet requirements under ISO/IEC 27001, GDPR, NIS2, and other legal obligations through enforceable mobile security practices.

3.4. Minimize Operational Risk: Reduce the likelihood of operational disruption caused by misuse, compromise, or failure of mobile devices.

3.5. Maintain Customer Trust: Demonstrate to customers and partners that their data remains protected even when accessed on mobile or personal devices.

## 4. Roles and Responsibilities

### 4.1. General Manager (GM):

4.1.1. Retains accountability for this policy.

4.1.2. Approves all mobile and BYOD access to company systems.

4.1.3. Ensures that BYOD agreements are signed, retained, and monitored.

4.1.4. Verifies that the external IT service provider enforces the required mobile security controls.

### 4.2. Designated Staff or IT Support:

4.2.1. Assists with the setup, registration, and configuration of mobile devices used for work.

4.2.2. Enforces mobile access controls, application restrictions, and monitoring requirements.

4.2.3. Supports incident reporting and incident management for mobile device incidents (lost, stolen, or compromised devices).

[ ... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ... ]

## 9. Review and Update Requirements

### 9.1. Annual Review

9.1.1. The General Manager (GM) must review this policy at least once every 12 months.

9.1.2. The review must verify continued alignment with ISO/IEC 27001 requirements, evolving mobile technologies, and changes in business operations.

9.1.3. Updates must also take into account recent incidents, audit results, and regulatory developments (e.g., GDPR, NIS2, DORA).

### 9.2. Trigger Events for Interim Reviews

#### 9.2.1. This policy must be updated immediately if any of the following occur:

9.2.1.1. A major mobile security incident (e.g., a breach involving a lost or compromised device)

9.2.1.2. A change in supported platforms or mobile device management tools

9.2.1.3. A legal or regulatory change affecting personal device use or data protection

9.2.1.4. Introduction of new applications, services, or third-party tools used on mobile devices

### 9.3. Documentation of Changes

9.3.1. All reviews and updates must be documented, including the review date, changes made, and the GM's approval

9.3.2. A version control history must be retained for audit purposes

### 9.4. Communication and Access

9.4.1. The GM must ensure that all users (employees, contractors, and third parties) are informed of changes

9.4.2. Updated versions must be made readily accessible, such as through shared folders or internal platforms

## 10. Related Policies and Linkages

**10.1. This policy forms part of the overall SME Information Security Policy suite and must be implemented alongside the following:**

10.1.1. P4S – Access Control Policy: Defines requirements for managing secure access to systems, including systems accessed via mobile devices. Enforces password hygiene and session control.

10.1.2. P8S – Information Security Awareness and Training Policy: Ensures that users receive training on the secure use of mobile devices, incident reporting, and BYOD conditions.

10.1.3. P17S – Data Protection and Privacy Policy: Establishes GDPR-compliant handling of personal and company data on mobile platforms, particularly where personal devices are used for work.

10.1.4. P9S – Remote Work Policy: Aligns with requirements for mobile device use when working off-site or from home, including device handling and network access control safeguards.

10.1.5. P30S – Incident Response Policy: Provides the response framework for mobile-related incidents, including compromised or lost devices.

10.2. These related policies operate together as a complete set of controls for mobile device security in SMEs without dedicated IT staff, ensuring enforceability, transparency, and audit readiness.

## 11. Reference Standards and Frameworks

11.1. This policy supports full alignment with the following security and compliance standards:

**11.2. ISO/IEC 27001:**

11.2.1. Clause 5.1 – Leadership and Commitment: Ensures management oversight and accountability for mobile and BYOD access

11.2.2. Clause 6.1 – Actions to Address Risks and Opportunities: Requires mobile security risks to be assessed and treated

11.2.3. Clause 8.1 – Operational Planning and Control: Requires consistent mobile access procedures to protect business data

**11.3. ISO/IEC 27002:**

11.3.1. Controls 5.10 (Use of Mobile Devices), 5.11 (Teleworking), 5.12 (Remote Access), and 5.13 (BYOD): Provide implementation guidance for managing device risks in an SME context

**11.4. NIST SP 800-53 Rev.5:**

11.4.1. AC-19 – Access Control for Mobile Devices: Requires security settings for authorized mobile device use

11.4.2. AC-20 – Use of External Systems: Governs BYOD and remote access risks

11.4.3. CM-6 – Configuration Settings: Enforces secure default and customized settings on mobile platforms

11.4.4. MP-7 – Media Use: Addresses appropriate use and restrictions for mobile storage and data access

**11.5. EU GDPR (2016/679):**

11.5.1. Article 5(1)(f) – Integrity and Confidentiality: Requires protection of personal data through appropriate security, particularly on mobile platforms

11.5.2. Article 32 – Security of Processing: Requires appropriate technical and organisational measures (TOMs) to secure data accessed or stored on mobile devices

**11.6. EU NIS2 Directive (2022/2555):**

11.6.1. Article 21(2)(d) – Device Security Measures: Requires security controls for hardware and software used to access critical business systems, including personal devices

**11.7. EU DORA (2022/2554):**

11.7.1. Article 9 – ICT Risk Management Framework: Requires protection of mobile endpoints used for critical business communications and cloud services

11.7.2. Article 10 – ICT Business Continuity: Requires continued secure access to business systems during disruption or remote working

**11.8. COBIT 2019:**

11.8.1. APO13 – Manage Security: Requires the organisation to enforce mobile and BYOD policies aligned with enterprise risk

11.8.2. DSS01 – Manage Operations: Ensures technical implementation of secure access mechanisms

11.8.3. DSS05 – Manage Security Services: Governs third-party involvement in maintaining secure mobile environments and coordinating incident response