SynrgiseLearn

Awareness and Training Plan

Document Reference	**[Insert Reference]**
Version	1.0
Effective Date	January 03, 2025
Prepared By	Xenothan Hojem
Confidentiality Level	Confidential

Document Control Information

Version History	**Date**	**Author**	**Change Description**
Version 1.0	January 03, 2025	Xenothan Hojem	Initial Document

Organization Information:

Department	**Contact Information**
Training	chris@synrgise.com

Table of Contents

1. Objective 3
2. Target Audience 3
3. Training Modules 4
4. Delivery Methods 4
5. Training Schedule 5
6. Survey and Feedback 5
7. Validity Management of Documents 5
8. Performance Metrics 6

1. Objective

The objective of this training plan is to ensure that all employees are aware of their roles and responsibilities in maintaining security standards and to foster a security-conscious culture. This plan supports compliance with ISO 27001 by providing targeted, role-based training and regular awareness initiatives to mitigate human-related security risks.

2. Target Audience

Employee Group	Training Type	Frequency
All Staff	General Security Awareness	Annually
IT Department	Advanced Security Practices	Quarterly
Managers/Supervisors	Role-Based Security Management	Bi-Annually
New Employees	Introduction to Security Policies	Upon Onboarding
Third-Party Vendors	Security Compliance Overview	Annually

3. Training Modules

Module	Description	Target Group	Delivery Method
Types of Security Threats	Overview of common threats	All Staff	Online/Webinar
Social Engineering	Identifying and mitigating social engineering	All Staff	Online/In-Person
Identity Theft	Preventing and responding to identity theft	All Staff	Online/Webinar
Data Classification	Handling sensitive data securely	Managers, IT	Online/In-Person
Incident Response and Reporting	Steps for handling security incidents	IT, Managers	Online/Webinar
Cloud Security Awareness	Best practices for cloud-based resources	IT, All Staff	Online
Mobile Device Security	Securing mobile devices in workplace settings	All Staff	Online/Webinar
Data Privacy and GDPR Compliance	Handling personal data securely	All Staff	Online/Webinar

4. Delivery Methods

Method	Description
Online Training	Conducted via LMS platform, self-paced
In-Person	Instructor-led sessions in designated locations
Webinars	Monthly interactive security webinars
Simulated Phishing	Regular phishing attack simulations
Gamified Challenges	Security awareness competitions and incentives
Posters/Emails	Visual reminders and updates

5. Training Schedule

Date	Session	Duration	Trainer	Compliance Target
25/02/2025	General Security Awareness	2 hours	Security Team	Pre-Audit (Q1)
17/03/2025	Phishing Simulation Workshop	1.5 hours	CyberSec Expert	Quarterly
17/03/2025	New Employee Security Training	2 hours	HR Department	Onboarding
01/06/2025	Advanced Security Practices	3 hours	IT Security Lead	Quarterly

6. Survey and Feedback

- **Knowledge Checks:** Employees will take tests to measure their knowledge of the subject after each training session.
- **Feedback Forms:** Attendees will be asked to rate the training's efficacy and provide areas for improvement.
- **Performance Metrics:** The security team will monitor evaluation results and participation rates to adjust future training.

7. Validity Management of Documents

The validity of this document is 01/01/2025 The training plan must be updated and maintained by the Security Officer, at least once a year or whenever there are major modifications.

8. Performance Metrics

To ensure the effectiveness of the training plan, the following key performance indicators (KPIs) will be tracked:

- **Participation Rate:** Target 90%+ completion of all training modules.
- **Phishing Test Success Rate:** Reduce failure rates progressively.
- **Assessment Scores:** Ensure 80%+ passing rate on post-training tests.
- **Employee Feedback:** Maintain an average satisfaction score of 4/5.