**Introduction**

[Company Name] takes the security of our data and information systems very seriously. This Security Awareness Training Policy outlines the mandatory training program designed to equip all employees with the knowledge and skills necessary to identify and mitigate security risks.

**2. Policy Objectives**

The primary objectives of this policy are:

* To raise awareness among employees regarding cyber threats and vulnerabilities.
* To educate employees on best practices for protecting company data and systems.
* To ensure employees understand their roles and responsibilities in maintaining a secure work environment.
* To promote a culture of security within the company.

**3. Training Requirements**

* All employees, including temporary and contract workers, are required to complete the mandatory Security Awareness Training program.
* New hires must complete the training program within **[Number]** days of their start date.
* Existing employees will complete the training program **annually**.
* Additional training may be required for employees with specific roles or access to sensitive information.

**4. Training Content**

The Security Awareness Training program will cover a variety of topics, including:

* **Cybersecurity threats and vulnerabilities:** This includes an overview of common threats such as phishing attacks, malware, social engineering, and data breaches.
* **Password security:** Creating strong passwords, password hygiene best practices, and avoiding password reuse.
* **Physical security:** Protecting company assets, data on portable devices, and proper disposal of sensitive information.
* **Email and internet security:** Recognizing phishing attempts, avoiding suspicious attachments and links, and safe browsing practices.
* **Reporting security incidents:** Knowing how to report suspicious activity, potential breaches, and security concerns.
* **Data security:** Understanding company policies for handling sensitive information, data classification, and avoiding data loss.

**5. Training Delivery**

The Security Awareness Training program will be delivered through a variety of methods, including:

* **Online modules:** Interactive eLearning courses that employees can complete at their own pace.
* **In-person workshops:** Interactive sessions conducted by the IT department or a security professional.
* **Security awareness videos:** Short, informative videos covering specific topics.
* **Phishing simulations:** Simulated phishing emails designed to test employee awareness and response.

**6. Enforcement**

* Failure to complete the mandatory Security Awareness Training program may result in disciplinary action, up to and including denial of access to company systems.

**7. Review**

This Security Awareness Training Policy will be reviewed and updated periodically to reflect any changes in technology, security best practices, or regulatory requirements.

**8. Questions and Support**

* If you have any questions regarding this Security Awareness Training Policy, please contact the IT Helpdesk at [Phone Number] or [Email Address].

**By signing below, you acknowledge that you have read and understood this Security Awareness Training Policy and agree to comply with its provisions.**

**Employee Name (Print):** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Employee Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_