Tier 1 Control Standards (State-Wide)

Information Security Training & Awareness

Standard ID
IOT-CS-SEC-013

Published Date
4/4/2017

Effective Date
4/4/2017

Last Updated
4/4/2017

Next Review Date
4/4/2018

Policy
07.0 Awareness and Training (PR.AT)
  07.1 PR.AT-1
       07.1.1 General Security Awareness Training

Purpose
Uninformed users can cause harm to the State network by responding to phishing e-mails, visiting websites infected with malware and so on. Information Security Training and Awareness provides the knowledge necessary to prevent costly errors in regards to information security.

Scope
IOT Supported Entities

Statement
All State personnel, and other users that have a State email are required to complete information security awareness training provided by IOT. The training is periodic in nature, as often as monthly. The following provides a general set of items that are covered directly or indirectly as part of the overall training and awareness program:

- Email Security/Phishing
- Information Protection
- Passwords
- Physical Security
- Social Engineering

The delivery mechanism will be through an online site or through the State's learning management system.

Agencies are required to take all of the trainings within 45 days of release or per any required completion date (if specified in a communication). Reporting will be provided to agency management for completion rates, including specific users that haven't completed the training.

Roles
All Personnel
Responsibilities
All personnel shall take the information security training(s) within the published due date or within 45 days of release.

Management Commitment
Management shall ensure that all personnel are completing the information security training(s) and discipline users that are delinquent in their responsibility.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT for SCORM compliant modules.

Compliance
Management can request reporting from IOT for completion rates. To the discretion of IOT management, users that haven't completed the training may be subject to protective measures until the training has been completed.

Exceptions
Exceptions will be handled on a case by case basis through the State CISO.