<Logo>

<Organization Name>

**Awareness & Training Program**

|  |  |
| --- | --- |
| **Standard** | ISO/IEC 27001:2022 |
| **Version** | <Version> |
| **Document Owner** | <Name of CISO/IT Security Lead> |
| **Approved by** | <Name of Approval Authority/Board> |
| **Date Approved** | <Approval Date> |
| **Next Review Date** | <Review Date (typically a year from the approval date)> |
| **Document Classification** | Confidential/Public/Internal Use Only |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision History** | | | | |
| **Version** | **Date** | **Prepared By** | **Approved By** | **Changes/Notes** |
| <version No> | <DD/MM/YYYY> | <Name> | <Name> | *Initial Version* |

|  |  |  |
| --- | --- | --- |
| **Distribution List** | | |
| **Recipient Name** | **Department** | **Distribution Date** |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |

**Table of Contents**

[Purpose 1](#_Toc179804390)

[Scope 1](#_Toc179804391)

[Objectives 1](#_Toc179804392)

[Roles and Responsibilities 2](#_Toc179804393)

[Training Content 3](#_Toc179804394)

[Training Methods 4](#_Toc179804395)

[Frequency 4](#_Toc179804396)

[Training and Awareness Plan 5](#_Toc179804397)

[Record Keeping and Compliance 6](#_Toc179804398)

[Measurement and Reporting 6](#_Toc179804399)

[Compliance with ISO 27001:2022 7](#_Toc179804400)

[Continuous Improvement 7](#_Toc179804401)

# Purpose

To raise awareness and provide training to employees about security policies, procedures, and best practices to ensure the protection of organizational assets and compliance with ISO 27001:2022.

# Scope

This program applies to all employees, contractors, and third parties with access to the organization’s information systems.

# Objectives

* Educate employees on security policies and procedures.
* Ensure compliance with ISO 27001:2022 requirements.
* Promote a culture of security awareness within the organization.
* Reduce the risk of security incidents by increasing staff awareness and understanding of threats and vulnerabilities.

# Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| CISO/IT Security Lead | Oversees the security awareness program, including development and delivery. |
| HR Department | Coordinates with IT to track employee training and completion. |
| Department Managers | Ensure staff participation and adherence to the security awareness program. |
| Employees | Participate in the training program and apply security best practices. |
| <Role> | <Responsibility> |
| <Role> | <Responsibility> |

# Training Content

|  |  |
| --- | --- |
| **Training Module** | **Description** |
| Introduction to Information Security | Overview of ISO 27001:2022 requirements and importance of information security. |
| Security Policies and Procedures | Review of key security policies (access control, password management, incident reporting). |
| Recognizing Threats | Identifying phishing, social engineering, malware, and ransomware. Safe browsing practices. |
| Secure Data Handling | Handling sensitive data (confidential, personal, financial). Data classification and labeling. |
| Physical Security | Best practices for securing physical devices and workspaces. Visitor and office security. |
| Password Management | Best practices for creating strong passwords. Importance of multi-factor authentication. |
| Incident Reporting | How to identify and report security incidents and breaches. |
| Access Control and Remote Work | Secure access protocols, VPN usage, and remote work security practices. |
| <Training Module> | <Description> |
| <Training Module> | <Description> |

# Training Methods

|  |  |
| --- | --- |
| **Method** | **Description** |
| Instructor-Led Training | On-site or virtual training sessions led by IT Security staff or external trainers. |
| Online Learning Modules | Interactive, self-paced courses covering essential topics. |
| Workshops | Scenario-based workshops focused on real-world security threats. |
| Email Newsletters | Periodic security tips and updates sent via email. |
| Quizzes and Assessments | Post-training assessments to evaluate understanding of the topics. |
| <Training Method> | <Description> |
| <Training Method > | <Description> |

# Frequency

|  |  |
| --- | --- |
| **Training Type** | **Frequency** |
| Initial Training | All new employees must complete training within the first month of employment. |
| Annual Refresher | All employees must undergo an annual refresher on security policies and threats. |
| Ad-Hoc Training | Additional training provided in response to incidents or policy changes. |
| <Training Type> | <Frequency> |
| <Training Type> | <Frequency> |

# Training and Awareness Plan

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Job Title** | **Trained By** | **Date** | **Time Period** | **What was Trained** | **Achieved Knowledge/ Skills/ Experience** |
| *IT Security Analyst* | *CISO* | *01/03/2024* | *2 hours* | *Incident response, phishing detection, password policies* | *Improved incident response skills, phishing prevention* |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Record Keeping and Compliance

|  |  |  |  |
| --- | --- | --- | --- |
| **Document/Record** | **Responsible Party** | **Frequency** | **Retention Period** |
| Training Attendance Sheets | HR Department | After each session | 3 years |
| Training Materials | IT Security Team | Yearly review | 2 years |
| Quiz/Assessment Results | IT Security Team | After each session | 2 years |
| Employee Acknowledgement Forms | HR Department | Upon completion | 3 years |
| <Document/Record> | <Title/ Department> | <Frequency> | <Time in Years> |
| <Document/Record> | <Title/ Department> | <Frequency> | <Time in Years> |

# Measurement and Reporting

|  |  |
| --- | --- |
| **Metric** | **Description** |
| Completion Rate | Monitor and report the percentage of employees completing the training. |
| Assessment Scores | Review quiz and assessment results to identify areas for further training. |
| Feedback Mechanism | Gather employee feedback to improve future training sessions. |
| Reporting | Summary of training completion and assessments presented quarterly to management. |
| <Metric> | <Description> |
| <Metric> | <Description> |

# Compliance with ISO 27001:2022

**Clause 7.2.2 Competence and Awareness**

Ensure employees are competent in information security practices.

**Clause 8.1 Operational Planning and Control**

Monitor the effectiveness of the security awareness program.

**Annex A.7.2 Information Security Awareness, Education, and Training**

Ensure employees, contractors, and third parties receive appropriate security training.

# Continuous Improvement

**Review and Update**

The awareness program should be reviewed annually or after major security incidents. Improvements based on feedback, new threats, or regulatory changes should be incorporated.

**Appendix**

*Add the following appendix for the document.*

|  |  |
| --- | --- |
| **Appendix** | **Description** |
| Training Calendar | Yearly calendar outlining scheduled training events. |
| Sample Training Slides | Preview of topics covered in training sessions. |
| Employee Acknowledgement Form | Template for employees to acknowledge completion of training. |
| Quiz Template | Sample quiz to assess knowledge on security awareness topics. |

***Note:*** *The content and schedule in this template can be customized based on organizational needs, policies, and evolving threats.*