					[Insert Registered Legal Entity Name Here]						
Document number: P9					Document Title: **Remote Work 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	Clause 6.1.3, 8.1	
ISO/IEC 27002:2022	Control 6.7	
NIST SP 800-53 Rev.5	AC-17, AC-2, SC-12, SC-13	
EU GDPR	Articles 32, 5(1)(f); Recital 39	
EU NIS2	Articles 21(2)(a, b, d), 21(3)	
EU DORA	Articles 5, 8, 9	
COBIT 2019	DSS01, BAI06, BAI09, APO13, MEA03	

		[Insert Registered Legal Entity Name Here]
Document number: P9		Document Title: **Remote Work 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 requirements for securely conducting remote work, including the use of organizational systems, access to data, and execution of job duties outside of corporate premises.

1.2 It ensures the confidentiality, integrity, and availability of information assets accessed remotely and establishes controls to mitigate risks associated with distributed work environments.

1.3 The policy fulfills ISO/IEC 27001:2022 Annex A Control 6.7 by implementing technical and procedural safeguards tailored to remote working conditions.

2. **Scope**

2.1 This policy applies to all personnel authorized to work remotely, including:

2.1.1 Employees (full-time, part-time, contract)

2.1.2 External service providers, consultants, and vendors

2.1.3 Temporary and project-based staff with approved remote access

2.2 It covers:

2.2.1 Access to organizational systems via VPN or approved remote tools

2.2.2 Handling of sensitive and regulated information outside secure facilities

2.2.3 Use of organization-owned or Bring Your Own Device (BYOD) equipment

2.2.4 Physical and logical protections in remote environments

2.3 The policy applies across all geographies and time zones where the organization permits remote work, whether regular, ad-hoc, or during business continuity events.

3. **Objectives**

3.1 To ensure that only authorized individuals can remotely access internal systems and information.

3.2 To enforce encryption, multi-factor authentication (MFA), and endpoint protections across all remote access paths.

3.3 To maintain a secure posture against threats such as phishing, malware, data exfiltration, and unauthorized system exposure.

3.4 To govern how sensitive data is transmitted, stored, or printed in off-site environments.

3.5 To embed physical security measures that reduce visibility and unauthorized observation during remote sessions.

3.6 To comply with international regulatory requirements regarding remote data access, including GDPR, NIS2, and DORA.

4. **Roles and Responsibilities**

4.1 **Executive Management**

4.1.1 Approves this policy and ensures it is resourced and integrated into HR, IT, and security operations.

4.1.2 Authorizes organizational remote work eligibility criteria and business unit applicability.

4.2 **CISO / ISMS Manager**

[…..]

11. Reference Standards and Frameworks

This policy aligns with internationally recognized security, data protection, and ICT risk management frameworks to ensure secure, traceable, and compliant remote work practices.

ISO/IEC 27001:2022

Clause 6.1.3 – Risk Treatment Planning: This policy contributes to the treatment of risks associated with remote access and distributed work environments.

Clause 8.1 – Operational Planning and Control: Requires implementation of controls for systems accessed outside organizational premises.

Annex A Control 6.7 – Remote Working: This policy fully addresses required controls for information security while personnel work outside organizational premises, including physical and logical protections, access governance, and user behavior monitoring.

ISO/IEC 27002:2022 – Control 6.7

This control mandates procedural and technical safeguards for remote working. It includes requirements for device security, access methods, data handling, environmental safeguards, and the management of third-party participants—all of which are enforced through this policy.

NIST SP 800-53 Rev.5

AC-17 (Remote Access): Directly supported via VPN controls, MFA, session logging, and role-based access authorization for remote users.

AC-2 (Account Management): Controls access eligibility, remote privilege assignment, and account deactivation.

SC-12 to SC-13 (Cryptographic Protection, Cryptographic Key Establishment): Implemented through mandatory use of VPNs and full-disk encryption for remote endpoints.

MP-5 (Media Transport Protection) and **PE-18 (Location of Information System Components)**: Remote work guidance mandates transport protection and physical safeguards in off-site environments.

AU-2, AU-6: Logging and monitoring of remote sessions support audit and incident response requirements.

EU GDPR (2016/679)

Article 32 – Security of Processing: This policy enforces remote access security, encryption, and logging controls necessary to secure personal data accessed or processed remotely.

Article 5(1)(f): Ensures that personal data accessed off-site is protected against unauthorized or unlawful processing and accidental loss.

Recital 39: Emphasizes access limitation, integrity, and confidentiality—especially relevant when devices leave secure premises.

EU NIS2 Directive (2022/2555)

Article 21(2)(a, b, d): Requires that remote access be secured as part of an organization's ICT risk management framework. This policy fulfills the requirement for security measures that cover access control, data security, and organizational policies for remote environments.

Article 21(3): Encourages security awareness and policy enforcement among staff working outside central premises.

EU DORA (2022/2554)

Article 5 – Governance and Internal Control Framework: This policy supports ICT risk control expectations for all operational scenarios, including hybrid and remote models.

Article 8 – ICT Risk Management Framework: Remote access risks are identified, mitigated, and governed via technical and organizational controls enforced here.

Article 9 – Information Sharing Arrangements: Protects against remote leakage of information shared within digital operational resilience networks.

COBIT 2019

DSS01 – Managed Operations: This policy supports secure continuity of business operations regardless of physical location.

BAI06 – Managed IT Changes and **BAI09 – Managed Assets**: Ensure that remote work devices are tracked, configured securely, and handled as critical assets.

APO13 – Managed Security: Promotes a defined security governance framework for remote environments.

MEA03 – Monitor, Evaluate, and Assess Compliance: Establishes that remote work activity must be logged, reviewed, and audited.