					Insert Registered Legal Entity Name Here							
Document number: P09S					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 6.1, 6.2, 8	
ISO/IEC 27002:2022	Control 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
EU NIS2	Articles 21(2)(b), 21(2)(h)	EU NIS2
EU DORA	Article 9	EU DORA
COBIT 2019	DSS05, APO13	COBIT 2019
EU GDPR	Article 32	EU GDPR

1. Purpose

1.1 This policy defines the security requirements for Employees and Contractors who work remotely, including from home, shared workspaces, or while travelling.

1.2 It is intended to protect the Confidentiality, Integrity, and Availability of business information accessed outside company-controlled environments.

1.3 This policy supports compliance with applicable international standards and reduces risks such as unauthorized access, data loss, and service disruption.

2. Scope

2.1 This policy applies to all personnel (employees, contractors, consultants, and temporary workers) who access company systems, networks, or data while working off-site.

2.2 It covers:

2.2.1 The use of company-issued and personally owned devices

2.2.2 Access via VPN, remote desktop, or cloud services

2.2.3 The secure handling of information outside company premises

2.2.4 Monitoring, exception handling, and compliance enforcement

2.3 It applies to both full-time and part-time remote work arrangements, including ad hoc remote access for training purposes.

3. Objectives

3.1 Prevent unauthorized access to company systems or sensitive data during remote work.

3.2 Ensure that devices and communication links used outside the office meet baseline security requirements.

3.3 Maintain control over remote access privileges and monitoring.

3.4 Provide clear guidance to employees and managers on secure remote working practices.

3.5 Comply with ISO, NIS2, GDPR, DORA, and COBIT expectations for remote and mobile work.

4. Roles and Responsibilities

4.1 General Manager

4.1.1 Approves remote work arrangements and monitors compliance.

4.1.2 Escalates security incidents or repeated non-compliance.

4.1.3 Reviews exceptions and ensures follow-up on incidents.

4.2 IT Support or External IT Provider

4.2.1 Establishes secure remote access (e.g. VPN, Multi-Factor Authentication (MFA)).

4.2.2 Enforces endpoint security, encryption, and device configuration requirements.

4.2.3 Supports users and investigates technical security issues.

[... 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 Annual Policy Review

9.1.1 The General Manager and IT Support must review this policy annually to ensure alignment with changes in technology, workforce arrangements, and legal requirements.

9.2 Triggers for Early Update

9.2.1 An immediate review is required following:

9.2.1.1 A major remote work security incident

9.2.1.2 Changes to NIS2, GDPR, or DORA requirements

9.2.1.3 Transition to new remote access technology (e.g. a different VPN platform)

9.3 Version Control and Archiving

9.3.1 All versions of this policy must be:

9.3.1.1 Dated and approved by the General Manager

9.3.1.2 Assigned a version number

9.3.1.3 Archived for at least three years

9.4 Staff Communication

9.4.1 Policy updates must be communicated to all remote users. Acknowledgement is required for any significant change.

10. Related Policies and Linkages

10.1 This policy links to and supports the following:

10.1.1 P2S – Governance Roles and Responsibilities Policy: Defines who authorizes and oversees remote access

10.1.2 P4S – Access Control Policy: Establishes secure remote access configuration and revocation procedures

10.1.3 P6S – Risk Management Policy: Tracks and evaluates risks related to off-site access

10.1.4 P8S – Information Security Awareness and Training Policy: Trains users on remote work risks and good practice

10.1.5 P30S – Incident Response Policy: Governs the response to remote access incidents such as credential compromise or device loss

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 6.1 – Risk-based planning for remote access scenarios

11.1.2 Clause 6.2 – Addresses Human Resources (HR) responsibilities in mobile and remote working contexts

11.1.3 Clause 8.1 – Operational planning and control for remote processes

11.2 ISO/IEC 27002

11.2.1 Control 6.7 – Provides practical guidance on security for remote and mobile work

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Remote access control, session protection, and security monitoring

11.3.2 AC-2 – Account management for off-site users

11.4 EU GDPR

11.4.1 Article 32 – Requires data protection “by design and by default,” including in remote settings

11.5 EU NIS2 Directive

11.5.1 Article 21(2)(b) – Requires secure use of network and information systems

11.5.2 Article 21(2)(h) – Requires HR-related security measures, including off-site controls

11.6 EU DORA

11.6.1 Article 9 – Requires financial entities to maintain ICT resilience across all operating modes, including remote access

11.7 COBIT 2019

11.7.1 DSS05 – Manage Security Services: Includes endpoint protection and secure remote work practices

11.7.2 APO13 – Managed Security: Ensures secure provisioning and risk oversight for mobile and remote access