Network Security Management Policy

DOCUMENT CLASSIFICATION	Internal
VERISON	1.0
DATE	
DOCUMENT AUTHOR	Ayaz Sabir
DOCUMENT OWNER	

REVISION HISTORY

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES

DISTRIBUTION LIST

NAME	SUMMARY OF CHANGE

APPROVAL

NAME	POSITION	SIGN

Contents

1. Introduction

In today's interconnected digital landscape, network infrastructure serves as the backbone of organizational operations, enabling communication, data exchange, and access to critical business systems. Networks facilitate the flow of sensitive information between users, systems, and external partners, making them attractive targets for cybercriminals and malicious actors. The increasing sophistication of cyber threats, combined with the growing complexity of network architectures including cloud services, remote access, and Internet of Things (IoT) devices, creates significant security challenges that require comprehensive management approaches.

This Network Security Management Policy establishes the framework for protecting the organization's network infrastructure and the information that traverses it in accordance with ISO/IEC 27001:2022 requirements, The policy outlines the principles, requirements, and processes for designing, implementing, and maintaining secure network architectures that protect against unauthorized access, data interception, network attacks, and service disruptions.

By implementing this policy, the organization demonstrates its commitment to maintaining robust network security that protects information assets, ensures business continuity, and supports regulatory compliance. The policy establishes a systematic approach to network security management that addresses both current threats and emerging risks while enabling secure and efficient business operations.

2. Purpose

The primary purpose of this Network Security Management Policy is to establish comprehensive security controls and management processes for the organization's network infrastructure. This policy aims to:

- **Protect Network Infrastructure**: Safeguard network components, including routers, switches, firewalls, wireless access points, and network management systems, from unauthorized access, tampering, and malicious attacks.

- **Secure Data in Transit**: Ensure the confidentiality, integrity, and availability of information as it travels across network connections, both within the organization and to external parties.
- **Control Network Access**: Implement appropriate access controls and authentication mechanisms to ensure that only authorized users and systems can access network resources and services.
- **Prevent Network-Based Attacks**: Establish defenses against common network attacks including denial of service, man-in-the-middle attacks, network scanning, and unauthorized network access attempts.
- **Ensure Network Availability**: Maintain reliable and resilient network services that support business operations and minimize the impact of network failures or security incidents.
- **Support Regulatory Compliance**: Meet applicable legal, regulatory, and contractual requirements related to network security, data protection, and privacy.
- **Enable Secure Remote Access**: Provide secure mechanisms for remote users to access organizational resources while maintaining appropriate security controls and monitoring.
- **Facilitate Incident Response**: Establish network monitoring and logging capabilities that support the detection, investigation, and response to security incidents.

3. Scope

This Network Security Management Policy applies to all network infrastructure components, connections, and services that support the organization's operations, including all organizational units, personnel, and third parties that design, implement, operate, or use network resources. The policy encompasses:

- **All Network Infrastructure**: Physical and virtual network components including routers, switches, firewalls, intrusion detection/prevention systems, wireless access points, network attached storage, and network management systems.
- **All Network Connections**: Internal network segments, internet connections, wide area network (WAN) links, virtual private networks (VPNs), wireless networks, and connections to third-party services and cloud providers.
- **All Network Services**: Domain name services (DNS), dynamic host configuration protocol (DHCP), network time protocol (NTP), email services, web services, file sharing, and other network-enabled applications and services.
- **All Network Users**: Employees, contractors, consultants, temporary workers, business partners, and authorized third parties who access or use network resources from any location or device.
- **All Network Environments**: Production networks, development and testing environments, disaster recovery networks, and any other network infrastructure that processes, stores, or transmits organizational information.
- **Entire Network Lifecycle**: From initial network design and implementation through ongoing operation, maintenance, monitoring, and eventual decommissioning of network components and services.

This policy establishes minimum security requirements for network management. Specific detailed procedures and technical configurations will be documented separately and referenced herein.

4. Policy Statements

This section outlines the mandatory principles and practices for managing network security, aligning with ISO/IEC 27001:2022 requirements. These statements provide clear management direction and support for all network security activities.

4.1 General Principles for Network Security

All network security activities must adhere to the following general principles to ensure comprehensive protection and effective management:

- **Defense in Depth**: Network security must implement multiple layers of protection, including perimeter security, network segmentation, access controls, monitoring, and incident response capabilities.
- **Least Privilege Access**: Network access must be granted based on the principle of least privilege, providing users and systems with only the minimum network access necessary to perform their authorized functions.
- **Network Segmentation**: Networks must be logically and physically segmented to limit the scope of potential security breaches and contain the impact of security incidents.
- **Continuous Monitoring**: Network traffic, performance, and security events must be continuously monitored to detect anomalies, security threats, and performance issues.
- **Secure by Design**: Network architectures and configurations must incorporate security considerations from the initial design phase rather than adding security as an afterthought.
- **Regular Assessment**: Network security controls and configurations must be regularly assessed, tested, and updated to address emerging threats and maintain effectiveness.

4.2 Network Architecture and Design

The organization shall implement secure network architecture principles and design standards:

- **Network Segmentation**: Networks shall be segmented based on business functions, security requirements, and risk levels, with appropriate controls between segments to prevent unauthorized access and limit the spread of security incidents.
- **Perimeter Security**: Network perimeters shall be clearly defined and protected with appropriate security controls including firewalls, intrusion detection/prevention systems, and access controls.
- **Secure Network Protocols**: Network communications shall use secure protocols and

encryption where appropriate to protect data in transit and prevent unauthorized interception or modification.

- **Redundancy and Resilience**: Critical network components and connections shall have appropriate redundancy and failover capabilities to ensure continued availability during failures or attacks.
- **Wireless Network Security**: Wireless networks shall implement strong authentication, encryption, and access controls to prevent unauthorized access and protect wireless communications.

4.3 Network Access Control

The organization shall implement comprehensive network access control measures:

- **User Authentication**: All network access shall require appropriate user authentication using strong authentication mechanisms and, where appropriate, multi-factor authentication.
- **Device Authentication**: Network-connected devices shall be authenticated and authorized before being granted network access, with appropriate controls for both managed and unmanaged devices.
- **Access Authorization**: Network access permissions shall be based on user roles, business requirements, and security policies, with regular review and approval processes.
- **Remote Access Security**: Remote network access shall be provided through secure channels with appropriate authentication, encryption, and monitoring controls.
- **Guest Network Access**: Guest and visitor network access shall be provided through segregated networks with limited access and appropriate monitoring.

4.4 Network Monitoring and Incident Response

The organization shall establish comprehensive network monitoring and incident response capabilities:

- **Traffic Monitoring**: Network traffic shall be monitored for security threats, performance issues, and policy violations using appropriate monitoring tools and techniques.
- **Security Event Detection**: Network security events shall be detected, logged, and analyzed using security information and event management (SIEM) systems or equivalent capabilities.
- **Incident Response**: Network security incidents shall be responded to promptly using established incident response procedures, with appropriate containment, investigation, and recovery actions.
- **Forensic Capabilities**: Network logging and monitoring systems shall maintain appropriate records to support forensic investigation of security incidents and compliance requirements.
- **Threat Intelligence**: Network security monitoring shall incorporate relevant threat intelligence to improve detection of known threats and attack patterns.

5. Roles and Responsibilities

5.1 Senior Management

Senior management is responsible for:

- Providing leadership and commitment to network security
- Allocating adequate resources for network security activities
- Approving network security policies and major architectural decisions
- Reviewing network security performance and incident reports
- Ensuring integration of network security with business planning

5.2 Chief Information Security Officer (CISO)

The CISO is responsible for:

- Developing and maintaining network security policies and procedures
- Overseeing network security architecture and design decisions
- Coordinating network security activities across the organization
- Monitoring network security performance and compliance
- Reporting network security status to senior management

5.3 Network Security Team

The network security team is responsible for:

- Implementing and maintaining network security controls
- Monitoring network traffic and security events
- Responding to network security incidents
- Conducting network security assessments and testing
- Maintaining network security documentation and procedures

5.4 IT Operations Team

The IT operations team is responsible for:

- Operating and maintaining network infrastructure
- Implementing network security configurations and changes
- Monitoring network performance and availability
- Supporting network security incident response activities
- Maintaining network inventory and documentation

5.5 Business Unit Managers

Business unit managers are responsible for:

- Identifying business requirements for network access and services

- Ensuring personnel understand network security requirements
- Supporting network security initiatives within their areas
- Reporting network security concerns and incidents
- Participating in network security risk assessments

5.6 All Personnel

All personnel are responsible for:

- Following network security policies and procedures
- Using network resources appropriately and securely
- Reporting suspected network security incidents
- Protecting network access credentials and devices
- Participating in network security training and awareness programs

6. Network Security Controls

6.1 Perimeter Security

Network perimeters shall be protected through comprehensive security controls:

- **Firewall Protection**: All network perimeters shall be protected by appropriately configured firewalls that control traffic based on established security policies and business requirements.
- **Intrusion Detection and Prevention**: Network perimeters shall be monitored by intrusion detection and prevention systems that can identify and respond to malicious network activity.
- **Network Address Translation**: Internal network addressing shall be protected through network address translation (NAT) and private addressing schemes that limit external visibility of internal network structure.

- **Demilitarized Zones**: Public-facing services shall be deployed in demilitarized zones (DMZ) with appropriate security controls and limited access to internal networks.

- **VPN Gateways**: Remote access shall be provided through secure VPN gateways with strong authentication, encryption, and access controls.

6.2 Internal Network Security

Internal networks shall implement appropriate security controls:

- **Network Segmentation**: Internal networks shall be segmented based on business functions, security requirements, and risk levels, with appropriate access controls between segments.

- **VLAN Security**: Virtual local area networks (VLANs) shall be used to logically separate network traffic, with appropriate security controls and access restrictions.

- **Switch Security**: Network switches shall be configured with appropriate security settings including port security, DHCP snooping, and dynamic ARP inspection.

- **Routing Security**: Network routing shall be secured through appropriate authentication, access controls, and monitoring of routing protocols and tables.

- **Network Access Control**: Internal network access shall be controlled through network access control (NAC) systems that authenticate and authorize devices before granting network access.

6.3 Wireless Network Security

Wireless networks shall implement comprehensive security controls:

- **Encryption**: All wireless communications shall be encrypted using strong encryption protocols (WPA3 or equivalent) to protect data in transit.

- **Authentication**: Wireless network access shall require strong authentication, preferably using enterprise authentication systems with individual user credentials.

- **Access Point Security**: Wireless access points shall be securely configured and managed, with regular security updates and monitoring.

- **Rogue Access Point Detection**: Networks shall be monitored for unauthorized wireless access points and appropriate response procedures shall be implemented.
- **Guest Network Isolation**: Guest wireless access shall be provided through isolated networks with limited access and appropriate monitoring.

6.4 Network Monitoring and Logging

Comprehensive network monitoring and logging shall be implemented:

- **Traffic Analysis**: Network traffic shall be analyzed for security threats, performance issues, and policy violations using appropriate monitoring tools.
- **Security Event Logging**: Network security events shall be logged and retained according to established retention policies and regulatory requirements.
- **Performance Monitoring**: Network performance shall be monitored to ensure availability and identify potential security issues or capacity problems.
- **Compliance Monitoring**: Network configurations and activities shall be monitored for compliance with security policies and regulatory requirements.
- **Alerting and Notification**: Automated alerting shall be implemented for critical network security events and performance issues.

7. Network Access Management

7.1 User Access Control

Network access for users shall be managed through systematic processes:

- **Access Request Process**: Network access requests shall follow established approval processes based on business requirements and security policies.
- **Identity Verification**: User identities shall be verified before granting network access, with appropriate documentation and approval.
- **Access Provisioning**: Network access shall be provisioned based on approved

requests and least privileged principles.

- **Access Review**: User network access shall be reviewed regularly to ensure continued appropriateness and business need.
- **Access Revocation**: Network access shall be promptly revoked when no longer required or when employment or contract relationships end.

7.2 Device Access Control

Network access for devices shall be controlled and managed:

- **Device Registration**: Network-connected devices shall be registered and approved before being granted network access.
- **Device Authentication**: Devices shall be authenticated using appropriate mechanisms such as certificates, MAC address filtering, or network access control systems.
- **Device Compliance**: Devices shall meet established security requirements including security updates, antivirus protection, and configuration standards.
- **Device Monitoring**: Network-connected devices shall be monitored for security compliance and suspicious activity.
- **Device Quarantine**: Non-compliant or suspicious devices shall be quarantined or isolated from the network until issues are resolved.

7.3 Remote Access Security

Remote network access shall be secured through appropriate controls:

- **VPN Requirements**: Remote access shall be provided through secure VPN connections with strong encryption and authentication.
- **Multi-Factor Authentication**: Remote access shall require multi-factor authentication to verify user identity.
- **Endpoint Security**: Remote access devices shall meet established security requirements including security updates and endpoint protection.

- **Session Management**: Remote access sessions shall be managed with appropriate timeouts, monitoring, and logging.
- **Split Tunneling Controls**: Split tunneling shall be controlled or prohibited to prevent unauthorized access to internal networks.

8. Network Incident Response

8.1 Incident Detection

Network security incidents shall be detected through multiple mechanisms:

- **Automated Monitoring**: Automated monitoring systems shall detect and alert suspicious network activity and security events.
- **User Reporting**: Personnel shall be trained to recognize and report potential network security incidents.
- **Threat Intelligence**: External threat intelligence shall be used to enhance detection of known threats and attack patterns.
- **Performance Monitoring**: Network performance monitoring shall identify potential security incidents that may impact network availability.
- **Log Analysis**: Network logs shall be regularly analyzed for indicators of security incidents or policy violations.

8.2 Incident Response Process

Network security incidents shall be responded to using established procedures:

- **Incident Classification**: Network incidents shall be classified based on severity, impact, and type to determine appropriate response procedures.
- **Incident Containment**: Network incidents shall be contained to prevent further damage or spread to other network segments.
- **Incident Investigation**: Network incidents shall be investigated to determine root causes, impact, and appropriate remediation actions.

- **Incident Recovery**: Network services shall be restored following security incidents with appropriate verification of security and functionality.

- **Incident Documentation**: Network incidents shall be documented with appropriate details for analysis, reporting, and lessons learned.

8.3 Business Continuity

Network security incident response shall support business continuity:

- **Backup Network Services**: Critical network services shall have backup or alternative capabilities to maintain operations during incidents.
- **Communication Plans**: Communication plans shall ensure appropriate notification of network incidents to stakeholders and management.

- **Recovery Procedures**: Network recovery procedures shall be established and tested to ensure rapid restoration of services.

- **Vendor Support**: Vendor support arrangements shall be established for critical network components and services.
- **Testing and Exercises**: Network incident response procedures shall be regularly tested through exercises and simulations.

9. Network Security Assessment

9.1 Vulnerability Assessment

Regular vulnerability assessments shall be conducted on network infrastructure:

- **Automated Scanning**: Automated vulnerability scanning shall be performed regularly on network devices and services.

- **Manual Testing**: Manual security testing shall be conducted to identify vulnerabilities that may not be detected by automated tools.

- **Penetration Testing**: Periodic penetration testing shall be conducted by qualified personnel to assess the effectiveness of network security controls.

- **Risk Assessment**: Identified vulnerabilities shall be assessed for risk and prioritized for remediation based on potential impact and likelihood.

- **Remediation Tracking**: Vulnerability remediation shall be tracked and verified to ensure timely resolution of security issues.

9.2 Security Auditing

Network security controls shall be regularly audited:

- **Configuration Audits**: Network device configurations shall be audited against established security baselines and standards.
- **Access Audits**: Network access permissions and controls shall be audited to ensure compliance with policies and least privilege principles.

- **Compliance Audits**: Network security controls shall be audited for compliance with applicable regulations and standards.

- **Third-Party Audits**: Independent third-party audits shall be conducted periodically to provide objective assessment of network security.

- **Audit Follow-up**: Audit findings shall be tracked and remediate according to established procedures and timelines.

9.3 Continuous Improvement

Network security shall be continuously improved based on assessment results:

- **Performance Metrics**: Network security performance shall be measured using established metrics and key performance indicators.

- **Trend Analysis**: Security trends and patterns shall be analyzed to identify areas for improvement and emerging threats.

- **Best Practices**: Industry best practices and standards shall be evaluated and implemented where appropriate.

- **Technology Updates**: New security technologies and solutions shall be evaluated for potential implementation.

- **Lessons Learned**: Lessons learned from incidents and assessments shall be incorporated into security improvements.

10. Training and Awareness

10.1 Personnel Training

Network security training shall be provided to relevant personnel:

- **Role-Based Training**: Training shall be tailored to specific roles and responsibilities related to network security.
- **Technical Training**: Technical personnel shall receive training on network security technologies, tools, and procedures.
- **Security Awareness**: General security awareness training shall include network security topics relevant to all personnel.
- **Incident Response Training**: Personnel involved in incident response shall receive specialized training on network incident response procedures.
- **Ongoing Education**: Continuing education shall be provided to maintain current knowledge of network security threats and technologies.

10.2 Competency Requirements

Personnel with network security responsibilities shall meet established competency requirements:

- **Qualifications**: Personnel shall have appropriate education, training, and experience for their network security responsibilities.
- **Certifications**: Relevant professional certifications shall be encouraged and supported for personnel with network security roles.
- **Skills Assessment**: Personnel skills and competencies shall be regularly assessed and development needs identified.

- **Professional Development**: Opportunities for professional development shall be provided to enhance network security capabilities.
- **Knowledge Transfer**: Knowledge transfer processes shall ensure continuity of network security expertise.

11. Definitions

- **Access Control List (ACL)**: A list of permissions attached to network resources that specifies which users or systems are granted access and what operations are allowed.
- **Demilitarized Zone (DMZ)**: A network segment that sits between the internal network and external networks, typically used to host public-facing services.
- **Firewall**: A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- **Intrusion Detection System (IDS)**: A security system that monitors network traffic for suspicious activity and alerts administrators to potential threats.
- **Intrusion Prevention System (IPS)**: A security system that monitors network traffic and can automatically block or prevent detected threats.
- **Network Access Control (NAC)**: A security solution that controls access to network resources by authenticating and authorizing devices and users.
- **Network Segmentation**: The practice of dividing a network into smaller segments to improve security and performance by limiting access between segments.
- **Perimeter Security**: Security measures implemented at the boundary between internal and external networks to control access and protect against threats.
- **Virtual Local Area Network (VLAN)**: A logical grouping of network devices that can span multiple physical network segments while maintaining isolation.
- **Virtual Private Network (VPN)**: A secure connection method that creates an encrypted tunnel over a public network to provide secure remote access.

- **Wireless Access Point**: A networking device that allows wireless devices to connect to a wired network using Wi-Fi or related standards.

- **Network Address Translation (NAT)**: A method of mapping private IP addresses to public IP addresses to hide internal network structure.
- **Security Information and Event Management (SIEM)**: A security management approach that combines security information management and security event management.

- **Man-in-the-Middle Attack**: A type of cyberattack where an attacker intercepts and potentially alters communications between two parties.

- **Denial of Service (DoS)**: An attack that attempts to make network resources unavailable to legitimate users by overwhelming them with traffic.

- **Distributed Denial of Service (DDoS)**: A DoS attack that uses multiple compromised systems to generate attack traffic.

- **Network Monitoring**: The continuous observation of network performance, availability, and security to identify issues and threats.

- **Packet Filtering**: A firewall technique that examines packets and allows or blocks them based on source and destination addresses, ports, and protocols.

12. References

- Information Security Policy
- Access Control Policy
- Incident Response Policy
- Business Continuity Policy
- Risk Management Policy

- Change Management Procedures