

Information Security for Every Technology User

Created to Satisfy HB 3834 for 2020

Course Objectives

Learners will understand the following terms in the context of information security:

- information security
- threat
- threat actor(s)
- risk

Learners will understand the types of information that need to be safeguarded online and in computer systems.

Learners will be aware of different forms in which that information might exist and different location in which it might be stored.

Learners will understand how to prevent the unauthorized access to information, information systems, and secure facilities.

Learners will understand how to prevent the unauthorized use of information and systems.

Learners will be aware of best practices for secure information storage.

Learners will be aware of best practices for securely deleting or otherwise disposing of information and information systems.

Learners will be aware of best practices for detecting, assessing, reporting and addressing threats to information security.

Learners will be able to describe indicators for common attacks.

Learners will understand how to respond to and report detected attacks or suspicious activity.

Modules

1. Introduction

Welcome Orientation Introductory Case Study

2. Passwords Matter

How Passwords are Used and Stored

Common Attacks

Brute-Force Attacks

Dictionary Attacks

Rainbow Tables

Social Engineering

Phishing

Keylogging

Shoulder Surfing

Guessing

Web spiders

Reused passwords exposed in breaches

3. Choosing and Protecting Strong Passwords