[INSERT FIRM LEGAL NAME]
Social Engineering Awareness Policy

[Insert Firm Logo]

Version 1.0
[Insert Date]

[Insert Firm Logo]

Contents

Instructions

Documents are in a template format and are to be customized to fit the appropriate business and operational requirements. Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company specific document. Otherwise, it would be a liability exposure to establish a policy and not to comply with it.

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

Delete the instructions after finalizing and adopting the policy.

Policy Overview

The Social Engineering Awareness Policy bundle is a collection of policies and guidelines for employees of **[Insert Firm Legal Name]**.

In order to protect **[Insert Firm Legal Name]**'s assets, all employees need to defend the integrity and confidentiality of **[Insert Firm Legal Name]**'s resources.

Scope and Purpose

This policy has two purposes:

To make employees aware that (a) fraudulent social engineering attacks occur, and (b) there are procedures that employees can use to detect attacks.

- Employees are made aware of techniques used for such attacks, and they are given standard procedures to respond to attacks.
- Employees know who to contact in these circumstances.
- Employees recognize they are an important part of **[Insert Firm Legal Name]**'s security. The integrity of an employee is the best line of defense for protecting sensitive information regarding **[Insert Firm Legal Name]**'s resources.

To create specific procedures for employees to follow to help them make the best choice when:

- Someone is contacting the employee - via phone, in person, email, fax or online - and elusively trying to collect **[Insert Firm Legal Name]**'s sensitive information.
- The employee is being "socially pressured" or "socially encouraged or tricked" into sharing sensitive data.

This policy applies to all employees of **[Insert Firm Legal Name]**, including temporary contractors or part-time employees participating with help desk customer service.

Policy

Sensitive information of **[Insert Firm Legal Name]** will not be shared with an unauthorized individual if he/she uses words and/ or techniques such as the following:

- An "urgent matter"
- A "forgotten password"
- A "computer virus emergency"
- Any form of intimidation from "higher level management"
- Any "name dropping" by the individual which gives the appearance that it is coming from legitimate and authorized personnel.
- The requester requires release of information that will reveal passwords, model, serial number, or brand or quantity of **[Insert Firm Legal Name]** resources.
- The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person.
- The techniques are used by a person that declares to be "affiliated" with **[Insert Firm Legal Name]** such as a sub-contractor.
- The techniques are used by an individual that says he/she is a reporter for a well-known press editor or TV or radio company.
- The requester is using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger).

All persons in which this policy applies to MUST attend the security awareness training within 30 days from the date of employment and every 6 months thereafter.

- If one or more circumstances described in this section is detected by a person, then the identity of the requester MUST be verified before continuing the conversation or replying to email, fax, or online.
- If the identity of the requester CANNOT be promptly verified, the person MUST immediately contact his/her supervisor or direct manager.
- If the supervisor or manager is not available, that person MUST contact the security personnel.
- If the security personnel is not available, [identify person] MUST immediately drop the conversation, email, online chat with the requester, and report the episode to his/her supervisor before the end of the business day.

Compliance

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Exceptions

Any exception to the policy must be approved by Remote Access Services and the Infosec Team in advance.

Revision Table

Revision History				
#	**Version #**	**Date**	**Updates/Changes**	**Owner**
1	1.0	September 2022	Initial Draft	Riskigy
2				