Network Access Management

Diné College Information Technology

Ihab Saleh

Revision History

Version Number	Revision Date
1.0	10/2/2024

Table of Contents

Table of Contents 2
1. Purpose 3
2. Scope 3
3. Roles and responsibilities 3
4. Access Control Standards 4
5. Network Access Requirements 4
6. Remote Access Management 6
7. Guest and Temporary Access 7
8. Enforcement 7

1. Purpose

This section outlines the purpose of the Network Access Management Policy, which is to ensure secure, authorized access to the organization's network. The policy establishes rules for granting, managing, and revoking access to both wired and wireless network resources to protect the confidentiality, integrity, and availability of information systems. Access controls will ensure that access is restricted to authorized personnel and compliant with regulatory, operational, and security requirements.

2. Scope

This policy applies to all employees, contractors, third-party personnel, and guests who access the organization's network resources, whether through wired, wireless, or remote connections. It covers the access management process, from initial access requests to ongoing monitoring and eventual revocation of access.

The policy encompasses all devices that connect to the network, including workstations, mobile devices, and personal devices, as well as any access to the network through remote services such as VPNs. It also includes guidelines for guest access and temporary access granted for specific purposes.

3. Roles and responsibilities

This section outlines the responsibilities of individuals and teams involved in the management and enforcement of network access controls.

Chief Information Security Officer (CISO)

The CISO is responsible for overseeing network access management, ensuring that access control policies and procedures align with organizational security requirements. The CISO also reviews access management reports and approves exceptions to this policy.

Network Engineering Team

The Network Engineering Team is responsible for implementing and managing technical controls that govern access to the network. This includes configuring network devices and ensuring that only authorized individuals and devices can connect to the network. The team also works closely with the Information Security Team to monitor network access and detect any unauthorized activity.

Information Security Team

The Information Security Team is tasked with monitoring network access to ensure that security protocols are enforced. This includes reviewing access logs, identifying anomalies, and responding to security incidents. The team also works with the Network Engineering Team to manage access for new hires, contractors, and third-party personnel.

Human Resources (HR)

HR is responsible for informing the Information Security Team and Network Engineering Team of changes to employment status, such as new hires, terminations, or role changes, which may affect network access permissions.

Employees and Contractors

All employees and contractors are responsible for complying with the organization's network access policies. They must ensure that their network credentials are secure and report any unauthorized access or suspicious activity immediately to the IT helpdesk or Information Security Team.

4. Access Control Standards

This section establishes the standards for granting and managing access to the organization's network, ensuring secure access practices are in place.

Access to the network is granted based on the principle of least privilege, meaning users are given the minimum level of access necessary to perform their job functions. Network access must be requested through the appropriate channels, with approvals from department heads and the Information Security Team before access is granted.

Access credentials, including usernames, passwords, and multifactor authentication (MFA) tokens, must be securely managed, and credentials must be unique to each user. Users must undergo periodic access reviews to ensure their access level remains appropriate. Access credentials must be revoked immediately upon termination or when access is no longer required.

5. Network Access Requirements

This section outlines the comprehensive requirements for obtaining, maintaining, and revoking access to the organization's network, ensuring that network security and access control measures are consistently applied.

User Identification and Authentication

All individuals requesting access to the network must be uniquely identified through a formal onboarding process. This process requires each user to be assigned a unique username and password, ensuring that their activities can be traced back to them. Multifactor Authentication (MFA) is mandatory for users with elevated privileges, including administrators and remote users. Passwords must meet the organization's complexity requirements, including a combination of uppercase and lowercase letters, numbers, and special characters. Passwords must be changed regularly, and users are prohibited from sharing credentials under any circumstances.

Device Compliance

Only devices that meet the organization's security standards are permitted to connect to the network. This includes personal devices (BYOD) and company-issued devices. All devices must have up-to-date operating systems, active antivirus software, and all critical security patches installed. Devices must also adhere to encryption standards to protect sensitive data in transit and at rest. The organization may implement endpoint security solutions to ensure compliance, and non-compliant devices will be denied network access until remediation is complete. The Information Security Team will conduct regular audits of devices connected to the network to ensure ongoing compliance.

Network Segmentation and Privileged Access

The organization utilizes network segmentation to limit the exposure of critical systems and sensitive data. Segments of the network that handle high-risk or confidential data are separated from general user access networks. Access to these segments is strictly limited and requires privileged access, which is managed through dedicated security controls. Privileged users, such as system administrators, database administrators, and IT security personnel, are subject to additional access controls, including regular audits and enhanced logging to track activities.

Periodic Access Reviews

Periodic reviews of all user access privileges must be conducted at least quarterly. These reviews are aimed at identifying any inappropriate access levels or dormant accounts that may pose security risks. Department heads, working in coordination with the Information Security Team, are responsible for reviewing and confirming that access privileges are appropriate and aligned with current job roles. Any discrepancies or outdated access permissions must be addressed immediately to prevent unauthorized access. Accounts that have not been used within a defined period will be flagged for review and may be disabled or revoked if no longer necessary.

Access Revocation

The organization must promptly revoke network access for any users whose employment or contract has been terminated or whose role has changed in a way that no longer requires access to certain systems or data. Access revocation should occur immediately upon the user's departure or role change. Human Resources must notify the Information Security Team and the Network Engineering Team of any terminations or role changes that may impact network access. Accounts related to terminated users should be disabled, and all network credentials, including VPN tokens, smart cards, and hardware keys, must be returned to the organization. Failure to return access credentials or hardware could result in disciplinary action or legal proceedings.

Data Encryption and Transmission Security

All sensitive information transmitted over the network, whether internally or externally, must be encrypted in transit using industry-standard encryption protocols such as TLS (Transport Layer

Security). Encryption must also be used for data stored on devices, including portable storage devices such as USB drives and laptops, to prevent unauthorized access in the event of loss or theft. Network traffic between segments that handle sensitive data must be monitored and encrypted to mitigate the risk of interception or unauthorized access.

Third-Party Access Management

Third parties, including contractors, vendors, and partners, who require access to the network must undergo a vetting process to ensure that they meet the organization's security and compliance requirements. Third-party access must be limited to the specific systems and data necessary for their work and must be time-bound to prevent prolonged access beyond project needs. Contracts with third-party service providers must include clear requirements for network access management, compliance with organizational policies, and regular security audits. All third-party access must be logged and monitored, and access privileges must be reviewed regularly to ensure ongoing compliance.

Role-Based Access Control (RBAC)

Access to network resources is governed by the principle of least privilege. Each user is assigned access based on their role within the organization, ensuring they can only access the resources required to perform their job functions. Users will not be granted access to systems, data, or applications outside their operational scope unless explicitly approved by management and the Information Security Team. Access to sensitive data, such as financial, personal, or health information, is further restricted to authorized personnel with additional security measures in place, including encryption, access logs, and audit trails.

6. Remote Access Management

This section provides guidelines for secure remote access to the organization's network and the management of personal devices (BYOD), ensuring that off-site access is tightly controlled and compliant with security standards.

Remote access to the network, including access via Virtual Private Networks (VPN), must be authorized by the Information Security Team and granted only to users with a legitimate business need. All remote access sessions must be secured using multifactor authentication (MFA) and strong encryption protocols. These sessions must be logged and monitored regularly for unauthorized activity or potential security threats.

Devices used for remote access, whether organizational or personal, must adhere to the organization's security compliance standards. Personal devices (BYOD) used for remote access must comply with the organization's BYOD policy, which requires devices to have enterprise-level security protections, including device encryption, remote wipe capabilities, and endpoint security solutions. Devices accessing sensitive organizational data must undergo regular security assessments to identify vulnerabilities. Any detected vulnerabilities must be resolved before the device is permitted access to

the network. Additionally, all sensitive data transmitted during remote access sessions must be encrypted to ensure the confidentiality and integrity of the information.

7. Guest and Temporary Access

This section outlines the rules for providing network access to guests or individuals who require temporary access for specific purposes.

Guest access may be granted for visitors, contractors, or temporary personnel who need access to the organization's network for a limited time. Guest access must be requested and approved through the IT helpdesk or Information Security Team. All guest access accounts must have an expiration date and limited privileges to ensure minimal risk.

Temporary access for employees or contractors working on short-term projects must follow the same access control standards, with appropriate review and revocation once the project is completed.

8. Enforcement

This section outlines how compliance with the Network Access Management Policy is enforced and the consequences of violations.

Violations of this policy will result in disciplinary actions in accordance with organizational regulations and applicable laws. Consequences may include mandatory re-training, suspension of network access, termination of employment, or legal action in severe cases where violations lead to data breaches or other security incidents.

Regular audits of network access controls will be conducted by the Information Security Team to ensure compliance. Non-compliance will be documented, and corrective actions will be taken immediately. Persistent violations or failure to resolve issues may result in escalated actions, including management reviews and involvement of external auditors.