					[Insert Registered Legal Entity Name Here]								
Document number: P34S					Document Title: **Mobile Device and BYOD Policy**								
Version: 1.0		Effective Date: 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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 5.1, 5.2, 6.1, 6.2, 8.1	
ISO/IEC 27002:2022	Controls 5.10–5.13	
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	
EU GDPR	Articles 5(1)(f)	
EU NIS2	Article 21(2)(d)	
EU DORA	Articles 9, 10	
COBIT 2019	APO13, DSS01, DSS05	

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

1. **Purpose**
   1.1. This policy defines the mandatory security requirements for using mobile devices—including smartphones, tablets, and laptops—when accessing company information, systems, or services.
   1.2. It also regulates Bring Your Own Device (BYOD) usage to ensure customer and business data is protected, regardless of who owns the device.
   1.3. The policy enforces consistent protections for mobile access, helps meet ISO/IEC 27001 certification goals, and prevents data loss or compromise from lost, stolen, or misused mobile endpoints.
   1.4. It ensures that both technical 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 apps, or internal systems via VPN
   2.2. It covers:
      2.2.1. All mobile devices: smartphones, tablets, laptops (company-issued or personal BYOD)
      2.2.2. All operating systems (e.g., iOS, Android, Windows, macOS)
      2.2.3. All locations (office, home, remote, public spaces)
   2.3. The policy applies across all work environments and must be enforced regardless of ownership of the device.
3. **Objectives**
   3.1. **Prevent Data Loss:** Ensure that mobile use does not expose sensitive company or customer data to unauthorized access, theft, or misuse.
   3.2. **Define Clear Rules for BYOD:** Provide enforceable conditions for using personal devices for business purposes, ensuring 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 chance of operational disruption caused by mobile device misuse, compromise, or failure.
   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. Maintains accountability for this policy.
      4.1.2. Approves all use of mobile and BYOD access to company systems.
      4.1.3. Ensures BYOD agreements are signed, stored, and monitored.
      4.1.4. Verifies external IT service providers enforce required mobile protections.
   4.2. **Designated Staff or IT Support:**
      4.2.1. Assists with setup, registration, and configuration of mobile devices used for work.

4.2.2. Enforces mobile-related access controls, app restrictions, and monitoring policies.

4.2.3. Supports mobile device incident response (lost, stolen, compromised devices).

4.3. **All Users (Employees, Contractors):**

4.3.1. Must follow all rules in this policy when using mobile or BYOD devices for work.

[…….]

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 those accessed via mobile devices. Enforces password hygiene and session controls.

10.1.2. **P8S – Information Security Awareness and Training Policy**: Ensures users are trained on secure mobile device use, 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, especially when personal devices are used for work.

10.1.4. **P9S – Remote Work Policy**: Aligns with mobile use expectations when working offsite or from home, including device handling and network access 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 work together to form a complete set of controls for mobile device security in SMEs without dedicated IT staff, ensuring enforceability, transparency, and certification-readiness.

11. Reference Standards and Frameworks

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

ISO/IEC 27001:2022

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

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

Clause 8.1 – Operational Planning and Control: Demands consistent mobile access procedures to safeguard business data

ISO/IEC 27002:2022

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 a small business context

NIST SP 800-53 Rev.5

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

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

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

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

EU GDPR (2016/679)

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

Article 32 – Security of Processing: Obligates use of appropriate technical and organizational measures for securing data accessed or stored on mobile devices

EU NIS2 Directive (2022/2555)

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

EU DORA (2022/2554)

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

Article 10 – ICT Business Continuity: Enforces continued secure access to business systems even during disruptions or remote work

COBIT 2019

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

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

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