1. Overview

The Social Engineering Awareness Policy bundle is a collection of policies and guidelines for employees of KVI. This employee front desk communication policy is part of the Social Engineering Awareness Policy bundle.

To protect Kinyo assets, all employees need to defend the integrity and confidentiality of Kinyo resources.

2. Purpose

The policy has two purposes.

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

2.1.0 Employees are made aware of techniques used for such attacks, and they are given standard procedures to respond to attacks.

2.1.1 Employees know who to contact in these circumstances.

2.1.2 Employees recognize they are an important part of Kinyo security. The integrity of an employee is the best line of defense for protecting sensitive information regarding Kinyo resources.

2.2 To create a specific procedure for employees to follow to help them make the best choice when:

2.2.0 Someone is contacting the employee – via phone, in person, email, fax or online – and elusively trying to collect Kinyo sensitive information.

2.2.1 The employee is being “socially pressured” or “socially encouraged or tricked” into sharing sensitive data information.

3. Scope

Includes all employees of Kinyo, including temporary contractors or part-time employees participating with help desk customer service.

4. Policy

4.1 Sensitive information of KVI will not be shared with an unauthorized individual if the employee uses words and/or techniques such as the following:

4.1.1 An “urgent matter”

4.1.2 A “forgotten password”.

4.1.3 A “computer virus emergency”.

4.1.4 Any form of intimidation from “higher level management”.

4.1.5 Any “name dropping” by the individual which gives the appearance that it is coming from legitimate and authorized personnel.

4.1.6 The requester requires release of information that will reveal passwords, model, serial number, or brand or quantity of Kinyo resources.

4.1.7 The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person.

4.1.8 The techniques are used by a person that declares to be “affiliated” with Kinyo such as a sub-contractor.

4.1.9 The techniques are used by an individual that says there a reporter for a well-known press editor or TV or radio company (only the Human Resource and General Affairs Manager has the authority).

4.1.10 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).

4.2 Action:

4.2.1 All persons described in section 3.0 (employees, or part-time employees, contractors, and sub-contractors) must attend the security awareness training within 30 days from the date of employment and every year thereafter.

4.2.2 If one or more circumstances described in section 4.0 is detected by a person described in section 3.0, then the identity of the requester must be verified before continuing the conversation or replying to email, fax, or online.

4.2.3 If the identity of the requester describes in section 4.1. cannot be promptly verified, the person must immediately contact their supervisor or direct manager.

4.2.4 If the supervisor or manager is not available, that person described in section 3.0 (employees, or part-time employees, contractors, and sub-contractors) must immediately drop the conversation, email, online chat with the requester, and report the episode to their supervisor before the end of business day.

5. Policy Compliance

5.1 Compliance Measurement

The I.T. department team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the I.T. department.

5.2 Exceptions:

Any exception to the policy must be approved by the I.T. department in advance.