FY 23-24 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) What 'information security' means.
      ii) The types of information (e.g., confidential, private, sensitive, etc.) users are responsible for safeguarding.
      iii) The forms and locations of the information they are responsible for safeguarding.
   b) Best Practices to safeguard information and information systems.
      i) How to safeguard against unauthorized access to information, information systems, and secure 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.
2) Best practices for detecting, assessing, reporting, and addressing information security threats.
   a) Awareness of the meaning of information security 'threat,' 'threat actor,' 'risk,' and 'attack.'
      i) The meaning of 'threat' with regards to information security.
      ii) Common 'threat actors' and their motivations.
      iii) The meaning of 'risk' with regards to information security.
      iv) The meaning of 'attack' with regards to information security.
   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.
      iii) The definition of spear phishing, and how to identify and report on spear phishing attempts.

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.

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 20.0AA or higher.
4) Phishing simulations.