					[Insert Registered Legal Entity Name Here]							
Document number: P21					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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 8.1	
ISO/IEC 27002:2022	Controls 8.20-8.22	
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	
EU GDPR	Article 32	
EU NIS2	Article 21(2)(d)	
EU DORA	Article 9	
COBIT 2019	DSS01.03, DSS05.01, MEA03	

					[Insert Registered Legal Entity Name Here]								
Document number: P21					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 define the organization's requirements for protecting its internal and external networks from unauthorized access, service disruption, data interception, and misuse.
   1.2 It ensures that all networking infrastructure—including physical, virtual, cloud, and hybrid—is protected through layered controls such as segmentation, firewall enforcement, secure routing, and centralized monitoring.
   1.3 This policy enforces ISO/IEC 27001 Clause 8.1 and Annex A Controls 8.20 through 8.22, ensuring compliance with applicable legal and regulatory obligations under GDPR Article 32, NIS2 Article 21, and DORA Article 9.
2. **Scope**
   2.1 This policy applies to all networks and related infrastructure components, including:
      2.1.1 Routers, switches, wireless access points, and firewalls
      2.1.2 Cloud virtual networks (e.g., AWS VPC, Azure VNET), VPN concentrators, and SD-WAN systems
      2.1.3 Internal LANs, DMZs, remote access paths, and inter-site or third-party connections
      2.1.4 Supporting systems such as DNS, DHCP, proxy servers, and monitoring appliances
   2.2 The policy is binding for all personnel and third-party service providers who manage, configure, monitor, or interface with organizational networks, whether on-premises or in the cloud.
   2.3 All systems and applications connected to the organization's networks—regardless of location or ownership—must conform to these network security requirements.
3. **Objectives**
   3.1 Ensure the confidentiality, integrity, and availability of data transmitted across networks through strong access controls, secure routing, and monitoring.
   3.2 3Prevent unauthorized access, lateral movement, and exploitation of networked resources by enforcing segmentation, zoning, and boundary protection.
   3.3 Maintain consistent network configurations based on industry standards and threat intelligence to defend against evolving cyber threats.
   3.4 Secure external communications, cloud interconnectivity, and remote access using encrypted channels, strict authentication, and endpoint validation.
   3.5 Provide visibility into network activity through centralized logging, real-time traffic inspection, and automated alerting.
   3.6 Ensure regulatory compliance by aligning all network operations with ISO/IEC 27001:2022, GDPR, NIS2, DORA, and COBIT 2019 requirements.
4. **Roles and Responsibilities**
   4.1 **Chief Information Security Officer (CISO)**
      4.1.1 Owns this policy and ensures it is reviewed and aligned with the organization's broader cybersecurity strategy.
      4.1.2 Approves network segmentation models, firewall rulesets for sensitive systems, and exception requests.
   4.2 **Network Security Manager / Infrastructure Security Lead**

4.2.1 Manages network defense architecture including firewalls, intrusion detection/prevention systems (IDS/IPS), VPNs, and secure routing.

4.2.2 Oversees network segmentation, VLAN assignments, traffic zoning, and external connectivity.

[….]

11. Reference Standards and Frameworks

This policy aligns with international standards and regulatory mandates that define secure network operations, segmentation, perimeter protection, and secure remote access.

ISO/IEC 27001:2022

Clause 8.1 - Operational Planning and Control: Requires technical controls, including network safeguards, to be embedded in operational processes.

ISO/IEC 27002:2022 - Controls 8.20-8.22

Provides detailed implementation guidance on protecting networks, segmenting services, and securing network services through access controls and monitoring.

NIST SP 800-53 Rev.5

SC-7 - Boundary Protection: Requires perimeter controls, segmentation, and secure interconnections.

AC-4 - Information Flow Enforcement: Supports zoning and rule-based traffic restrictions.

SC-32 - Information System Partitioning: Promotes logical separation of information systems to prevent unauthorized interaction.

EU GDPR (2016/679)

Article 32 - Security of Processing: Requires technical measures—such as firewalls and segmentation—to safeguard personal data against unauthorized access or transmission.

EU NIS2 Directive (2022/2555)

Article 21(2)(d): Requires effective network and information systems security, including perimeter protection, secure configuration, and segregation controls.

EU DORA (2022/2554)

Article 9 - ICT Risk Management: Obligates financial entities to protect their networks and interconnections from unauthorized access, data leakage, and operational disruption.

COBIT 2019

DSS01.03 - Monitor Infrastructure: Requires proactive control over network health and connectivity.

DSS05.01 - Protect Against Malware: Includes segmentation and boundary control to minimize propagation.

MEA03 - Monitor, Evaluate and Assess Compliance: Reinforces network policy enforcement and compliance assessments.