Document Name: [COMPANY] Training and Awareness Policy
Last Revision: [INSERT]
Next Revision: [INSERT]
Document Owner: [INSERT TEAM(S)]

[COMPANY] Training and Awareness Policy

Version 1.0

CONFIDENTIAL

CONFIDENTIAL

Table of Contents

Introduction

At [COMPANY], we recognize that our employees are the first line of defense in protecting sensitive information and maintaining the security of our operations. This Employee Training and Awareness Policy outlines our commitment to providing employees with the necessary training to understand security risks, follow best practices, and respond appropriately to potential threats.

Our goal is to build a culture of security awareness across the organization, empowering employees to contribute to the overall security of the business.

Objectives

The purpose of this policy is to:

- Ensure all employees understand their role in maintaining information security.
- Provide regular training on key security practices, including data protection, incident response, and recognizing threats.
- Keep employees informed of the latest security risks and how to mitigate them.
- Ensure compliance with industry regulations and security standards.
- Promote a proactive approach to identifying and reporting security issues.

Scope

This policy applies to:

- All employees, contractors, vendors, and third parties who have access to [COMPANY] systems or data.
- All departments and business functions, regardless of location.

The policy covers security awareness training related to information protection, cybersecurity, physical security, and data privacy.

Training Requirements

At [COMPANY], we provide the following mandatory training programs for all employees:

- **Initial Security Training:** All new employees must complete security training within their first 30 days of employment. This training covers:
    - Basic cybersecurity principles.
    - Company security policies (e.g., acceptable use, password management).

    - How to recognize and respond to common threats (e.g., phishing emails, malware).
    - Incident reporting procedures.
- **Role-Specific Training:** Employees in specific roles (e.g., IT, finance, HR) may be required to complete additional training tailored to their responsibilities. This includes handling sensitive data, managing access controls, or administering security systems.
- **Compliance Training:** Employees must complete any required training related to industry regulations (e.g., GDPR, HIPAA), ensuring we comply with legal standards for data protection.

Security Awareness Program

Our Security Awareness Program is designed to reinforce key security principles on an ongoing basis. The program includes:

- **Phishing Simulations:** Regularly scheduled phishing tests are sent to employees to help them recognize phishing attempts and avoid falling victim to cyberattacks. Employees who click on simulated phishing links may be required to undergo additional training.
- **Security Tips and Reminders:** We send periodic security tips via email or internal messaging platforms to remind employees of best practices and alert them to emerging threats.
- **Workshops and Webinars:** Employees are encouraged to attend security workshops and webinars hosted by internal or external experts to deepen their understanding of current security trends and threats.

Ongoing Training and Updates

Security is an evolving field, and at [COMPANY], we commit to keeping employees updated on new risks and practices. To ensure continuous learning, we provide:

- **Annual Refresher Training:** All employees must complete a mandatory annual security refresher course that reviews key security policies and introduces any updates to our security practices.
- **Ad-Hoc Training:** In response to emerging threats or significant security incidents, we may roll out additional training sessions to address specific vulnerabilities or attack vectors.
- **Security Incident Lessons:** When a security incident occurs, a follow-up training session may be conducted to ensure that employees understand what happened, how it was addressed, and how to prevent future incidents.

Employee Responsibilities

All employees are expected to actively participate in security training and to follow security best practices in their day-to-day work. Employees must:

- **Complete Required Training:** Participate in and complete all assigned security training courses and modules within the designated time frames.
- **Report Security Threats:** Immediately report any suspicious activity, potential security breaches, or vulnerabilities to the IT or security team.
- **Follow Security Policies:** Annually acknowledge and abide by all company security policies, including the Acceptable Use Policy, Password Management Policy, and Information Security Policy.
- **Maintain Vigilance:** Stay alert to potential security threats and apply what they've learned in training to protect the company's systems, data, and assets.

Monitoring and Compliance

To ensure that training and awareness programs are effective, [COMPANY] monitors employee participation and compliance with this policy.

- **Training Records:** We track and maintain records of all completed training sessions to ensure compliance with internal policies and external regulations.
- **Performance Metrics:** We measure the effectiveness of the Security Awareness Program through performance metrics such as phishing test results, incident reports, and employee feedback.
- **Consequences of Non-Compliance:** Employees who fail to complete required training or demonstrate repeated violations of security practices may face disciplinary actions, including loss of access to company systems, warnings, or termination.

Appendix A: Revision History

This is a controlled document. This section highlights major and minor changes to the document as it is revised.

Revision	Date	Description	Approved by
1.0		Initial Version	