# Security Awareness and Training Policy Template v.1

Data Privacy Institute

# Security Awareness and Training Policy

*This document should not be considered legal advice and should not be used in the determination of compliance or adherence to CCPA or CPRA, it is information and intended to be an overview and guide for businesses to use in assisting with compliance efforts. For questions please contact Data Privacy Institute and info@dataprivacyinsitute.org.*

**www.dataprivacyinstitute.org**

# Security Awareness and Training Policy TEMPLATE

## *Purpose:*

To ensure that the appropriate level of information security awareness training is provided to all Information Technology (IT) users.

**REFERENCES:** National Institute of Standards and Technology (NIST) Special Publications: NIST SP 800-53 – Awareness and Training (AT), NIST SP 800-12, NIST SP 800-16, NIST SP 800-50, NIST SP 800-100; Electronic Code of Federal Regulations (CFR): 5 CFR 930.301

**POLICY:** *This policy is applicable to all departments and users of IT resources and assets.*

## SECURITY AWARENESS TRAINING

________________________ Manager shall:

- Schedule security awareness training as part of initial training for new users.
- Schedule security awareness training when required by information system changes and then annually thereafter.

________________________ IT Manager shall:

- Determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:
    - *Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.*
    - *Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.*

## ROLE-BASED SECURITY TRAINING

*IT Department shall:*

- Provide role-based security training to personnel with assigned security roles and responsibilities:
- Before authorizing access to the information system or performing assigned duties.
- When required by information system changes and annually thereafter.

## PHYSICAL SECURITY CONTROLS

*IT Department shall:*

- Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).
- Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.

## SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

*IT Department shall:*

- Provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.

# SECURITY TRAINING RECORDS

_________________________ Manager shall:

- Designate personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

- Retain individual training records with individual employee records.

## COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

## RESPONSIBLE DEPARTMENT

____________________________ IT Department
____________________________ Manager

**DATED  ISSUED/DATE REVIEWED**

| | |
|---|---|
| **DATE ISSUED:** | **DECEMBER 1, 2022** |
| **DATE REVIEWED:** | |

# Cybersecurity Awareness Training Resource

## Online:

https://learnsecurity.amazon.com/

https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html

## For Questions Please Contact:

***info@dataprivacyinstitute.org***