COURSE OUTLINE

Course Code: CN-CSF

Course Name: CyberSAFE Foundation

DURATION	SKILL LEVEL	DELIVERY METHOD	TRAINING CREDITS	TECHNOLOGY
1 Day	Foundation	VILT/In Class	N/A	Cybersecurity

Course Overview

The CyberSAFE course provides candidates with the knowledge, skills, and abilities to identify the common risks associated with using digital technology and safely protect themselves and their organizations from security risks.

In this course, you will use discussions, case studies, and the experiences of your instructor and fellow students to explore the hazards and pitfalls of technology and learn how to use that technology safely and securely.
.

Prerequisites

To ensure your success in this course, you should have experience with the basic use of conventional computing technology, including desktop, laptop, or tablet computers; mobile phones; and basic Internet functions, such as web browsing and email.

Target Audience

Non-technical end-users within an organization that may use technology that places the organization's critical information systems and data at risk.

.

Topics

Module 1: Identifying Security Compliance Measures

Module 1.1: Identify Organizational Compliance Requirements and Resources

- What Is Security Compliance?
- Security Policies
- AUP
- Protected Data Types
- Differentiation of Job Functions
- Facilities Policies
- Consequences of Non-Compliance with
- Organizational Resources
- Incident Reporting
- Resources for Maintaining Organizational
- Security Compliance
- Identifying Organizational Compliance
- Requirements and Resources

Module 1.2: Identify Legal Compliance Requirements and Resources

- Types of Legal Compliance Requirements
- HIPAA
- SOX
- GDPR
- NISD
- Legal Consequences of Non-Compliance
- Resources for Maintaining Legal Security
- Compliance
- Identifying Relevant Legal Compliance Requirements and Resources

Module 1.3: Identify Industry Compliance Requirements and Resources

- Industry Compliance Requirements
- PCI DSS
- ISO 27001
- NIST
- Resources for Maintaining Industry Security
- Compliance
- Consequences of Non-Compliance with
- Industry Requirements
- Identifying Industry Compliance Requirements
- and Resources

Module 2: Recognizing and Addressing Social Engineering Attack

- Recognize Social Engineering Attacks
- Social Engineering
- Social Engineering Goals
- Attack Vectors
- High-Value Targets
- Types of Social Engineering Attacks
- Recognizing Social Engineering Attacks

Module 2.1: Defend Against Social Engineering Attacks

- Resources to Defend
- Mitigation Techniques
- Guidelines for Defending Against Social
- Engineering Attacks
- Defending Against Social Engineering
- Attacks

Module 3: Securing Devices

Module 3.1: Maintain Physical Security of Devices

- Physical Security of Devices

- Organizational Device Security
- Requirements
- Personal Device Security Requirements
- Digital Presence
- Guidelines for Maintaining Device Security
- Maintaining Physical Security of Devices
- Use Secure Authentication Methods
- Authentication
- Authentication Factors
- Single-Factor, Two-Factor, and Multifactor
- Authentication
- Something You Know: Passwords, PINs,
- and Patterns
- Something You Have: Physical Devices
- and Special Apps
- Something You Are: Biometrics
- Guidelines for Using Secure Authentication
- Methods
- Using Secure Authentication Methods

Module3.2: Protect Your Data

- Data Protection
- Sensitive Data Protection
- Data Backup
- Storage Locations
- Mobile Device Considerations
- Guidelines for Protecting Your Data
- Protecting Data

Module3.3: Defend Against Malware

- Malware
- Types of Malware
- Malware Sources
- Effects of Malware
- Guidelines for Malware Mitigation
- Identifying Malware and Mitigating Its Effects

Module3.4: Use Wireless Devices Securely

- Wireless Security
- Wi-Fi Network Types
- Wireless Security Techniques
- Common Wireless Network Risks
- Organizational and Personal Devices
- Bluetooth
- Guidelines for Using Wireless Devices
- Securely
- Use Wireless Devices Securely

Module 4: Using the Internet Securely

Module 4.1: Browse the Web Safely

- Well-Known Web Browsers
- URL Structure
- Guidelines for Browsing the Web Safely
- Browsing the Web Safely

Module 4.2: Use Email Securely

- Email Security
- Common Email Risks
- Email Attachments
- Common Phishing Techniques
- Guidelines for Using Email Securely
- Using Email Securely
- Use Social Networks Securely
- Social Networking Security
- Common Social Networking Security Risks
- Guidelines for Using Social Networks
- Securely
- Employing Social Networking Security

- Use Cloud Services Securely
- Cloud Services
- Cloud Services Risks
- IoT Device Considerations
- Guidelines for Secure Use of Cloud
- Services
- Using Cloud-Based Services Securely

4.3: Work from Remote Locations Securely

- Secure Connections
- Home Network Security
- Remote Management and Managed
- Devices
- Smart Home Devices
- Collaboration Platforms
- Guidelines for Working from Remote
- Locations Securely
- Working from Remote Locations Securely

Job Role

Exams and Certifications

Associated Exam and Certification:

The CyberSAFE assessment will certify that a successful candidate has the knowledge, skills, and abilities to use computers, mobile devices, networks and the internet in a way that minimizes digital risks to themselves and their organization.

Exam Details

Delivery: Online via the CHOICE LMS

Format: Multiple Choice / Multiple Response / True-False

Duration: 20-45 minutes (on average) and candidates may retake as many times as desired.

No. of Questions: 25

Pass Score: 80%

After completing this course, students will receive a Netcampus course attendance certification**.**

Learning Objectives:

What you will learn:

- Understand security compliance needs and requirements.
- Recognize and avoid phishing and other social engineering.
- Recognize and avoid viruses, ransomware, and other malware.
- Help ensure data security on computers, mobile devices, networks, the Internet, and in the cloud.

- Identify the need for security
- Secure devices like desktops, laptops, smartphones and more.
- Use the internet securely

What is next?

Follow on Course:

Link to the next recommended course -link to course on website