

Program Outline

Course Name: Office Security, Documents and Information.

Code NO: Technical Security

Date: 18-Aug-2019

Course Overview

Office security is one of the most fundamental concerns for all businesses, irrespective of their sizes and domains of industry. Any threat to the office assets or employees incurs heavy losses on the businesses in the form of capital expenditure, healthcare and social securities.

On the other hand, Information Security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

This training is to inform you of the threats to your company's offices, documents, information and information systems and to provide you with best practices and knowledge to defend and protect the company's mission from internal and external threats.

Objectives

At the end of this course you will be able to:

- Explain the fundamental, and standard features of office security and access control
- Competently explain the infrastructure of alarm notification types
- Understand your role and responsibilities to protect information security.
- Define the basic components of an information security program.
- Recognize cyber threats to information systems.
- Identify and report potential breaches and privacy incidents promptly.
- Employ best practices to protect privacy and safeguard controlled unclassified documents and information.
- Identify areas of vulnerability within your organization
- Prepare a risk assessment for your organization.

Training Mechanism

This training is conducted in workshop fashion and is based on role playing and interaction in simulations of real-life scenarios, from which you will learn and practice the skills needed to apply the principles of office, documents and information security. It includes:

- Presentation & Slides
- Audio Visual Aids
- Interactive Discussion
- Participatory Exercise
- Action Learning
- Class Activities
- Case Studies
- Workshops

Outline/Contents:

- Roles and responsibilities of security officers
- Description of operational capability process
- Determining critical and sensitive operational or administrative needs
- Standard features of office security and access control
- Basic components of an information security program.
- Recognize cyber threats to information systems.
- Identify and report potential breaches and privacy incidents promptly
- Conducting risk assessments
- Identifying vulnerabilities and threats
- Determining how to mitigate risk
- Adversary Sequence Diagram (ASD) model
- Planning for physical security resources
- Security-related information technology systems
- Internal and external threat
- Resource integration
- Emergency and Crisis management
- The six vital capabilities security information technology integration software system
- Best practices to protect privacy and safeguard controlled unclassified documents and information

Duration: ٠٥ Days

Location : Asia, KSA, Yanbu

Time:08:00 AM -02:00 PM

Numbers of hours: 35 Hours

Kingdom of Saudi Arabia
Khobar Gate Tower
King Fahad Street , Khobar 31952
Tel.: 00966133308334

Kingdom of Saudi Arabia
101 Business Tower, 8th Floor
Al Jubail 35513, Bldg# 9278 ,KSA
Tel.: +966 13 361 5552