[Company Name] Security Awareness & Training Policy

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

## 1. Overview

This Security Awareness and Training Policy outlines [Company Name]'s commitment to educating employees, contractors, and vendors about information security risks and best practices. It establishes a program to ensure that all personnel understand their responsibilities in protecting company data and systems.

## 2. Purpose

The purpose of this policy is to:

* Raise awareness of information security threats and vulnerabilities.
* Educate personnel about their roles and responsibilities in protecting company information.
* Reduce the risk of security incidents caused by human error.
* Promote a culture of security awareness within the organization.
* Comply with any relevant regulatory requirements related to security training.

## 3. Scope

This policy applies to all employees, contractors, vendors, and any other individuals who access or use [Company Name]'s information systems, data, or facilities.

## 4. Policy

### 4.1. Training Program

* [Company Name] will implement a security awareness and training program that includes the following components:
  + **Initial Training:** All new hires will receive security awareness training as part of their onboarding process.
  + **Regular Training:** All personnel will receive ongoing security awareness training at least annually.
  + **Targeted Training:** Specific training may be provided to individuals with specific roles or responsibilities (e.g., those handling sensitive data).
  + **Training Methods:** Training may be delivered through various methods, including:
    - Online modules.
    - In-person presentations.
    - Newsletters or email updates.
    - Posters or other visual aids.
    - Simulated phishing exercises.

### 4.2. Training Content

* The security awareness and training program will cover the following topics, at a minimum:
  + Password security.
  + Phishing and social engineering.
  + Malware prevention.
  + Data security and handling.
  + Acceptable use of company resources.
  + Incident reporting.
  + Physical security.
  + Remote work security.
  + Relevant company policies (e.g., Acceptable Use Policy, Data Classification & Handling Policy).

### 4.3. Responsibilities

* **Management:** Is responsible for providing resources and support for the security awareness and training program.
* **[Office Manager/Designated Person]:** Is responsible for developing, implementing, and maintaining the training program.
* **IT Support (Internal or External):** May assist with the technical aspects of training delivery and content development.
* **All Personnel:** Are responsible for completing required security awareness training and applying the knowledge and skills learned to their daily work.

### 4.4. Training Records

* [Company Name] will maintain records of all security awareness training completed by personnel.
* These records will be used to track compliance with this policy.

### 4.5. Program Evaluation

* The security awareness and training program will be evaluated regularly to ensure its effectiveness.
* Feedback from personnel will be collected and used to improve the program.
* Metrics, such as phishing simulation click rates, may be used to assess the program's impact.

## 5. Compliance

Failure to complete required security awareness training may result in disciplinary action.

## 6. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description of Change |
| 1.0 | March 11, 2025 | Shijie Yin | Initial Policy Creation |