Security Awareness Training Procedure

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX..

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Procedure Statements 4

2.1 Roles and Responsibilities 4

3. Steps on Security Awareness and Training Procedures 4

4. Procedure Compliance & Enforcement 5

4.1 Compliance Measures 5

4.2 Enforcement 5

5. Glossary / Acronyms 6

5.1 Glossary / Acronyms 6

6. Document Management 7

6.1 Document Revision Log 7

6.2 Document Ownership 7

6.3 Document Coordinator 7

6.4 Document Approvers 7

6.5 Distribution 7

# Introduction

## Document Definition

This document is a Procedure.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Objective

The scope of this procedure covers what an organization should do to design, develop, implement, and maintain an IT security awareness and training procedure, as a part of the IT security program. This document covers awareness and training needs of all users of an organization’s IT, from employees to supervisors and functional managers, to executive-level managers

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This procedure applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant procedure statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This procedure applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program
* NIST Special Publication 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model

# Procedure Statements

## Roles and Responsibilities

|  |  |
| --- | --- |
| Roles | Responsibilities |
| Management— all levels including team leaders, program managers, system managers, and organization leaders | • To determine staff training needs • To prioritize use of training resources • To evaluate training effectiveness |
| Information Security Officer | • To identify training courses and training aids that meet established requirements  • To identify training gaps and needs in the organization's IT security program  • To determine the amount of course customization needed  • To develop a compliance baseline for the organization |
| Training Professionals   • Career Planners/Human Resource Personnel  • Training Coordinators/Curriculum Developers  • Course Developers  • Trainers | • To gain an understanding of IT security requirements and the knowledges, skills, and abilities needed to meet those requirements  • To evaluate course quality  • To assist in obtaining appropriate courses and materials  • To develop or customize courses/materials  • To tailor their teaching approach to achieve the desired behavioural outcomes |
| Every Employee | • To identify IT security training needs for their current job assignment and career path |

# Steps on Security Awareness and Training Procedures

1. Head IT/ISO to conduct Information Security training for all new hires at induction.
2. ISO to send weekly mails on information security to all staff weekly
3. Scheduled e-learning on information security to be taken by all staff quarterly.
4. Phishing tests to be carried out regularly by IT on all staff.

# Procedure Compliance & Enforcement

## Compliance Measures

Not applicable.

## Enforcement

All staff of XXXX must comply with all Information Security Procedures. Failure to comply with these procedures may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Glossary / Acronyms

## Glossary / Acronyms

|  |  |
| --- | --- |
| NIST | National Institute of Standards and Technology |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Procedure is owned by the YYYY

## Document Coordinator

This Procedure is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Distribution

* Distribution is to all staff