Security Awareness Policy

Building Risk-Aware Culture

SA

Secured approach  www.securedapproach.com

Use Disclaimer: This policy has been developed by Secured Approach Inc. for the benefit of the community. You are welcome to use this policy, in whole or in part, for your organization without the need for prior approval. Should you wish to contribute to creating or updating a new version of this policy, please reach out to us via email at resources@securedapproach.com.
Furthermore, if you require assistance in crafting a tailored security policy for your specific environment, do not hesitate to contact us at support@securedapproach.com.

Table of Contents

[Confidentiality Statement 2](#_Toc159342225)

[Disclaimer 2](#_Toc159342226)

[1. Overview 2](#_Toc159342227)

[2. Purpose 2](#_Toc159342228)

[3. Scope 2](#_Toc159342229)

[4. Policy 2](#_Toc159342230)

[4.1 Mandatory Training 2](#_Toc159342231)

[4.2 Continuous Learning 3](#_Toc159342232)

[5. Policy Compliance 3](#_Toc159342233)

[5.1 Compliance Measurement 3](#_Toc159342234)

[5.2 Exceptions 3](#_Toc159342235)

[5.3 Non-Compliance 3](#_Toc159342236)

[6. Related Standards, Policies, and Processes 3](#_Toc159342237)

[7. Revision History 4](#_Toc159342238)

# Confidentiality Statement

This document is confidential and intended solely for the internal use of [Organization Name]'s employees and authorized individuals. Unauthorized distribution, copying, or disclosure of this document, or any information contained herein, is strictly prohibited and may lead to disciplinary actions.

# Disclaimer

This Security Awareness Policy is subject to revisions and updates to adapt to evolving cybersecurity threats, regulatory requirements, and industry best practices. It is the responsibility of all employees and stakeholders to stay informed of these changes.

# Overview

The Security Awareness Policy outlines [Organization Name]'s commitment to ensuring that all employees and contractors are informed, vigilant, and equipped with the knowledge to protect the organization’s information assets against cyber threats.

# Purpose

To establish a comprehensive security awareness training program aimed at reducing risk and enhancing the security posture of [Organization Name] by educating its workforce on cybersecurity principles, practices, and response strategies.

# Scope

This policy applies to all employees, contractors, and third-party service providers of [Organization Name] with access to organizational information systems and data.

# Policy

## Mandatory Training

* All users must complete the mandatory security awareness training upon induction and participate in annual refresher courses.
* Users will be included in periodic phishing simulation campaigns to assess and enhance their ability to identify and respond to phishing attempts.
* The training program will cover topics such as password security, data protection, recognizing and reporting potential security threats, and understanding the legal and regulatory obligations regarding information security.

## Continuous Learning

* Users are encouraged to engage in continuous learning and stay informed about emerging cybersecurity threats and trends through newsletters, webinars, and other resources provided by [Organization Name].

# Policy Compliance

## Compliance Measurement

The effectiveness of the Security Awareness Policy will be measured through training completion rates, phishing campaign results, and the frequency and severity of security incidents.

## Exceptions

Any exceptions to this policy must be submitted in writing with a business justification and approved by the IT Security Department or relevant authority within the organization.

## Non-Compliance

Violations of this policy may result in disciplinary action, up to and including termination of access, employment, legal action, and financial liabilities.

# Related Standards, Policies, and Processes

* Acceptable Use Policy
* Identity and Access Management Policy
* Remote Access Policy
* Data Protection Policy
* Data Backup Policy

# Revision History

This policy will be reviewed and updated annually or as needed to reflect changes in technology, legal requirements, and organizational priorities. The revision history will be documented here, including the date of the revision, a brief description of the changes, and the version number.

|  |  |  |  |
| --- | --- | --- | --- |
| Date of Change | Responsible | Summary of Change | Version |
| January 2024 | Information Security Manager | Building the first draft | 1.0 |
| January 2024 |  |  |  |
|  |  |  |  |