[Company Name] Endpoint Security Policy

**Document Version:** 1.0 **Date:** March 11, 2025

## 1. Overview

This Endpoint Security Policy defines the security requirements for all endpoints that connect to [Company Name]’s network or access company data. Endpoints include desktops, laptops, servers, tablets, smartphones, and any other devices used to access company resources. This policy aims to protect these devices and the data they store and process from threats. It applies to all employees, contractors, and vendors.

## 2. Purpose

The purpose of this policy is to:

* Protect endpoints from malware, unauthorized access, and data loss.
* Ensure the confidentiality, integrity, and availability of data stored on and accessed by endpoints.
* Minimize the risk of security breaches originating from endpoints.
* Comply with relevant security standards and regulations.
* Establish a consistent level of security across all company endpoints.

## 3. Scope

This policy applies to all endpoints, including:

* **Company-Owned Devices:** Desktops, laptops, servers, tablets, and smartphones provided by [Company Name].
* **Personally-Owned Devices (BYOD):** Personal devices used to access company data or networks (subject to the Remote Work & BYOD Policy).
* **Operating Systems:** Windows, macOS, Linux, iOS, Android.
* **Data:** All company data stored on or accessed by endpoints.

## 4. Policy

### 4.1. Antivirus and Anti-Malware Protection

* All endpoints must have up-to-date antivirus and anti-malware software installed and running.
* Regular scans must be performed.
* Real-time protection must be enabled.
* Virus definitions must be updated automatically.
* Users are prohibited from disabling or tampering with antivirus/anti-malware software.

### 4.2. Software Updates and Patching

* All endpoints must have the latest operating system and application security patches installed promptly.
* Automatic updates should be enabled where possible.
* Users will be notified of required updates and given a reasonable timeframe to install them.

### 4.3. Host-Based Firewall

* A host-based firewall must be enabled on all endpoints.
* The firewall should be configured to block unnecessary inbound connections.

### 4.4. Password Protection

* All endpoints must be password-protected.
* Passwords must comply with the company’s Password Policy (as defined in the Access Control Policy).
* Screen locks must be enabled and set to activate after a short period of inactivity.

### 4.5. Data Encryption

* Full-disk encryption (e.g., BitLocker, FileVault) is strongly recommended for all laptops and other portable devices.
* Sensitive data stored on endpoints should be encrypted.
* Encryption keys must be securely managed.

### 4.6. Mobile Device Management (MDM)

* [If the company uses mobile devices extensively, consider implementing a Mobile Device Management (MDM) solution to manage and secure these devices. If not feasible, focus on the other sections.]
* MDM can be used to enforce security policies, remotely wipe lost or stolen devices, and manage applications.

### 4.7. Removable Media

* The use of removable media (e.g., USB drives, external hard drives) should be restricted or controlled.
* Data transferred to removable media must be encrypted.
* Scanning removable media for malware before use is recommended.
* Do not use untrusted removable media.

### 4.8. Software Installation

* Users are prohibited from installing unauthorized software on company-owned endpoints.
* Software installations should be performed by authorized IT personnel or through approved channels.

### 4.9. Physical Security

* Endpoints must be physically secured to prevent theft or unauthorized access.
* Laptops should be locked with a cable lock when left unattended.
* Report lost or stolen devices immediately.

### 4.10. Acceptable Use

* All endpoint 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 11, 2025 | Shijie Yin | Initial Policy Creation |