Security Awareness Training Standard

*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. Standard Statements 4

2.1 Roles and Responsibilities 4

2.2 Awareness, Training and Education 4

2.3 Core Set of IT Security Terms and Concept 5

3. Curriculum Framework 7

4. Evaluation 13

5. Standard Compliance & Enforcement 14

5.1 Compliance Measures 14

5.2 Enforcement 14

6. Glossary / Acronyms 15

6.1 Glossary / Acronyms 15

7. Document Management 16

7.1 Document Revision Log 16

7.2 Document Ownership 16

7.3 Document Coordinator 16

7.4 Document Approvers 16

7.5 Distribution 16

# Introduction

## Document Definition

This document is a Standard.

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

## Objective

The scope of this standard 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

# Standard 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 |

## Awareness, Training and Education

|  |  |  |  |
| --- | --- | --- | --- |
| Comparative Framework | | | |
|  | AWARENESS | TRAINING | EDUCATION |
| Attribute: | "What" | "How" | "Why" |
| Level: | Information | Knowledge | Insight |
| Learning Objective: | Recognition and Retention | Skill | Understanding |
| Example Teaching Method: | Media  -Videos -Newsletters -Posters | Practical Instruction -Lecture and/or demo -Case Study -Hands-on Practice | Theoretical Instruction -Seminar and discussion -Reading and Study -Research |
| **Test Measure:** | True/False Multiple Choice  (identify learning) | Problem Solving, i.e., Recognition and Resolution  (apply learning) | Essay   (interpret learning) |
| **Impact Timeframe:** | Short-term | Intermediate | Long-term |

## Core Set of IT Security Terms and Concept

Certain basic concepts form the foundation of any effective IT security program and environment,

These terms and concepts must be learned and applied as the individual proceeds from security

awareness to training and then to education.

The core set of IT security terms and concepts is presented below as the "ABC's of

Information Technology Security," 26 items related to the alphabet, as summarized below

This memory tool approach aids the learning process while communicating fundamental IT security concepts. It is anticipated that course material developed under this model will build on the memory tool approach to learning.

|  |  |
| --- | --- |
| **ABC's OF INFORMATION SECURITY** | |
| **A** | Assets - Something of value requiring protection (hardware, software, data, reputation) |
| **B** | Backup - The three most important safeguards - backup, backup, backup |
| **C** | Countermeasures and Controls - Prevent, detect, and recover from security incidents |
| **D** | Designated Representatives of Executive Management - Manage and accept risk and authorize the system to operate |
| **E** | Ethics - The body of rules that governs an individual's behaviours. |
| **F** | Firewalls and Separation of Duties - Minimize the potential for "incident encroachment" |
| **G** | Goals - Confidentiality, Integrity, and Availability (CIA) |
| **H** | Hackers/Crackers - Intruders who are threats to any system |
| **I** | Individual Accountability/Responsibility - Individuals responsible for their own actions |
| **J** | Job Description/Job Function - Defines the individual's roles within the organization |
| **K** | Keys to Incident Prevention - Awareness, compliance, common sense |
| **L** | Laws and Regulations - Establish basic control/security objectives |
| **M** | Model Framework - Relates training needs to roles and responsibilities |
| **N** | Need to Know - Limits access to data, sets objective for ongoing learning |
| **O** | Ownership - Establishes responsibility/accountability for asset protection |
| **P** | Policies and Procedures - What to accomplish and how to accomplish it |
| **Q** | Quality Assurance/Quality Control - Ensure the integrity of the process |
| **R** | Risk Management - Balances potential adverse impact against safeguard cost |
| **S** | Security Training - The best return on investment of any security safeguard |
| **T** | Threats - Are always present, and generally occur when least expected |
| **U** | Unique Identifiers - Provide for individual accountability and facilitate access control |
| **V** | Vulnerabilities - Security weaknesses through which threats impact the system |
| **w** | Waste, Fraud, and Abuse - The three primary impacts of a security incident |
| **X** | Expect the unexpected - Don't assume that because something hasn't happened, it won't |
| **Y** | You - Your actions/inactions are critical to maintaining an effective security environment |
| **Z** | Zoning/Compartmentalization - Establish security layers and minimize incident impact |

# Curriculum Framework

This framework shows the areas of information security awareness, training and education will be developed on to ensure it meets the needs of XXXX. He preferred method in XXXX is to encourage participation by the learners in interactive discussions on how the various concepts relate to the XXXX or individual roles. This approach allows learner to understand the significance of IT security principles and procedures to the XXXX, and to begin finding ways of applying this new knowledge in their work environment.

The following curriculum framework incorporates and expands on the basic concepts introduced in the ABC's, introduces a set of the relevant information security topics and concepts which have been identified as the foundation for security training, and provides a mechanism for learners to relate and apply the information learned on the job.

1. **Laws and Regulations**

**Subjects to include:**

• Government IT security laws, regulations, standards and guidelines

• Organization specific policies and procedures

• Role of government-wide and organization specific laws, regulations, policies,

guidelines, standards and procedures in protecting the organization's IT resources

* Tangible and intangible IT resources (assets)

• Current and emerging social issues that can affect IT assets

• Laws and regulations related to social issues affecting security issues

• Effect of social issues on accomplishment of organizations mission(s)

* Social conflicts with the Freedom of Information Act
* Public concern for protection of personal information

• Legal and liability issues

* Laws concerning copyrighted software
* Organization policies concerning copyrighted software
* Laws concerning privacy of personal information
* Organization policies concerning privacy of personal information
* Mission related laws and regulations
* Effects of laws, regulations or policies on the selection of security controls

**Includes basic IT security concepts introduced in the following ABC's:**

L - Laws and Regulations

P - Policies and Procedures

1. **The Organization and IT Security**

**Subjects to include:**

• Organization mission(s)

• How information technology supports the mission(s)

• Reliance on IT systems for mission accomplishment

• FT security programs protect against violations of laws and regulations

• Purpose and elements of organizational FT security programs.

* Difference between organization level and system level IT security programs

• Changing FT security issues and requirements

• System ownership and its importance from a user or client perspective

• Information ownership and its importance from a user or client perspective

• Identification of IT security program and system level points of contacts

**Includes basic IT security concepts introduced in the following ABC's:**

A - Assets

G - Goals

0 – Ownership

1. **System Interconnection and Information Sharing**

**Subjects to include:**

• Increased vulnerabilities of interconnected systems and shared data

• Responsibilities of system or information owner organizations if systems have external

users or clients

• Responsibility of users or clients for notifying system owners of security requirements

• Sharing information on system controls with internal and external users and clients

• Formal agreements between systems for mutual protection of shared data and resources,

* User rules of behaviour and individual accountability in interconnected systems ^
* System rules of behaviour and technical controls based on most stringent protection requirements

• Electronic mail security concerns

• Electronic commerce

* Electronic Fund Transfer
* Electronic Data Interchange
* Digital/electronic signatures

• Monitoring user activities

**Includes basic IT security concepts introduced in the following ABCs:**

A - Assets

C - Countermeasures and Controls

E - Ethics

H - Hackers/Crackers

I - Individual Accountability/Responsibility

T - Threats

V - Vulnerabilities

W- Waste, Fraud, and Abuse

X - Expect the unexpected

Y-You

1. **Sensitivity**

**Subjects to include:**

• Categorization of system sensitivity

* Criticality
* Unauthorized use
* Reliability

• Categorization of information sensitivity

Sensitive information in general

- Types of sensitive information

- Aggregation of information

Organization's sensitive information

- Need to know

- Authorized access

- Unauthorized disclosure

• IT asset protection requirements

• The organization's need for confidentiality of its information

* Adverse consequences of unauthorized information disclosure

• The organization's need for integrity of its information

Corruption of information

- Accidental

- Intentional

Adverse consequences if public or other users do not trust integrity and reliability of

information

• The organization's need for availability of its information and IT systems

* Adverse consequences of system or information unavailability
* Public dependance on information
* Internal or external user's dependence on information

**Includes basic IT security concepts introduced in the following ABC's:**

G - Goals

N - Need to Know

1. **Risk Management**

**Subjects to include:**

• Managing risk

* Threats
* Vulnerabilities
* Risk
* Relationships between threats, vulnerabilities, risks

• Threats from "authorized system users"

• Increased threats and vulnerabilities from connection to external systems and networks

* "Hacker" threats
* Malicious software programs and virus threats

• Types of security controls (safeguards, countermeasures)

* Management controls
* Acquisition/development/installation/implementation controls
* Operational controls
* Security awareness and training controls
* Technical controls

• How different categories of controls work together

• Examples of security controls for:

* Confidentiality protection
* Availability protection
* integrity protection

• Added security controls for connecting external systems and networks

• Protecting assets through IT security awareness and training programs

• Contingency-disaster recovery planning

* Importance of plan to deal with unexpected problems
* Importance of testing plan and applying lessons learned

• "Acceptable levels of risk" vs. "absolute protection from risk"

• "Adequate" and "appropriate" controls

* Unique protection requirements of IT systems and information
* Severity, probability, and extent of potential harm
* Cost effective/cost benefits
* Reduction of risk vs. elimination of risk

• Working together with other security disciplines

• Importance of internal and external audits, reviews, and evaluations in security decisions

**Includes basic IT security concepts introduced in the following ABC's:**

C - Countermeasures and Controls

R - Risk Management

S - Security Training

1. **Management Controls**

**Subjects to include:**

• System/application-specific policies and procedures

• Standard operating procedures

• Personnel security

* Background investigations/security clearances
* Roles and responsibilities
* Separation of duties
* Role-based access controls

• System rules of behaviour contribute to an effective security environment

• Organization-specific user rules

• System-specific user rules

- Assignment and limitation of system privileges

- Intellectual property/Copyright issues

- Remote access and work at home issues

- Official vs. unofficial system use

- individual accountability

- Sanctions or penalties for violations

• Individual accountability contributes to system and information quality

• Individual acceptance of responsibilities

• Signed individual accountability agreements

• IT security awareness and training

• Determining IT security training requirements for individuals

• Effect of IT security awareness and training programs on personal responsibility and

positive behavioural changes

• "Computer ethics"

• System-specific user IT security training

• User responsibilities for inappropriate actions of others

**Includes basic IT security concepts introduced in the following ABC's:**

E- Ethics

I - Individual Accountability/Responsibility

J - Job Description/Job Function

M - Model Framework

P - Policies and Procedures

S - Security Training

Y- You

1. **Acquisition/Development/Installation/Implementation Controls**

**Subjects to include:**

• System life cycle stages and functions

• IT security requirements in system life cycle stages

• Initiation stage

• Development stage

•Test and evaluation stage

•Implementation stage

•Operations stage

•Termination stage

• Formal system security plan for management of a system

* Identification of system mission, purpose and assets
* Definition of system protection needs
* Identification of responsible people
* Identification of system security controls in-place or planned and milestone dates for
* implementation of planned controls

• Relationship of configuration and change management programs to IT security goals

• Testing system security controls synergistically and certification

• Senior manager approval (accredit) an IT system for operation

**Includes basic IT security concepts introduced in the following ABC's:**

D – Designated representatives of Executive Management

G - Goals

O – Ownership

**8. Operational Controls**

**Subjects to include:**

• Physical and environmental protection

* Physical access controls
* Intrusion detection
* Fire/water/moisture/heat/electrical maintenance
* Mobile and portable systems

• Marking, handling, shipping, storing, cleaning, and clearing

• Contingency planning

* Importance of developing and testing contingency/disaster recovery plans
* Importance of users providing accurate information about processing needs, allowable

down time and applications that can wait

* Responsibility for backup copies of data files and software programs
* Simple user contingency planning steps

**Includes basic IT security concepts introduced in the following ABC's:**

B - Backup

Z - Zoning/Compartmentalization

1. **Technical Controls**

**Subjects to include:**

• How technical (role-based access) controls support management (security rules) controls

• User identification and passwords/tokens

•User role-based access privileges

• Public access controls

• How system controls can allow positive association of actions to individuals

* Audit trails
* System monitoring

• Recognizing attacks by hackers, authorized or unauthorized users

* Effects of hacker attack on authorized users
* Unauthorized use or actions by authorized users
* Reporting incidents

• User actions to prevent damage from malicious software or computer virus attacks

• Organization specific procedures for reporting virus incidents

• Technical support and help from security incident response teams

• Software products to scan, detect and remove computer viruses

• Role of cryptography in protecting information

**Includes basic IT security concepts introduced in the following ABC's:**

F - Firewalls and Separation of Duties

H - Hackers/Crackers

I - Individual Accountability/Responsibility

J - Job Description/job Function

K - Keys to Incident Prevention

Q - Quality Assurance/Quality Control

U - Unique Identifiers

V- Vulnerabilities

Z - Zoning/Compartmentalization

# Evaluation

Evaluating training effectiveness is a vital step to ensure that the training delivered is meaningful.

Training is "meaningful" only when it meets the needs of both the student (employee) and the

organization.

Four levels of evaluation, in order of complexity, are:

• Level 1 : End-of-Course Evaluations (Student Satisfaction)

• Level 2: Behaviours Objective Testing (Learning Effectiveness, which is also a measure of

Teaching Effectiveness)

• Level 3: Job Transfer Skills (Performance Effectiveness)

• Level 4: Organizational Benefit (Training Program Effectiveness)

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Training curriculum to cover the ABCs of information security | * Review presentation slides, webinars, and e-learning to ensure all areas of information security are covered |
| Sign offs and acknowledgements for training conducted | * Review samples of trainings done and confirm if participants sign and acknowledged they participated in the training |
| Evaluation of effectiveness of training | * Review participants evaluation scores on trainings. * Review if information security posture for staff have improved through incidents prevented, phishing test scores etc |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards 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 Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

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

## Distribution

* Distribution is to all staff