					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	N/A
ISO/IEC 27002:2022	Controls 8.20-8.22	N/A
NIST SP 800-53 Rev. 5	SC-7, AC-4, SC-32	N/A
EU GDPR	Article 32	N/A
EU NIS2	Article 21(2)(d)	N/A
EU DORA	Article 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/A

1. Purpose

1.1 The purpose of this policy is to define the organization's requirements for protecting its internal and external networks against unauthorized access, service disruption, data interception, and misuse.

1.2 It ensures that all network infrastructure, including physical, virtual, cloud, and hybrid environments, is protected through layered controls such as network segmentation and isolation, firewall enforcement, secure routing, and centralized monitoring and threat detection.

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 (for example, AWS VPC and 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 This policy is binding on all personnel, contractors, 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 Prevent 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 best practices and threat intelligence to defend against the evolving threat landscape.

3.4 Secure external communications, cloud interconnectivity, and remote access using encrypted channels, strong 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 rule sets for sensitive systems, and exception requests.

4.2 Network Security Manager / Infrastructure Security Lead

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

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

4.2.3 Ensures continuous review of ingress/egress filtering and Zero Trust enforcement across network tiers.

[... 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 This policy shall be reviewed annually by the Network Security Manager in collaboration with the CISO and updated based on:

9.1.1 Emerging threats, such as new attack techniques and protocol vulnerabilities

9.1.2 Changes in infrastructure, such as cloud migrations and SD-WAN deployments

9.1.3 Regulatory or standards updates affecting network protections

9.1.4 Audit findings, incident trends, or control-related performance degradation

9.2 Reviews must also be triggered by:

9.2.1 Major changes to network architecture

9.2.2 Implementation of new firewall, VPN, or cloud network platforms

9.2.3 Decommissioning requirements affecting key assets or trusted zones

9.3 Updates must be logged in the ISMS Document Register and communicated to:

9.3.1 Infrastructure and network operations teams

9.3.2 SOC and security engineering teams

9.3.3 Application teams with system dependencies on network flows

9.3.4 All third-party vendors with active interconnectivity

9.4 All previous policy versions must be archived securely with change log annotations to preserve auditability and change traceability.

10. Related Policies and Linkages

10.1 P1 - Information Security Policy. Establishes foundational security principles and requires layered protections, including network-based access and threat controls.

10.2 P4 - Access Control Policy. Ensures that network segmentation is enforced in alignment with user roles, least privilege principles, and user provisioning rules.

10.3 P5 - Change Management Policy. Governs firewall modifications, VPN rule changes, and routing changes through a documented and auditable process.

10.4 P12 - Asset Management Policy. Supports the identification and classification of networked systems and ensures all connected assets are managed within policy-defined scopes.

10.5 P22 - Logging and Monitoring Policy. Governs the collection, correlation, and retention of network logs, including firewall events, access attempts, and anomaly detections.

10.6 P30 - Incident Response Policy. Defines escalation, containment, and eradication procedures in response to network-borne threats or intrusions, such as DDoS, lateral movement, or unauthorized access.

11. Reference Standards and Frameworks

11.1 This policy aligns with international standards and regulatory requirements defining secure network operations, segmentation, perimeter protection, and secure remote access.

11.2 ISO/IEC 27001

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

11.3 ISO/IEC 27002:2022

11.3.1 Controls 8.20-8.22. Provide guidance on protecting networks, segmenting services, and securing network services through access controls and monitoring.

11.4 NIST SP 800-53 Rev. 5

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

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

11.4.3 SC-32 - Information System Partitioning: Promotes logical separation of information systems.

11.5 EU GDPR (2016/679)

11.5.1 Article 32 - Security of Processing: Requires technical measures, such as firewalls and segmentation, to protect personal data.

11.6 EU NIS2 Directive (2022/2555)

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

11.7 EU DORA (2022/2554)

11.7.1 Article 9 - ICT Risk Management: Requires financial entities to protect networks and interconnections against unauthorized access, data leakage, and operational disruption risk.

11.8 COBIT 2019

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

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

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