[Company Name] Access Control Policy

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

## 1. Overview

This Access Control Policy defines how [Company Name] manages and controls access to its information systems, data, and physical facilities. It establishes principles and procedures to ensure that only authorized individuals have appropriate access, based on the principles of least privilege and need-to-know. This policy applies to all employees, contractors, vendors, and any other individuals accessing company resources.

## 2. Purpose

The purpose of this policy is to:

* Protect the confidentiality, integrity, and availability of company information and systems.
* Prevent unauthorized access to sensitive data and resources.
* Ensure compliance with relevant regulations and legal requirements.
* Minimize the risk of security breaches and data loss.
* Establish clear accountability for access management.

## 3. Scope

This policy applies to all forms of access to [Company Name]’s resources, including:

* **Logical Access:** Access to computer systems, networks, applications, databases, and data files.
* **Physical Access:** Access to company offices, buildings, server rooms, and other restricted areas.
* **Remote Access:** Access to company resources from outside the company network.
* **User Accounts:** All user accounts, including employee accounts, contractor accounts, and vendor accounts.
* **Data Access:** Access to all forms of company data, electronic and physical.

## 4. Policy

### 4.1. Access Control Principles

* **Least Privilege:** Users should be granted only the minimum necessary access rights required to perform their job duties.
* **Need-to-Know:** Access to sensitive information should be restricted to individuals who have a legitimate business need to access it.
* **Separation of Duties:** Critical tasks should be divided among multiple individuals to prevent any single person from having complete control and the potential for abuse. (This may be challenging in a very small company, but should be considered where possible.)
* **Accountability:** All access to company resources should be traceable to individual users.

### 4.2. User Account Management

* **Account Creation:** New user accounts will be created only upon proper authorization from [Designated Authority - e.g., Office Manager, Owner].
* **Unique User IDs:** Each user will be assigned a unique user ID.
* **Password Policy:** All users must adhere to the company’s password policy, which includes requirements for password complexity, length, and expiration. (See Section 4.3)
* **Account Review:** User accounts and access rights will be reviewed regularly (at least annually) to ensure they are still appropriate.
* **Account Deactivation:** User accounts will be deactivated promptly when an employee leaves the company, a contract ends, or access is no longer needed.
* **Account Lockout:** Accounts will be automatically locked after a specified number of failed login attempts.

### 4.3. Password Policy

* **Complexity:** Passwords must meet minimum complexity requirements, including a mix of uppercase and lowercase letters, numbers, and symbols.
* **Length:** Passwords must be at least [Number] characters long. (Recommendation: 8 or more)
* **Expiration:** Passwords must be changed every [Number] days. (Recommendation: 90 days)
* **History:** Users cannot reuse previous passwords. (Recommendation: Remember at least the last 5 passwords)
* **Prohibited Passwords:** Users must not use easily guessable passwords, such as their name, username, birthdate, or common words.

### 4.4. Access Authorization

* Access to specific systems, applications, and data will be granted based on job roles and responsibilities.
* Requests for access must be submitted to [Designated Authority] and approved before access is granted.
* Access rights will be documented and maintained.

### 4.5. Remote Access

* Remote access to company resources 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).

### 4.6. Physical Access Control

* Physical access to company facilities will be restricted to authorized personnel.
* Visitors must be escorted by authorized personnel.
* Access to sensitive areas (e.g., server rooms) will be further restricted and monitored.
* Keycard or other access control systems should be used where appropriate.

### 4.7. Data Access

* Data access will be controlled based on data classification and sensitivity levels.
* Sensitive data will be encrypted both in transit and at rest where feasible.

## 5. Monitoring and Auditing

* Access to company resources will be monitored and audited regularly.
* Audit logs will be reviewed for suspicious activity.
* Security violations will be investigated and addressed promptly.

## 6. 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.

## 7. Revision History

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