					Insert Registered Legal Entity Name Here							
Document number: P09					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**

1. Purpose

1.1 This policy defines the mandatory requirements for securely conducting remote work activities, including the use of organizational systems, access to data, and the performance of job responsibilities outside 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 This 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 workers and project-based personnel with approved remote access

2.2 It covers:

2.2.1 Access to organizational systems via VPN or approved remote access 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 controls in remote environments

2.3 This policy applies across all geographies and time zones where the organization permits remote work, whether on a regular basis, on an ad hoc basis, 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 protection (AV/EDR) 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 implement physical controls 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 Top Management

4.1.1 Approves this policy and ensures it is adequately resourced and integrated into Human Resources (HR), IT, and security operations.

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

4.2 CISO / ISMS Manager

4.2.1 Owns and maintains this policy and ensures alignment with the organization’s risk posture and regulatory requirements.

4.2.2 Defines security controls for remote access (e.g., encryption, endpoint protection (AV/EDR), session timeouts).

4.2.3 Approves exception handling and monitors control effectiveness.

[... 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 Review Frequency

9.1.1 This policy must be reviewed annually, or more frequently upon:

9.1.1.1 Introduction of new remote access technologies

9.1.1.2 Significant expansion of remote work arrangements (e.g., hybrid workforce initiatives)

9.1.1.3 Emergence of new threats, vulnerabilities, or incidents linked to remote environments

9.1.1.4 Changes to relevant legal or regulatory frameworks

9.2 Ownership and Review Process

9.2.1 The policy owner is the CISO. Review must be coordinated with:

9.2.1.1 IT Operations and Architecture

9.2.1.2 Human Resources (HR) and Facilities and Asset Management (for operational and workspace implications)

9.2.1.3 Data Protection Officer (DPO) (for data privacy and cross-border data controls)

9.2.2 Policy updates must be:

9.2.2.1 Approved by the ISMS Steering Committee

9.2.2.2 Communicated to all affected staff and contractors

9.2.2.3 Integrated into onboarding and annual refresher training materials

9.3 Document Control and Distribution

9.3.1 This policy shall include version control, effective date, and a change log.

9.3.2 Superseded versions must be retained in accordance with the Document Management Policy (P14).

9.3.3 Revised versions must trigger mandatory acknowledgment by users eligible for remote work.

10. Related Policies and Linkages

10.1 This policy operates in conjunction with:

10.1.1 P1 – Information Security Policy: Establishes the baseline for secure handling of assets, applicable to all work environments including remote work.

10.1.2 P3 – Acceptable Use Policy: Governs appropriate use of organizational devices and systems during remote work sessions.

10.1.3 P4 – Access Control Policy: Ensures that remote access privileges follow least privilege and appropriate authentication mechanisms.

10.1.4 P6 – Risk Management Policy: Defines how remote work risks are identified, treated, and monitored within the Information Security Management System (ISMS).

10.1.5 P12 – Asset Management Policy: Requires inventory and configuration management for all devices used remotely.

10.1.6 P22 – Logging and Monitoring Policy: Ensures that remote sessions are monitored, audited, and retained in accordance with compliance requirements.

10.1.7 P14 – Data Retention and Disposal Policy: Defines data handling rules relevant to remote work, including removable media and device disposal.

10.2 Collectively, these policies ensure that remote work remains secure, compliant, and enforceable across all functions and geographies.

11. Reference Standards and Frameworks

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

11.2 ISO/IEC 27001

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

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

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

11.3 ISO/IEC 27002:2022 – Control 6

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

11.4 NIST SP 800-53 Rev.5

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

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

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

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

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

11.5 EU GDPR (2016/679)

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

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

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

11.6 EU NIS2 Directive (2022/2555)

11.6.1 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 covering access control, data security, and organizational policies for remote environments.

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

11.7 EU DORA (2022/2554)

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

11.7.2 Article 8 – ICT Risk Management Framework: Remote access risks are identified, mitigated, and governed through technical and organizational controls enforced by this policy.

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

11.8 COBIT 2019

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

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

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

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