<table>
<tr><td colspan="5"></td><td colspan="7">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="5">Document number:
P21S</td><td colspan="7">Document Title:
<b>Network Security Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="3">Effective Date:
01.01.2025</td><td colspan="7">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

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 8.1	
ISO/IEC 27002:2022	Control 8.20	
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, APO13.01	

PREVIEW ONLY

					[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

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, eavesdropping, or misuse by clearly defined security controls.
    - 1.2. It establishes rules for secure design, usage, and management of network infrastructure including routers, wireless access points, remote access connections, and segmented networks.
    - 1.3. It aims to minimize exposure to internet-based threats, ensure the confidentiality of data transmitted over 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 meeting legal and regulatory obligations under GDPR, NIS2, and DORA, while offering 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. The policy covers 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 proper 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 auditing of network activity to support incident detection and compliance
    - 3.6. Ensure only approved and secured devices are allowed to connect to internal networks
    - 3.7. Fulfill 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 appropriate resources are assigned for secure network design and management

PREVIEW ONLY

4.1.2. Reviews exceptions to network security controls and approves vendor network access agreements
4.1.3. Reviews incidents or audit findings related to network security weaknesses

4.2. **IT Support Provider / Internal IT Role**

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 timely

4.3. **Privacy or Security Coordinator**

4.3.1. Verifies that network controls support compliance with personal data protection requirements
4.3.2.

[…….]

Reference Standards and Frameworks

ISO/IEC 27001:2022

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

ISO/IEC 27002:2022

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

NIST SP 800-53 Rev.5

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

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

EU GDPR

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

EU NIS2 Directive

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

Article 21(2)(e) – Requires system segmentation and isolation to prevent cyber incidents from propagating.

EU DORA

PREVIEW ONLY

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

Article 10 – Demands that digital resilience strategies encompass protection for network infrastructure and remote connectivity.

COBIT 2019

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

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

PREVIEW ONLY

This document is a licensed cybersecurity compliance policy provided by ClarySec LLC.

Unlicensed reproduction, resale, or redistribution is strictly prohibited.

For legal use, purchase and download only via https://clarysec.com