Company Name

Social Engineering Awareness Policy

Month – 2022

Table of Contents

Document Control

Type of Information	Document Data
Title	ASSIGNED Policy
Version	<Document Number>
Issue Date	<Year>
Document Owner	<COMPANY>
Document Creator	<Name>

Revision History

Version	Date	Author	Summary of Changes
1.0	1 Mar 2022	<Name>, <Designation>	First document

Document Approver

Version	Approval Date	Approving Authority	Signature
1.0	1 April 2022	<Designation>	

Social Engineering Awareness Policy

Overview

Social engineering is a common attack method used by cyber criminals to coerce employees into disclosing sensitive information to authorized individuals. It can happen over the phone, on social media, or even in person. As a result, this policy applies to COMPANY employees, stakeholders, or anyone involved in the use of COMPANY assets. All employees must protect the integrity and confidentiality of COMPANY resources to protect COMPANY assets.

Purpose

The primary purpose of this policy to make staff aware of social engineering attacks and to provide a method for responding when they are approached through phone call, social media, email, fax, or being socially pressured into revealing sensitive information.

The following are the important points.

- Made them aware of the strategies employed in social engineering attacks and provided them with a response process.
- They are aware of who to notify in the event of an attack.

Scope

This policy applies to all employees, managers, stakeholders, vendors, and anyone else who has access to COMPANY resources.

Policy

Do not disclose sensitive COMPANY information to an unknown/unauthorized individual if he or she uses the words, phrases, or techniques listed below:

- An important concern
- A lost password