					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Applies security controls and compliance requirements
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Provides detailed controls for mobile device management
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Access control, remote access, configuration, and security requirements for mobile devices
EU GDPR	5(1)(f), 25, 32	Mandatory privacy, data encryption, and processing security requirements
EU NIS2	21(2)(d)	Technical and organizational protection measures for mobile access
EU DORA	9, 10	ICT risk management and security requirements for mobile devices
COBIT 2019	APO13.02, DSS01.04, BAI09	Information security plans, asset configuration, and controls for mobile environments

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 is intended to ensure the Confidentiality, Integrity, and Availability of company information accessed or processed through mobile endpoint devices, including smartphones, tablets, laptops, and hybrid devices.

1.3 It also mandates 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 Bring Your Own Device (BYOD) arrangement.

2.4 The policy encompasses all access methods, including remote access tools and VPNs, virtual desktop infrastructure (VDI), cloud applications, email, collaboration platforms (e.g., SharePoint, Teams), and file synchronization tools (e.g., OneDrive, Dropbox where authorized).

2.5 It includes use in remote working, on-premises, travel, or hybrid work arrangements.

3. Objectives

3.1 To reduce the risk of data compromise, leakage, or loss resulting from insecure use of mobile devices.

3.2 To enforce consistent and auditable security controls across all mobile endpoint devices, regardless of ownership model (corporate or Bring Your Own Device (BYOD)).

3.3 To ensure that mobile device usage complies with ISO/IEC 27001 and other regulatory frameworks applicable to data privacy, data protection and minimization, and cybersecurity.

3.4 To enable the secure integration of mobile devices into the organization's operational, communication, and collaboration workflows.

3.5 To establish clearly defined responsibilities and processes for mobile device management (MDM), including device onboarding, remote wipe, encryption, authentication, and monitoring and threat detection.

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 the policy and technical standards for mobile and Bring Your Own Device (BYOD) usage.

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

4.1.3 Coordinates with Legal and Compliance and Human Resources (HR) to ensure enforcement is legally sound and aligned with organizational requirements.

4.2 IT Administrators / Mobile Device Management (MDM) Administrator

4.2.1 Manage user provisioning, enrollment, and configuration of mobile devices through mobile device management (MDM) solutions.

4.2.2 Enforce device-level controls (e.g., encryption, PINs, and application controls).

4.2.3 Perform remote wipe, lockout, and revocation of access where required.

[... 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 This policy shall be reviewed at least annually by the CISO or designated ISMS Manager to ensure alignment with:

9.1.1 Changes in mobile OS platforms, mobile device management (MDM) technologies, or authentication standards

9.1.2 Regulatory or contractual changes affecting mobile data protection (e.g., GDPR, DORA, NIS2)

9.1.3 Revisions to ISO/IEC 27001:2022, ISO/IEC 27002:2022, or NIST SP 800-53 Rev.5 control sets

9.1.4 Feedback from audits, incident post-mortems, or employee reports

9.2 Interim reviews may be triggered by:

9.2.1 Security incidents involving mobile devices or Bring Your Own Device (BYOD) platforms

9.2.2 Vendor notification of high-risk vulnerabilities in supported platforms

9.2.3 Introduction of new mobile applications or collaboration platforms used for business operations

9.3 Policy updates shall be:

9.3.1 Documented in the policy version history

9.3.2 Communicated to All Personnel and affected contractors

9.3.3 Reconfirmed through updated acknowledgement by all Bring Your Own Device (BYOD) users

9.4 All reviews and revisions must be formally approved by Top Management and recorded in the Policy Change Register.

10. Related Policies and Linkages

10.1 This policy is interdependent with several key policies within the organization's Information Security Management System (ISMS). Key linkages include:

10.1.1 P1 – Information Security Policy: Establishes the overarching governance principles for all information security controls, including those governing mobile device usage.

10.1.2 P3 – Acceptable Use Policy: Defines permitted behaviors and restrictions related to technology usage, which apply directly to mobile and Bring Your Own Device (BYOD) access.

10.1.3 P9 – Remote Work Policy: Addresses additional security obligations for mobile working environments, complementing the mobile-specific controls defined in this policy.

10.1.4 P13 – Data Classification and Labeling Policy: Governs how data on mobile devices must be handled based on classification level, affecting storage, transfer, and enforcement of encryption.

10.1.5 P22 – Logging and Monitoring Policy: Supports the collection and review of mobile access logs to detect anomalies or violations.

10.1.6 P30 – Incident Response Policy: Governs how mobile-related incidents (e.g., device loss, unauthorized access) are handled and escalated.

10.1.7 P33 – Audit and Compliance Monitoring Policy: Provides the basis for periodic checks of mobile security compliance, including adherence to the Bring Your Own Device (BYOD) policy.

11. Reference Standards and Frameworks

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

11.2 ISO/IEC 27001:

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

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

11.2.3 Clause 5.12 – Use of Mobile Devices: Requires risk-based controls for mobile endpoint devices and Bring Your Own Device (BYOD) configurations.

11.2.4 Clause 5.13 – Information Transfer: Requires protection of information transferred through mobile channels.

11.3 ISO/IEC 27002:2022 – Controls 5.10 to 5.13:

11.3.1 Annex A Controls 5.10 to 5.13: Specify how mobile access, encryption, monitoring, and loss mitigation must be enforced within an Information Security Management System (ISMS). These controls provide detailed implementation guidance for securing mobile endpoint devices, enforcing

containerization, monitoring device integrity, and ensuring privacy-aware configurations for Bring Your Own Device (BYOD) use.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Access Control for Mobile Devices: Defines baseline protections, including encryption, authentication, and mobile device management (MDM) enforcement.

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

11.4.3 CM-7 – Least Functionality: Supports removal of unnecessary applications and features from mobile endpoint devices to reduce risk.

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

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

11.5 EU GDPR (2016/679):

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

11.5.2 Article 25 – Data Protection by Design and by Default: Requires privacy by design and privacy by default to be embedded into Bring Your Own Device (BYOD) and mobile device management (MDM) processes.

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

11.6 EU NIS2 Directive (2022/2555):

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

11.7 EU DORA (2022/2554):

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

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

11.8 COBIT 2019:

11.8.1 APO13.02 – Establish and Maintain an Information Security Plan: Requires mobile device use, including Bring Your Own Device (BYOD), to be integrated into organizational security strategies.

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

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