FY 26-27 Training Program Certification Standards

These standards will be used to assess and determine whether a cybersecurity training program meets the minimum requirements for certification under Section 2063.102 of Texas Government Code.

Mandatory Course/Program Topics

1. Information security habits and procedures that protect information resources.
    a. The Principles of Information Security
        i. The importance of awareness training.
        ii. What 'information security' means.
        iii. The types of information (e.g., public, sensitive, confidential, regulated, etc.) users are responsible for safeguarding.
        iv. The forms and locations of the information they are responsible for safeguarding.
    b. Best Practices to safeguard information and information systems.
        i. How to prevent unauthorized access to information and information systems, including by using multi-factor authentication and securing facilities/locations.
        ii. How to safeguard against unauthorized use of information and information systems.
        iii. Best practices related to securely storing information.
        iv. Best practices related to securely disposing and sanitizing information and information systems and record retention.
        v. Best practices related to working remotely.
        vi. Best practices related to using generative artificial intelligence (AI).
2. Best practices for detecting, assessing, reporting, and addressing information security threats.
    a. Awareness of common information security terms and types of attacks.
        i. The meaning of common information security terms, including 'threat' and 'threat actor'.
        ii. Common 'threat actors' and their motivations.
        iii. Common types of attacks, including spear phishing, quishing (QR code phishing) and social engineering.
        iv. Common types of Business Email Compromise (BEC) attacks, including forced urgency, unnatural text patterns, repetitive writing, and unverifiable details.
    b. How to identify, respond to, and report on information security threats and suspicious activity.
        i. How to identify indicators for common attacks.
        ii. How to respond to and report on common attacks or suspicious activity.

3. Awareness of foreign adversary(s) influence operations and reporting foreign adversary activities, as required by Texas Government Code Section 2063.102.
    a. What "foreign adversaries" and "foreign influence operations" means, and how to identify and recognize suspected foreign influence operations.
    b. Awareness of threats from foreign adversaries, other hostile foreign actors, and coordinated foreign influence operations, including the United Front Work Department of the Central Committee of the Chinese Communist Party and other coordinated foreign influence operations.
    c. Methods used by foreign adversaries to target and influence state and local governments, including tactics used by the United Front Work Department.
    d. Where to find resources on United Front Work Department activities in Texas and adjacent states.
    e. How to report suspected foreign influence operations or contact with individuals suspected of acting on behalf of a foreign adversary to the Texas Ethics Commission and law enforcement.
4. Awareness of restrictions and reporting requirements for foreign adversary interactions, as required by Texas Government Code Section 572.070.
    a. Awareness of restrictions for employees or volunteers of a Texas state agency or a political subdivision, which include not accepting transportation or lodging that is either located in a foreign adversary country or funded by a foreign adversary, or any gift or item of value including but not limited to travel expenses and conference attendance.
    b. How an employee or volunteer of a state agency or a political subdivision of this state should report interactions, communications, or meetings with individuals representing foreign adversaries within 30 days, to the Texas Ethics Commission.
    c. Consequences for violations, including potential state felony charges, for knowingly violating these requirements.

Strongly Recommended Topics for IT Roles (Administrators and Management)

We strongly recommend, but do not require, that training programs with a target audience of IT roles contain the following:

1) Best practices for cyber hygiene.
2) Best practices for back-ups, including types, locations, frequency, testing, and protection.
3) Awareness of the Traffic Light Protocol (TLP) levels and how to follow TLP sharing guidance.
4) Common AI attacks and mitigation tactics.
5) Best practices for third-party operational risk management, including business continuity and disaster recovery.
6) Appropriate use and protection of accounts with elevated privileges.

Program Format and Features

We strongly recommend, but do not require, that training programs contain the following:

1) An assessment of learning outcomes.
2) Proof of completion.
3) Comply with accessibility standards: Texas Administrative Codes 1TAC 213, 1TAC 206 and/or WCAG 2.0 AA or higher.
4) Phishing simulations.