TECH THAT MATTERS

Elevaite365

Network Management Policy

Version 1.0

PURPOSE

This Network Management Policy outlines the standards and practices that Elevaite365 (herein referred to as “Organization”) follows to ensure the safety and security of the company’s networks. The policy aims to protect the Organization’s information assets and those of its clients from unauthorized access, disclosure, alteration, and destruction.

SCOPE

This policy applies to the organization and its employees, contractors, and third parties. It covers all individuals with authorized access to any of the Organization’s information assets. It encompasses all network infrastructure, including Local Area Networks (LAN), Wide Area Networks (WAN), Wireless LANs (WLAN), and other related network systems.

DEFINITION

1. **Network:** A set of two or more computing devices connected for exchanging electronic information (e.g., LAN, WAN, WLAN, etc.).
2. **Guest Account:** A default set of permissions and privileges given to non-registered users of a system or service.
3. **Vulnerability Assessment is the** testing process used to identify and assign severity levels to as many security defects as possible within a given timeframe. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage.
4. **Penetration Testing:** The practice of simulating cyberattacks against an organization’s systems to identify vulnerabilities that could be potentially exploited.

RESPONSIBILITY

1. **IT and DevOps Team**
    a. **Technical Support:** Provide technical support and ensure all network devices meet security requirements.
    b. **Configuration Management:** Ensure the proper configuration of network devices complies with this policy.
    c. **Security Controls Implementation:** Implement and maintain security controls on network systems, such as firewalls, encryption, and access controls.
    d. **Vulnerability Management:** Conduct regular vulnerability assessments and penetration testing and ensure timely remediation of identified vulnerabilities.
2. **Information Security Group (ISG)**
    a. **Policy Implementation:** Responsible for implementing this policy in coordination with the IT and DevOps teams.
    b. **Awareness and Training:** Ensure all employees understand and undertake their responsibilities regarding network management.
    c. **Compliance Monitoring:** Monitor adherence to this policy and report non-compliance to top management.
    d. **Incident Response:** Manage and respond to security incidents related to network systems.

POLICY

Network Controls

Network Design and Documentation

1. **Secure Design Practices**: Networks shall be designed to conform to sound security practices.
2. **Formal Documentation:** Maintain formal documentation outlining the network’s details and service requirements to support the network design.
3. **Redundancy and Availability:** Ensure adequate redundancy of critical network components to guarantee high availability.
4. **Minimization of Vulnerabilities:** Minimize single points of failure and reduce the number of entry points into the network.

Network Protocols and Encryption

1. **Secure Protocols:** Prefer secure protocols over unsecured ones (e.g., HTTPS over HTTP, SFTP over FTP, SSH over Telnet).
2. **Encryption:** Implement encryption for sensitive data at rest and in transit using strong encryption algorithms (e.g., AES-256 for data storage, TLS/SSL for data transmission).

3. **Encryption Approval:** The IT Head must approve the encryption methods to ensure they meet the Encryption and Key Management Policy requirements.

Firewalls and Access Control

1. **Firewall Deployment:** Deploy firewalls to control network traffic and prevent unauthorized access. Firewalls must be configured to allow only necessary traffic and block all other traffic.
2. **Access Allocation:** Access to the network and network services shall be allocated, changed, or revoked following the Access Control Policy.
3. **Vendor Credentials:** Change vendor-supplied default credentials (administrative or otherwise) on network devices before operationalizing them.
4. **Guest Accounts:** Deactivate all network systems with built-in guest accounts by default.

Network Service Management

1. **Authorized Services:** Ensure that network services accept communications only from authenticated sources.
2. **Secure Remote Access:** Internal parties can access the cloud from remote locations only through secure remote access mechanisms. External parties are prohibited from accessing the Organization's cloud environment.
3. **Standard Configurations**: Maintain and use standard configurations for network devices. The DevOps team shall periodically review network configurations against these standards.

Device and Port Security

1. **Diagnostic Ports:** Control access to diagnostic ports on network devices to prevent unauthorized use.
2. **Data Source Restrictions**: Mobile devices and removable media should not be used as primary data sources. Primary copies of source data must reside in Organization-managed central repositories.
3. **Data Synchronization:** Synchronize data only with Organization-owned and approved devices when dealing with confidential information.

Security of Network Services

Web Server Protection

1. **Firewall Protection:** All web servers accessible through the Internet must be protected by a firewall approved by the CISO.
2. **Authenticated Access:** Network services must only accept communications from authenticated sources.

Secure Communications

1. **Encryption:** All transmissions across wireless networks must use encryption.
2. **Wireless Firewalls:** Wireless network gateways must employ firewalls to filter communications with remote devices.
3. **Confidential Data Transmission:** Confidential information must never be transmitted unencrypted.

Vulnerability Assessments and Penetration Testing

1. **Regular Assessments:** The CISO is responsible for scheduling and overseeing the network and applications' annual vulnerability assessments and penetration tests.
2. **Patch Management:** The DevOps team must regularly plan and deploy appropriate patches, adhering to the Patch and Vulnerability Management Policy.

Outsourcing and Vendor Management

1. **Outsourced Services:** Network device acquisition and deployment may only be outsourced to third parties if they follow best security practices and comply with the IT Hardening Guidelines.
2. **Configuration Standards:** Ensure that any outsourced services adhere to the Organization's configuration standards and security policies.

Business Continuity and Disaster Recovery

1. Maintenance: Maintain and annually test business continuity and disaster recovery plans for the network following the Business Continuity Policy.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Aug 29 2025	Initial Release	Borhan	Linh	Borhan