[Company Name] Network Security Policy

**Document Version:** 1.0 **Date:** March 7, 2025

## 1. Overview

This Network Security Policy defines the rules and guidelines for securing [Company Name]’s network infrastructure and protecting it from unauthorized access, misuse, and disruption. It applies to all employees, contractors, vendors, and anyone accessing the company network.

## 2. Purpose

The purpose of this policy is to:

* Protect the confidentiality, integrity, and availability of data transmitted and stored on the company network.
* Prevent unauthorized access to network resources.
* Minimize the risk of network-based attacks (e.g., malware, hacking, denial-of-service).
* Ensure compliance with relevant regulations and security standards.
* Provide a secure and reliable network environment for business operations.

## 3. Scope

This policy applies to all network infrastructure owned, leased, or controlled by [Company Name], including:

* **Network Devices:** Routers, switches, firewalls, wireless access points, modems.
* **Servers:** File servers, application servers, email servers.
* **Endpoints:** Computers, laptops, mobile devices connected to the network.
* **Network Connections:** Wired and wireless connections, VPN connections, internet connections.
* **Network Traffic:** All data transmitted over the company network.
* **Cloud Services:** Any cloud-based services accessed through the company network.

## 4. Policy

### 4.1. Network Access Control

* Access to the company network will be granted only to authorized users and devices.
* Strong authentication mechanisms (e.g., passwords, multi-factor authentication) will be used to verify user identity.
* Network segmentation will be implemented, where feasible, to limit the impact of security breaches. (This might be limited in a small company, but consider separating guest Wi-Fi from the main network).
* Wireless networks will be secured using strong encryption protocols (e.g., WPA2 or WPA3).
* Guest Wi-Fi access, if provided, will be separate from the internal company network and have restricted access.

### 4.2. Firewall Management

* A firewall will be implemented to protect the company network from external threats.
* Firewall rules will be configured to allow only necessary traffic and block all other traffic.
* Firewall logs will be regularly monitored for suspicious activity.
* Firewall software will be kept up-to-date with the latest security patches.

### 4.3. Intrusion Detection and Prevention

* [Intrusion detection/prevention systems (IDS/IPS) may be implemented, depending on the company’s size and risk profile. If not feasible, consider using a managed security service provider (MSSP) that offers this.]
* IDS/IPS logs will be regularly monitored for security alerts.

### 4.4. Remote Access

* Remote access to the company network will be granted only to authorized users and through secure methods (e.g., VPN).
* Remote access devices must comply with company security policies (e.g., endpoint security, password protection).
* Two-factor authentication is strongly recommended for remote access.

### 4.5. Network Monitoring

* Network traffic will be monitored for suspicious activity.
* Network performance will be monitored to identify potential problems.
* Logs from network devices will be collected and analyzed.

### 4.6. Vulnerability Management

* Regular vulnerability scans will be conducted to identify security weaknesses in network devices and systems.
* Identified vulnerabilities will be addressed promptly through patching or other mitigation measures.

### 4.7. Wireless Security

* Strong encryption (WPA2/WPA3) will be used for all wireless networks.
* Default wireless network names (SSIDs) and passwords will be changed.
* Wireless access points will be physically secured.
* Rogue access points will be detected and disabled.

### 4.8. Acceptable Use

* All network users must adhere to the company’s Acceptable Use Policy.

## 5. Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract, and potential legal action.

## 6. Revision History

| Version | Date | Author | Description of Change |
| --- | --- | --- | --- |
| 1.0 | March 7, 2025 | Shijie Yin | Initial Policy Creation |