Computer Information Systems (CIS)

CIS 170 Cisco I

5 Hours

Prerequisites: None

7 hours weekly (3-4)

The CCENT Certification validates the skills required for entry-level network support positions, the starting point for many successful careers in networking. CCENT certified professionals have the knowledge and skill to install, operate, and troubleshoot a small enterprise branch network, including basic network security.

CIS 171 Introduction to Scripting

4 hours

Prerequisite: None

5 hours weekly (3-2)

This course provides students with the fundamental knowledge and skills to use scripting. It focuses on primary Windows PowerShell command line features and techniques for use with Windows Server and other Microsoft Windows products. Students will also learn basic scripting including, loops, counters, and arrays.

CIS 200 Network Essentials

3 Hours

Prerequisites: None

3 hours weekly (2-2)

This course will provide the student with a general background in networking concepts, procedures and skills necessary in a computer network environment. This course is designed to familiarize the student with an overview of network topologies, physical network architecture, various networking operating systems and a brief introduction into Microsoft Active Directory. This class will also provide the student with necessary skills in troubleshooting and help desk topics necessary for the network's technician and software specialist.

CIS 206 Managing Network Environments I

3 Hours

Prerequisites: CIS 200 or concurrent enrollment

4 hours weekly (2-2)

This course is designed to give the student knowledge and practical experience in administering a Microsoft Server network. Students will be able to describe the principle features of a network operating system and the networking basics of active directory. Students will gain an understanding of the basic components of an information technology system. The student will work with and troubleshoot in the areas of installation of the network operating system, setting up users and groups, assignment of group policy and permissions of a network. This course will assist the student in preparing for an industry recognized certification exam.

CIS 208 Security Awareness

3 Hours

Prerequisites: None

4 hours weekly (2-2)

This course is designed to provide a security awareness overview and emphasize the importance of information systems as well as the home computer system will be covered. Issues will include personal, Internet, and organizational security. Types of security attacks will be discussed, prevention methods will be determined, and recovery plans will be developed. Policies and procedures that will

assist in preventing an invasion of privacy will be covered.

CIS 209 Introduction to Cybercrimes

3 Hours

Prerequisites: Must be 18 years of age or older.

3 hours weekly (3-0)

This course will introduce students to the investigation of computer-based crimes and the importance of preserving and correctly interpreting digital evidence. The course material will review computer crimes and associated terminology and the types of crimes committed in cyberspace. The student will also research and use data collection tools, learn proper collection and preservation of digital evidence, study domestic and international legal issues in cyberspace, and document and report data acquisition findings.

CIS 213 Penetration Testing

3 Hours

Prerequisites: CIS 208

4 hours weekly (2-2)

This course teaches students the underlying principles and many of the techniques associated with the cybersecurity practice known as penetration testing. Students will learn about the entire penetration testing process including planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. The course will provide the fundamental information associated with each of the methods employed and insecurities identified. In all cases, remedial techniques will be explored. Students will develop an excellent understanding of current cybersecurity issues and ways that user, administrator, and programmer errors can lead to exploitable insecurities.

CIS 216 Cloud Technology

3 Hours

Prerequisites: CIS 206 with Minimum Grade: C

4 hours weekly (2-2)

This course introduces students to the implementation and management of private/public/hybrid cloud environments. Students will gain both conceptual knowledge and hands-on experience in deploying, configuring, and maintaining cloud infrastructures. Topics include working with hypervisors, managing virtual machines, and integrating cloud services. The course prepares students to work with enterprise-scale solutions from providers such as Amazon, Microsoft®, and Google, as well as designing and supporting smaller-scale private cloud systems within organizational networks.

CIS 219 Ethical Hacking

3 Hours

Prerequisites: CIS 209 or CIS 230 with a grade of "C" or higher

4 hours weekly (2-2)

This course provides an in-depth understanding of how to effectively protect computer networks. Students will learn the tools and penetration testing methodologies used by ethical hackers. In addition, the course provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber-attacks. Students will learn updated computer security resources that describe new vulnerabilities and innovative methods to protect networks. Also covered is a thorough update of federal and state computer crime laws, as well as changes in penalties for illegal computer hacking.

CIS 229 Digital Forensics

3 Hours

Prerequisites: CIS 209 with a grade of "C" or higher

4 hours weekly (2-2)

Provides an introduction to Digital Forensics from a theoretical and practical perspective and an introduction to investigative tools and techniques used in the field. Personal computer operating system architectures and disk structures are reviewed and the proper use of available computer forensic hardware and software tools are examined. Other topics include the importance of digital evidence controls, the method of processing crime and incident scenes, the details of data acquisition, and the requirements of an expert witness. The course provides a range of laboratory and hands-on activities and assignments that emphasize both the theory and the practical application of computer forensic investigations.

CIS 230 Operating Systems

3 Hours

Prerequisites: None

4 hours weekly (2-2)

Students will learn important concepts about operating systems while applying skills and knowledge to support computers in a business environment or an IT position. Students will also learn the theory and technical information professionals need as they work with today's popular operating systems, such as Windows and UNIX/Linux platforms. Topics include operating system theory, installation, upgrading, configuring, (operating system and hardware), file systems, security, hardware options, and storage, as well as resource sharing, network connectivity, maintenance, and troubleshooting. This course prepares students to understand the fundamental concepts of today's computer operating systems.

CIS 231 Firewalls and VPNs

3 Hours

Prerequisites: CIS 230 with a grade of "C" or higher

4 hours weekly (2-2)

This course examines the major network security tools in use today, with the idea that firewalls are most effective when backed by thoughtful security planning, well-designed security policies, and integrated support from anti-virus software, intrusion detection systems, and related tools. Coverage includes packet filtering, authentication, proxy servers, encryption, bastion hosts, virtual private networks (VPNs), log file maintenance, and intrusion detection systems. The course will provide numerous realistic projects and cases incorporating cutting-edge technology and current trends, giving students the opportunity to hone and apply the knowledge and skills they will need as working professionals. Students will also learn about relevant National Institute Standards and Technology guidelines that are used by businesses and information technology professionals.

CIS 270 Cisco II

4 Hours

Prerequisites: CIS 170 with a grade of "C" or higher

5 hours weekly (3-2)

The CCNA R&S certification validates the ability to install, configure, operate, and troubleshoot medium-size routed and switched networks. CCNA certified professionals have the knowledge and skills to make connections to

remote sites via a WAN, and mitigate basic security threats. CCNA R&S training covers (but is not limited to) the use of these topics: IOS, IPv6, IPv4, OSPF, Cisco Licensing, Enhanced Interior Gateway Routing Protocol (EIGRP), Serial Line Interfaces, Frame Relay interfaces VLANs, Ethernet, VLSM, and basic traffic filtering.