CyberSecure

CyberSecure Certification and Objectives

The CyberSecure certified individual is a professional having strong security awareness skills with an understanding of security concepts related to information processing, data protection actions, and attack awareness. The individual is not responsible for implementing security technologies but understands their purpose and impact on security posture. The CyberSecure certified individual understands the importance of the actions taken on a computer network or on a computer system and how they impact the security of the network or system.

The CyberSecure exam may be attempted by individuals who have completed the CyberSecure training course. The training course delivers essential knowledge for the modern professional in the areas of security concepts, solutions, and actions. Those who score 70% or better on the CyberSecure exam are awarded the certification, which is valid for one year from the date of exam completion. The exam consists of 60 multiple-choice, single-correct answer questions. The CyberSecure certification may be renewed by passing the latest version of the exam or acquiring continuing education credits through participation in learning modules provided annually by AACSP.

Knowledge Domains

- Security Concepts – 40%
- Secure Solutions – 30%
- Secure Actions – 30%

1.0 Security Concepts

- 1.1 Understand security as it is defined related to computing technology
  - 1.1.1 Asset protection
  - 1.1.2 Rights vs. permissions
  - 1.1.3 Identities
- 1.2 Describe the difference between security and privacy
  - 1.2.1 Security as a policy
  - 1.2.2 Security as a process
  - 1.2.3 Privacy regulations
  - 1.2.4 Privacy as a policy
  - 1.2.5 Privacy as a process

- 1.3 Explain the AAA concept and why it is important to secure operations
  - 1.3.1 Authentication
  - 1.3.2 Authorization
  - 1.3.3 Accounting
- 1.4 Describe the CIA concept and its impact on security and privacy
  - 1.4.1 Confidentiality
  - 1.4.2 Integrity
  - 1.4.3 Availability
- 1.5 Understand common vulnerabilities, threats, and risks
  - 1.5.1 Causes of security breaches
  - 1.5.2 Characters of security breaches
  - 1.5.3 Cost of security breaches
  - 1.5.4 Situational awareness
- 1.6 Explain information classification concepts and policies
  - 1.6.1 Classified vs. unclassified
  - 1.6.2 Levels of classification
  - 1.6.3 Original and derivative classification
  - 1.6.4 Security clearance concepts

2.0 Security Solutions

- 2.1 Data security technologies and applications
  - 2.1.1 Authentication technologies
  - 2.1.2 Authorization technologies
  - 2.1.3 Accountability technologies
  - 2.1.4 Confidentiality technologies
  - 2.1.5 Integrity technologies
  - 2.1.6 Availability technologies
- 2.2 Security technologies and processes used to secure computing devices
  - 2.2.1 Local storage encryption, authentication, and authorization
  - 2.2.2 Removable storage encryption, authentication, and authorization
  - 2.2.3 Trusted computing
  - 2.2.4 Mobile device security
  - 2.2.5 Safe use practices
- 2.3 Security solutions used with Internet technologies
  - 2.3.1 Web browsers and security
  - 2.3.2 File downloads and security
  - 2.3.3 E-mail and security
  - 2.3.4 Safe use practices

2.4 Physical, facility, and environmental security solutions
    2.4.1 Video cameras
    2.4.2 Building authentication and authorization
    2.4.3 Room/floor authentication and authorization
    2.4.4 Evacuation plans
    2.4.5 Active shooter/terrorist/armed robbery awareness and plans
    2.4.6 Natural disaster plans

3.0 Secure Actions
    3.1 Perform basic actions to encrypt sensitive data
    3.2 Perform basic actions to manage your identity and credentials
    3.3 Perform basic actions to maintain privacy of organizational and personal information
    3.4 Perform basic actions to avoid social engineering and phishing attacks
    3.5 Perform basic actions to protect sensitive information during business travel
    3.6 Perform basic actions to protect sensitive organizational information during remote work
    3.7 Perform basic actions to ensure data availability in disaster or hardware failure scenarios
    3.8 Report security incidents to appropriate personnel and take appropriate personal actions during an incident