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, ps ly-4.95(s)-1.3 (,.) e83c8 (u(i)10.610.675 0 Td( )TjEMC /H1 /MCID 12 BDC /TT0 01 f-0.004 Tc-0.0210.6-8.87)-

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

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 21eloud Technology

3 Hours

Prerequisites: CIS 206 with Minimum Grade: C

4 hours weekly (e22)

Guide to Supporting Microsoft Private Clouds instructs future networe administrators how to effectively implement and maintain Microsoft® private clouds with a balance of conceptual expertise and hands-on sills Ideal foreourratnds

e wit8 (0)6 -1.9 (a1a.9 (o)-6.7 ((g)2.6 36-.)1

CIS 225 Advanced Data Base Management

3 Hours

Prerequisites: CIS 120

4 hours weekly (2-2)

This course is a continuation of CIS 120. The concepts needed to develop and maintain a database system at an advanced level will be emphasized. Items that will be covered are: advanced query manipulation, table linking, macro programming, planning and creating a switchboard application as well as applying custom toolbars. Business simulated projects will be a major part of the curriculum. Upon completion of this course, the student should be prepared to take the Microsoft Certification exam.

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
ki3 (ic)-1.9 (411.5 (ill)( )10.6 71 (o)-9.(ic)-1.9 (415.5 (i3 (6 (q)-0.7

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