FY 24-25 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 2054.519(b) of the 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.
    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.

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.

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.