					Insert Registered Legal Entity Name Here							
Document number: P21S					Document Title: **Network Security 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 8	-
ISO/IEC 27002:2022	Control 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
EU GDPR	Article 32	-
EU NIS2	Articles 21(2)(d), (e)	-
EU DORA	Articles 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Purpose

1.1. The purpose of this policy is to ensure that all internal and external network communications are protected against unauthorized access, tampering, interception, or misuse through clearly defined security controls.

1.2. It establishes requirements for the secure design, use, and management of network infrastructure, including routers, wireless access points, remote access connections, and segmented networks.

1.3. It is intended to minimize exposure to internet-based threats, ensure the confidentiality of data transmitted across internal and external networks, and maintain the availability of critical services.

1.4. This policy supports ISO/IEC 27001:2022 certification and directly contributes to compliance with legal and regulatory obligations under GDPR, NIS2, and DORA, while providing technical assurance to customers and auditors.

2. Scope

2.1. This policy applies to all components of the organization's IT network, including:

2.1.1. Wired and wireless infrastructure at office locations

2.1.2. Routers, switches, access points, firewalls, and gateways

2.1.3. Remote access connections, including VPNs, RDP, and cloud tunnels

2.1.4. Cloud-based applications accessed from internal or external networks

2.1.5. Devices connected to the network by employees, contractors, or guests

2.2. This policy governs both physical and logical network segments, including guest zones, IoT devices, and back-office systems.

2.3. This policy applies to all personnel with access to the organization's network, including:

2.3.1. Internal employees

2.3.2. Remote workers and hybrid staff

2.3.3. External vendors, consultants, and service providers

2.3.4. Guests using temporary Wi-Fi access

3. Objectives

3.1. Ensure the organization's network is protected against unauthorized access and external cyber threats

3.2. Enforce appropriate segmentation between trusted and untrusted networks (e.g., guest Wi-Fi, vendor access)

3.3. Enable secure remote connectivity without compromising internal systems

3.4. Prevent malware propagation and data exfiltration through network channels

3.5. Provide monitoring, alerting, and auditability of network activity to support incident detection and compliance

3.6. Ensure that only approved and secured devices are permitted to connect to internal networks

3.7. Fulfil obligations under ISO 27001, GDPR, and related cybersecurity frameworks

4. Roles and Responsibilities

4.1. General Manager (GM)

4.1.1. Owns this policy and ensures that appropriate resources are allocated for secure network design and management

4.1.2. Reviews exceptions to network security controls and approves vendor network access agreements

4.1.3. Reviews incidents or audit findings relating to network security weaknesses

4.2. IT Support Provider / Internal IT Function

4.2.1. Implements, configures, and maintains all firewalls, routers, switches, and wireless controllers

4.2.2. Manages segmentation between internal, guest, and external networks

4.2.3. Monitors logs and alerts for unauthorized access attempts or network anomalies

4.2.4. Ensures firmware and configuration updates are applied securely and in a timely manner

[... 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 Review

9.1.1. This policy must be reviewed at least annually by the General Manager together with the IT Support Provider and Privacy Coordinator.

9.2. Triggers for Interim Review

9.2.1. Policy review must also be triggered by:

9.2.1.1. Major changes to network architecture (e.g., new VPN or firewall systems)

9.2.1.2. A network-related incident (e.g., intrusion, ransomware propagation, or data exfiltration)

9.2.1.3. Legal, regulatory, or framework updates affecting network protection

9.2.1.4. New vendor platforms requiring alternative access methods or protocols

9.3. Version Management and Documentation

9.3.1. Policy revisions must be recorded with a version number, date, and summary of changes

9.3.2. Previous versions must be archived for no less than 3 years

9.3.3. Updates must be communicated to affected employees, and acknowledgment must be obtained where significant behavioural changes are introduced

10. Related Policies and Linkages

10.1. This policy must be implemented alongside the following SME security policies:

10.1.1. P9S – Remote Work Policy: Establishes secure remote access methods, VPN requirements, and endpoint protection for off-site users.

10.1.2. P12S – Asset Management Policy: Ensures that all network-connected systems are identified, categorized, and tracked with up-to-date security status.

10.1.3. P17S – Data Protection and Privacy Policy: Ensures that network segmentation, access controls, and logging support privacy and data protection principles under GDPR.

10.1.4. P22S – Logging and Monitoring Policy: Defines requirements for collecting and reviewing logs from network devices, remote connections, and wireless controllers.

10.1.5. P30S – Incident Response Policy: Defines required actions in response to network breaches, unauthorized access attempts, or malware propagation through internal networks.

11. Reference Standards and Frameworks

11.1. ISO/IEC 27001

11.1.1. Clause 8.1 – Requires the implementation of controls to ensure secure and resilient operations, including networks.

11.2. ISO/IEC 27002

11.2.1. Control 8.20 – Provides technical and procedural guidance for securing network access, segmentation, and monitoring.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Requires control of information flow within networks and between systems.

11.3.2. SC-7 – Requires boundary protection, secure routing, and network segmentation to reduce the risk of unauthorized access.

11.4. EU GDPR

11.4.1. Article 32 – Requires appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of networked systems and services that process personal data.

11.5. EU NIS2 Directive

11.5.1. Article 21(2)(d) – Requires risk-based technical measures, including network security and access control.

11.5.2. Article 21(2)(e) – Requires system segmentation and isolation to prevent the propagation of cyber incidents.

11.6. EU DORA

11.6.1. Article 9 – Requires organizations to implement ICT risk management controls, including controls for secure networks and communications.

11.6.2. Article 10 – Requires digital resilience strategies to include protection of network infrastructure and remote connectivity.

11.7. COBIT 2019

11.7.1. DSS05.02 – Requires effective protection of IT infrastructure and network environments against internal and external threats.

11.7.2. APO13.01 – Requires risk management strategies that include network segmentation and monitoring as part of threat mitigation.