				[Insert Registered Legal Entity Name Here]							
Document number: P9S				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, 6.2, 8.1	
ISO/IEC 27002:2022	Control 6.7	
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 establishes security requirements for employees and contractors working remotely, including from home, shared workspaces, or while traveling.

1.2. It aims to protect the confidentiality, integrity, and availability of business information accessed outside company-controlled environments.

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

2. Scope

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

2.2. It covers:

2.2.1. Use of company-issued and personally owned devices

2.2.2. Access via VPN, remote desktop, or cloud services

2.2.3. Secure handling of information outside company premises

2.2.4. Monitoring, exception handling, and enforcement

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

3. Objectives

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

3.2. Ensure 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 for 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 incident follow-up.

4.2. **IT Support or External IT Provider**

4.2.1. Sets up secure remote access (e.g., VPN, MFA).

4.2.2. Enforces endpoint security, encryption, and device configurations.

4.2.3. Supports users and investigates any technical security issues.

4.3. **Office Manager / HR**

4.3.1. Maintains a record of approved remote workers.

4.3.2. Ensures employees acknowledge this policy upon approval for remote work.

4.4. **Remote Workers (Employees, Contractors)**

4.4.1. Must use only authorized devices and secure connections.

4.4.2. Must report lost devices, suspicious activity, or policy violations immediately.

4.4.3. Are responsible for physical and digital security while working off-site.

5. Governance Requirements

5.1. **Remote Access Approval**
- 5.1.1. Remote access must be formally approved by the General Manager.
- 5.1.2. A register of approved remote workers must be maintained, including name, role, device type, and approval date.

5.2. **Use of Secure Connections**
- 5.2.1. Remote users must access company systems through encrypted connections (e.g., VPN).
- 5.2.2. Where supported, multi-factor authentication (MFA) must be enabled.
- 5.2.3. Public Wi-Fi may only be used if a secure tunnel (VPN) is active.

5.3. **Device Controls and Configuration**
- 5.3.1. Devices must be:
  - 5.3.1.1. Password-protected or secured with biometrics

[…….]

ISO/IEC 27001:2022

Clause 6.1 – Risk-based planning for remote access scenarios

Clause 6.2 – Addresses HR responsibilities in mobile/remote contexts

Clause 8.1 – Operational planning and control of remote processes

ISO/IEC 27002:2022

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

NIST SP 800-53 Rev.5

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

AC-2 – Account control for off-site users

EU GDPR

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

EU NIS2 Directive

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

Article 21(2)(h) – Calls for HR-related security measures including off-site controls

EU DORA

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

COBIT 2019

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

APO13 – Managed Security: Ensures secure provisioning and risk oversight of mobile/remote access