# ISO 27001 Information Security and Awareness Training Policy Template

## Introduction:

This policy outlines the approach for Information Security and Awareness Training at [COMPANY NAME] in alignment with ISO 27001 requirements. It ensures that all personnel are equipped with the knowledge and skills necessary to protect information assets, comply with policies, and respond effectively to security threats.

## 1. Purpose of the Training Policy

The purpose of this policy is to:  
1. Foster a security-conscious culture across the organization.  
2. Equip employees, contractors, and third parties with the knowledge to safeguard information assets.  
3. Ensure compliance with ISO 27001 requirements and other regulatory or contractual obligations.  
4. Reduce risks associated with human error by improving awareness of security policies, threats, and responsibilities.  
5. Continuously adapt training content to address evolving risks and industry best practices.

## 2. Scope

This policy applies to:  
1. All employees, contractors, and third-party personnel who handle, access, or manage information assets.  
2. All information assets, systems, and processes managed by or on behalf of [COMPANY NAME].

## 3. Training Requirements

### 3.1 Initial Training

- New Employee Onboarding: All new hires must complete mandatory security awareness training within their first [Insert timeframe, e.g., 30 days] of employment.  
- Contractor and Third-Party Orientation: Contractors and third-party personnel must complete training before gaining access to company systems or information assets.

### 3.2 Regular Training

- Annual Refresher Training: All personnel must complete annual security awareness training, focusing on updates to policies, emerging threats, and lessons learned from incidents.  
- Role-Specific Training: Personnel in high-risk roles (e.g., IT administrators, data handlers) must receive additional, specialized training.

### 3.3 Just-in-Time Training

Training will be delivered when significant changes occur, such as:  
- Policy updates.  
- Introduction of new systems or technologies.  
- Identification of new threats or vulnerabilities.

## 4. Training Content

* Information Security Policies: Overview of the organization’s policies and standards.
* Data Handling and Classification: Guidelines for managing confidential, sensitive, and public data.
* Password Management: Best practices for creating and managing strong passwords.
* Phishing and Social Engineering: Techniques to recognize and report phishing attempts and scams.
* Incident Reporting: Steps for reporting suspected security breaches or incidents.
* Physical Security: Protecting physical assets such as workstations and mobile devices.
* Regulatory Compliance: Awareness of laws and regulations (e.g., GDPR, HIPAA) relevant to the organization.

## 5. Delivery Methods

* E-Learning Platforms: Interactive, self-paced courses.
* In-Person Sessions: Workshops and seminars conducted by internal or external trainers.
* Simulated Exercises: Phishing simulations and other hands-on activities to test awareness.
* Documentation: Manuals, guides, and FAQs accessible through the company’s intranet.

## 6. Training Matrix

The table below maps roles to their required training:

| Role | Mandatory Training Topics | Frequency | Additional Requirements |
| --- | --- | --- | --- |

## 7. Monitoring and Evaluation

- Attendance Tracking: Participation in training sessions will be recorded and monitored to ensure compliance.

- Knowledge Assessments: Quizzes and tests will measure understanding and retention of training content.

- Feedback Mechanisms: Post-training surveys will gather feedback to improve future training programs.

- Metrics for Effectiveness:  
 - Percentage of personnel completing mandatory training on time.  
 - Number of incidents attributed to human error.  
 - Success rate in phishing simulations.

## 8. Roles and Responsibilities

Human Resources (HR): Coordinate onboarding training for new hires and maintain attendance records.

Information Security Manager (ISM): Develop and update training content, monitor effectiveness, and ensure compliance.

Department Managers: Ensure team members complete assigned training and recommend role-specific needs.

All Employees and Contractors: Attend mandatory training and adhere to information security policies.

## 9. Revision and Maintenance

This policy will be reviewed and updated [Insert frequency, e.g., annually or as needed] to ensure alignment with organizational priorities, regulatory requirements, and evolving threats.

## 10. Approval

| Name | Title | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |