					[Insert Registered Legal Entity Name Here]							
Document number: **P34**					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 5.10, 5.11, 5.12, 5.13	
ISO/IEC 27002:2022	Controls 5.10–5.13	
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	
EU GDPR	Articles 5(1)(f), 25, 32	
EU NIS2	Article 21(2)(d)	
EU DORA	Articles 9, 10	
COBIT 2019	APO13.02, DSS01.04, BAI09.0	

1. **Purpose**
   1.1. This policy establishes the security, compliance, and operational requirements for the use of mobile devices and personal technology (BYOD – Bring Your Own Device) when accessing organizational systems, applications, or data.
   1.2. It aims to ensure the confidentiality, integrity, and availability of company information accessed or processed via mobile endpoints, including smartphones, tablets, laptops, and hybrid devices.
   1.3. It also enforces the technical and procedural controls required to mitigate risks such as data leakage, unauthorized access, device loss or theft, and compromise of mobile applications.
   1.4. This policy supports regulatory and contractual compliance while enabling secure mobile productivity for employees, contractors, and authorized third parties.
2. **Scope**
   2.1. This policy applies to all personnel—including employees, contractors, interns, and third-party service providers—who use mobile devices to access company data, systems, applications, or communication platforms.
   2.2. It covers all mobile computing devices, including but not limited to:
      2.2.1. Smartphones and tablets (iOS, Android, etc.)
      2.2.2. Laptops and ultrabooks (Windows, macOS, Linux)
      2.2.3. Wearables and hybrid smart devices capable of data synchronization
   2.3. It applies regardless of whether the device is company-owned or personally owned under a BYOD agreement.
   2.4. The policy encompasses all access vectors including VPNs, virtual desktops, cloud apps, email, collaboration platforms (e.g., SharePoint, Teams), and file synchronization tools (e.g., OneDrive, Dropbox if authorized).
   2.5. It includes use in remote work, on-premises, travel, or hybrid work arrangements.
3. **Objectives**
   3.1. To reduce the risk of data compromise, leakage, or loss due to insecure mobile device usage.
   3.2. To enforce consistent and enforceable security controls across all mobile endpoints, regardless of ownership model (corporate or BYOD).
   3.3. To ensure mobile device usage complies with ISO/IEC 27001 and other regulatory frameworks applicable to data privacy, protection, and cybersecurity.
   3.4. To facilitate secure integration of mobile devices into the organization’s operational, communication, and collaboration workflows.
   3.5. To provide clearly defined responsibilities and processes for mobile device management (MDM), including enrollment, remote wipe, encryption, authentication, and monitoring.
   3.6. To protect the privacy rights of individuals using their own devices while safeguarding the organization’s sensitive information.
4. **Roles and Responsibilities**
   4.1. **Chief Information Security Officer (CISO) / IT Security Lead**
      4.1.1. Defines policy and technical standards for mobile and BYOD usage.

4.1.2. Oversees compliance, incident response, and exception management for mobile device controls.

4.1.3. Coordinates with legal and HR teams to ensure enforcement is legally sound and organizationally aligned.

4.2. **Information Technology (IT) Administrator / MDM Administrator**

4.2.1. Manages mobile device provisioning, enrollment, and configuration through MDM solutions.

[…….]

11. Reference Standards and Frameworks

This policy is aligned with internationally recognized cybersecurity frameworks and legal obligations to ensure the secure use of mobile devices and personal (BYOD) technologies in enterprise environments.

ISO/IEC 27001:2022

Clause 5.10 – Acceptable Use of Information and Assets: Requires controls for responsible use of corporate assets, including mobile devices.

Clause 5.11 – Remote Working: Governs secure practices when accessing systems from outside company premises.

Clause 5.12 – Use of Mobile Devices: Mandates risk-based controls for mobile endpoints and BYOD configurations.

Clause 5.13 – Information Transfer: Enforces the protection of information transferred via mobile channels.

ISO/IEC 27002:2022 – Controls 5.10 to 5.13

Annex A Controls 5.10 to 5.13: Specify how mobile access, encryption, monitoring, and loss mitigation must be enforced within an ISMS. These controls provide detailed implementation guidance for securing mobile endpoints, enforcing containerization, monitoring device integrity, and ensuring privacy-aware configurations for BYOD use.

NIST SP 800-53 Rev.5

AC-19 – Access Control for Mobile Devices: Defines baseline protections, including encryption, authentication, and MDM enforcement.

AC-17 – Remote Access: Requires secure authentication and session protections for remote mobile users.

CM-7 – Least Functionality: Supports removal of unnecessary apps and features from mobile endpoints to reduce risk.

MP-5 – Media Transport Protection: Governs the secure transmission of data from mobile systems to external or cloud destinations.

SC-12 – Cryptographic Key Establishment: Mandates use of secure cryptographic protocols for mobile communication and storage.

EU GDPR (2016/679)

Article 5(1)(f) – Integrity and Confidentiality: Requires organizations to protect personal data on mobile devices against unauthorized or unlawful access.

Article 25 – Data Protection by Design and by Default: Requires privacy to be embedded into BYOD and MDM processes.

Article 32 – Security of Processing: Enforces risk-based controls (e.g., encryption, authentication, access control) for personal data on mobile platforms.

EU NIS2 Directive (2022/2555)

Article 21(2)(d): Mandates that mobile access to critical systems and information be protected through appropriate technical and organizational measures, such as endpoint control, encryption, and monitoring.

EU DORA (2022/2554)

Article 9 – ICT Risk Management Framework: Requires financial sector entities to mitigate mobile and remote access risks as part of operational resilience.

Article 10 – ICT Systems Security Requirements: Demands secure mobile architecture, monitoring, and response mechanisms for mobile-originated cyber threats.

COBIT 2019

APO13.02 – Establish and Maintain an Information Security Plan: Requires mobile device use, including BYOD, to be integrated into organizational security strategies.

DSS01.04 – Manage Asset Configuration and Integrity: Applies to configuration control and secure deployment of mobile devices.

BAI09.01 – Establish and Maintain Controls: Supports implementation of technical and procedural safeguards for secure mobile and remote operations.