

INFORMATION TECHNOLOGY (IT)

Course Descriptions

IT 100. Introduction to Cybersecurity. 1 Credit Hour.

Introduction to Cybersecurity introduces the people, products, and processes that protect electronic data from those with malicious intent. This course will introduce students to various experts who discuss the concepts of cybersecurity including what it is, why it is important, and some of the products and processes that they use to secure data. Connections between the required courses in the Cybersecurity Program will be explored. The opportunities within this growing field will be covered. This course is not intended to teach students to implement security products and processes, but rather to make students aware of the global need for cybersecurity and the advancement in this industry. Cybersecurity requires a basic understanding of networking concepts. Supplemental information and activities for specific networking concepts are included where needed throughout the course.

Prerequisites: Reading Proficiency

IT 101. Cisco Networking Academy I: Introduction to Networks. 5 Credit Hours.

Cisco Networking Academy I: Introduction to Networks focuses on learning the fundamentals of networking. Practical and conceptual skills that build the foundation for understanding basic networking will be covered. This is the first of three (3) courses in preparation for the Cisco Certified Network Associate (CCNA) certification. (Credit is only allowed for either IT 101 or IT 501 or IT 589.)

Prerequisites: Reading Proficiency

IT 102. Desktop Software Support - CompTIA A+ Core 2 (Software). 3 Credit Hours.

Desktop Software Support - CompTIA A+ Core 2 (Software) prepares students to take the current CompTIA A+ software (Core 2) exam. Students will learn to implement, administer, and troubleshoot the Microsoft Windows client operating system. Topics include installation, upgrades, restoration, user profiles and accounts, troubleshooting, operating system security, and the TCP/IP protocol. Windows, Linux, and mobile operating systems are covered.

Prerequisites: Reading Proficiency

Recommended Preparation: Basic computer literacy is expected

IT 103. Help Desk Principles. 3 Credit Hours.

This course focuses on key information and skills for user support professionals, including troubleshooting and problem solving, communicating successfully with clients, performing end-user needs analysis and assessment, and training end-users. With balanced coverage of both people skills and technical skills, this course is an excellent resource for those in or preparing for the technical support field.

Prerequisites: Reading Proficiency

IT 120. Enterprise Security Management. 3 Credit Hours.

This course examines managerial aspects of computer security and assurance for enterprises. Topics include risk management, contingency planning, access control models, and information security governance including FISMA compliance, program assessment and metrics. The student will acquire knowledge of accreditation, certification, procurement and operating principles for secure computing systems.

Prerequisites: IS 237 with a minimum grade of "C" and Reading Proficiency

IT 121. Secure E-Commerce. 3 Credit Hours.

Secure E-Commerce examines the principles and techniques for secure electronic commerce. Topics include cryptography, certification authorities, public key infrastructure, biometrics, digital signatures, and legal and national policy issues surrounding e-commerce.

Prerequisites: IS 229 and IS 237, both with a minimum grade of "C" and Reading Proficiency

IT 201. Cisco Networking Academy II: Switching, Routing, and Wireless Essentials. 5 Credit Hours.

Cisco Networking Academy II: Switching, Routing, and Wireless Essentials focuses on the architecture, components, and operations of routers and switches in a small network. Configuration of routers, switches, and wireless access points for basic functionality will be covered. This is the second of three (3) courses offered as preparation for the Cisco Certified Network Associate (CCNA) certification exam. (Credit is only allowed for either IT 201 or IT 502.)

Prerequisites: IT 101 with a minimum grade of "C", and Reading Proficiency

IT 202. Cisco Networking Academy III: Enterprise Networking, Security, and Automation. 5 Credit Hours.

Cisco Networking Academy III: Enterprise Networking, Security, and Automation focuses on hierarchical network design, Internet Protocol version 4 (IPv4) Open Shortest Path First (OSPF) single area routing, and Quality of Service (QoS) concepts. Configuring and securing enterprise network devices will be more fully developed. Application programming interfaces (APIs) will be introduced, as well as, the configuration management tools that make network automation possible. This is the third of three (3) courses in preparation for the Cisco Certified Network Associate (CCNA) certification. (Credit is only allowed for either IT 202 or IT 503.)

Prerequisites: IT 201 with a minimum grade of "C", and Reading Proficiency

IT 208. Cisco Networking Academy: CCNA Security. 5 Credit Hours.

Cisco Networking Academy: CCNA Security focuses on network security processes emphasizing hands-on skills for security policy design and management. This course emphasizes the skills needed for security technologies, security products and solutions; such as, firewall and secure router design, installation, configuration, maintenance, Authentication, Authorization, and Accounting (AAA) implementation using routers and firewalls. Securing the network at the Open Systems Interconnection (OSI) layers 2 and 3, stressing documentation, design, and installation are also emphasized. The knowledge gained here is an important step towards other certifications like the CCNP Security. (Credit is only allowed for either IT 208 or IT 528.)

Prerequisites: IT 201 with a minimum grade of "C" or a Cisco CCENT or CCNA certification and Reading Proficiency

IT 210. Firewall and VPN Security. 3 Credit Hours.

Firewall and VPN Security focuses on security solutions and processes in a network with emphasis on practical skills in the following areas: firewall, Intrusion Prevention System (IPS), Virtual Private Network (VPN) design, implementation, configuration, and maintenance.

Prerequisites: IT 201 with a minimum grade of "C" and Reading Proficiency

IT 211. Introduction to Virtualization and Cloud Computing. 3 Credit Hours.

Introduction to Virtualization and Cloud Computing explores the installation, configuration, and management of virtualization tools, including VMware vSphere using ESXi and vCenter Server, and/or other leading virtualization solutions. Completion of this hands-on course prepares students to obtain recognized industry certifications, including the VMWare Certified Associate and VMWare Certified Professional.

Prerequisites: IT 201 with a minimum grade of "C", and Reading Proficiency

IT 212. Ethical Hacking. 3 Credit Hours.

Ethical Hacking examines the background, history, and theory of identifying potential threats on a computer or network by attempting to bypass system security and search for any weak points that could be exploited by malicious individuals or organizations. Hands-on activities using practical applications and real-life simulations to practice hacking techniques and methodologies will be used to find and attempt to exploit vulnerabilities of an organization's network infrastructure. Best countermeasures will be determined to improve security policies to protect information resources in an effort to minimize or eliminate any potential attacks. Communication skills and techniques for the cybersecurity workplace are emphasized throughout the course.

Prerequisites: IS 229 and IS 237 with minimum grades of "C", and Reading Proficiency

IT 214. Systems Security Engineering. 3 Credit Hours.

This course prepares the student to identify, evaluate, and prioritize potential threats, and manage and mitigate threats through risk management concepts, assessment activities, and monitoring terminology, techniques, and systems. Students will gain skills to properly respond to a security incident or forensic investigation with incident handling processes and procedures such as Business Continuity Planning (BPC) and Disaster Recovery Planning (DRP).

Prerequisites: IS 237 with a minimum grade of "C" and Reading Proficiency

IT 216. Digital Forensics. 3 Credit Hours.

Digital Forensics prepares students for digital crime scene investigation practices and digital evidence capture, documentation, validation, and preservation techniques through in-depth participatory exercises. Steganography, mobile data acquisition, network monitoring, decryption, and manual and automated file and password recovery techniques are taught.

Prerequisites: IS 229 and IS 237 with minimum grades of "C" and Reading Proficiency

IT 234. Principles of Incident Response and Disaster Recovery. 3 Credit Hours.

Principles of Incident Response and Disaster Recovery examines detailed aspects of event reaction and the three areas of contingency planning: incident response, disaster recovery, and business continuity. This course focuses on developing and executing plans to deal with incidents in the organization as a critical function in information security. Additional focus will be on the execution of response to human and non-human incidents in compliance with these policies.

Prerequisites: IS 237 with a minimum grade of "C" and Reading Proficiency

IT 235. Network Infrastructure Design. 3 Credit Hours.

This course covers the skills and knowledge necessary for network design engineers. Topics include design of routed and switched network infrastructures and services involving LAN, WAN, and broadband access for organizations, including service virtualization. The Enterprise Composite Model facilitates planning, design, implementation, operation and optimization (PDIOO) through modular design and the relations between modules.

Prerequisites: IT 201 with a minimum grade of "C" and Reading Proficiency

IT 250. Cisco Networking Academy: CCCA Cybersecurity Operations. 5 Credit Hours.

The Cisco Networking Academy: CCCA Cybersecurity Operations covers knowledge and skills needed to handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC). The course emphasizes best practices and provides hands-on experience needed to respond to security events to maintain and ensure security operational readiness of secure networked systems. This course prepares the student to take the Cisco Certified CyberOps Associate (CCCA) certification.

Prerequisites: IT 101 with a minimum grade of "C" and Reading Proficiency

Recommended Preparation: Basic Windows and Unix operating system knowledge is recommended, and the other Cisco courses, IT 201 and IT 202, are also very helpful

IT 251. Cisco Networking Academy: CCNA DevNet Associate. 5 Credit Hours.

Cisco Networking Academy: CCNA DevNet Associate (DEVASC) develops workforce readiness skills and builds a foundation for success in automation-related careers and degree programs. Students learn, apply, and practice programming and infrastructure automation knowledge and skills through a series of in-depth hands-on experiences that reinforce their learning. Upon completion of the DEVASC course, learners will be prepared to take the Cisco DEVASC certification exam.

Prerequisites: IT 101 with a minimum grade of "C", and Reading Proficiency

Recommended Preparation: It is recommended students to have basic skills with Linux and Python programming