Curriculum

2 Levels

Cybersecurity Level I

Cybersecurity Level II

Harper College

ApprenticeshipUSA

CYBERSECURITY APPRENTICESHIP

The Cybersecurity Apprenticeship focuses on the skills and core competencies sought after in Cybersecurity Professionals in order to perform work responsibilities which are protective of the organization's computer and digital infrastructure. The program consists of courses aligning to DoD Workforce Structure categories and National Initiative for Cybersecurity Education (NICE) Framework. Multiple courses are mapped to third-party certification exams.

Cybersecurity I

Related Learning Topics

1. **Workplace Communication and Interpersonal Skills**
   Objectives: Covers the skills to work effectively within a professional business and team environment. Understand team dynamics and resolving interpersonal conflict. Effective communication, business analysis, problem solving and team development are covered.

2. **CompTIA A+**
   Objectives: Teaches how to install, upgrade, repair, configure, troubleshoot, optimize, and perform preventive maintenance of personal computer hardware and operating systems. *Passing the CompTIA A+ Certification Exam meets the requirements for U.S. DoD Directive 8570.01 Technical Level-I*

3. **CompTIA Network+**
   Objectives: Teaches network security practices, networking models, TCP/IP addressing, how to troubleshoot and implement networks across LAN and WAN infrastructures. *Passing the CompTIA Network+ Certification Exam meets the requirements for U.S. DoD Directive 8570.01 Technical Level-I*

4. **Web Maintenance and Management**
   Objectives: Covers web authoring skills, creating a web page, and maintaining a simple website. Understand the purpose, meaning, and proper structure of HTML tags.

Contact Hours

144 Instructional Hours

Prerequisites

Knowledge of computing and networking concepts, hardware and software, functions of software, operating systems, applications, the Internet and file systems.

Cybersecurity II

Related Learning Topics

1. **CompTIA Server+**
   Objectives: Teaches how to administer any type of network server. Covers server architecture, administration, storage, security, networking, troubleshooting and disaster recovery.

2. **CompTIA Security+**
   Objectives: Covers workstation and server security, network vulnerabilities, risk assessments, monitoring tools, network security tools, authentication, rights and privileges, encryption, and disaster recovery. *Passing the CompTIA Security+ Certification Exam meets the requirements for U.S. DoD Directive 8570.01 Management Level-I and Technical Level-I*

3. **CompTIA Cybersecurity Analyst+**
   Objectives: Covers monitoring and detecting security incidents in information systems and networks, and executing a proper response. Introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. *Passing the CompTIA Cybersecurity Analyst+ Certification Exam meets the requirements for U.S. DoD Directive 8570.01 Technical Level-II, and Cybersecurity Service Provider (CSSP): Analyst, Incident Responder, Infrastructure Support, Auditor.*

4. **CompTIA Penetration Tester+** (New Course)
   Objectives: Covers penetration testing, vulnerability assessment and vulnerability management skills. Identify weaknesses and determine if existing cybersecurity practices deviate from accepted practices, configurations and polices. Determine network resiliency of network defense architecture and unknown attacks.

Contact Hours

160 Instructional Hours

Prerequisites

CompTIA A+ or equivalent experience plus 18-24 months of IT experience or equivalent knowledge.