DCT Cybersecurity awareness

Program Duration:

2 Days

Program Objectives

- Understand legal, ethical, and professional practices in cybersecurity, including cyber security and data protection laws.
- Learn the Security Triangle: Confidentiality, Integrity, and Availability, and the importance of Non-Repudiation.
- Identify and analyze major data breaches globally, their impacts, and common security breach forms.
- Develop skills in detecting, reporting, and preventing security breaches, including social engineering and malware.
- Gain knowledge on securing passwords, physical security, data protection, and safety on mobile devices and wireless networks.

Program Overview

Designed to give learners an understanding of how to secure their data and devices while using organizational or personal resources.

DCT Cybersecurity awareness Topics

Chapter 1: Security Principles

- **Module 1:** Understand the Security Concepts of Information Assurance.
- **Module 2:** Understand the Risk Management Process
- **Module 3:** Understand Security Controls
- **Module 4:** Understand Governance Elements and Processes
- **Module 5:** Understand (ISC)² Code of Ethics

Chapter 2: Incident Response, Business Continuity and Disaster Recovery Concepts

- **Module 1:** Understand Incident Response
- **Module 2:** Understand Business Continuity
- **Module 3:** Understand Disaster Recovery

Chapter 3: Access Controls Concepts

- **Module 1:** Understand Access Control Concepts
- **Module 2:** Understand Physical Access Controls
- **Module 3:** Understand Logical Access Controls

Chapter 4: Network Security

- **Module 1:** Understand Computer Networking
- **Module 2:** Understand Network (Cyber) Threats and Attacks
- **Module 3:** Understand Network Security Infrastructure

Chapter 5: Security Operations

- **Module 1:** Understand Data Security
- **Module 2:** Understand System Hardening
- **Module 3:** Understand Best Practice Security Policies
- **Module 4:** Understand Security Awareness Training