Policy #:	Title:	Effective Date:
x.xxx	Security Awareness and Training Policy	MM/DD/YY

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.

1. SECURITY AWARENESS TRAINING
   The cisecurity shall:

   a. Schedule security awareness training as part of initial training for new users.

   b. Schedule security awareness training when required by information system changes and then at least annually thereafter.

   c. IT 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:

      i. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

      ii. 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.

2. SECURITY AWARENESS | INSIDER THREAT

IT Department shall:

a. Include security awareness training on recognizing and reporting potential indicators of insider threat.

3. ROLE-BASED SECURITY TRAINING
   IT Department shall:

   a. Provide role-based security training to personnel with assigned security roles and responsibilities:

      i. Before authorizing access to the information system or performing assigned duties.

      ii. When required by information system changes and at least annually thereafter.

   b. Designate personnel to receive initial and ongoing training in the employment and operation of environmental controls to include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.

4. PHYSICAL SECURITY CONTROLS
   IT Department shall:

   a. 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).

   b. Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.

5. PRACTICAL EXERCISES
   IT Department shall:

   a. Provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

6. SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR
   IT Department shall:

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

7. SECURITY TRAINING RECORDS
   The [entity] shall:

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

   b. Retain individual training records for a minimum of one year.

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.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests and confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY