COMPUTER INFORMATION SYSTEMS (CIS)

CIS 128 Microcomputer Hardware I (3 Credits)
Students will learn the functionality of hardware components of computing devices, including personal computers, laptops, mobile devices, and printers. Students will be exposed to best practices in maintenance and safety. The students, through hands-on activities and labs, learn to assemble and configure a computing devices and troubleshoot hardware problems. This is the first of two courses that prepares students for the CompTIA A+ certification.

CIS 143 Cloud Computing Fundamentals (3 Credits)
This course introduces cloud computing fundamentals, including underlying technologies, key service models, deployment models, and security considerations. Students will examine current cloud providers and service models, as well as best practices and tools for securing cloud environments. This course prepares students for the CompTIA Cloud+ certification exam.

CIS 147 Principles of Information Security (3 Credits)
This course introduces students to the field of information security. Topics covered include basic security principles, terminology, legal and ethical issues, as well as examining security from business and personal perspectives. Students will discuss current cybersecurity events and breaches. This is the first of two courses that prepares students for the CompTIA Security+ certification.

CIS 164 Networking Fundamentals I (4 Credits)
This course focuses on network terminology, network infrastructure, the OSI model, IP addressing, network protocols, ports and standards, and structured cabling. Students will learn how to use network tools Cisco Packet Tracer, Wireshark, and basic command prompts. This is the first of two courses that prepares students for the CompTIA Network+ certification.

CIS 165 Networking Fundamentals II (4 Credits)
This course focuses on wireless networking, network architecture, virtual computing, network segmentation, and network security. Students learn how to configure routers and switches for basic functionality. By the end of this course, students will be able to configure and troubleshoot network devices and resolve common network issues. This is the second of two courses that prepares students for the CompTIA Network+ certification.
Prerequisite: CIS 164

CIS 180 Creating Web Pages (3 Credits)
The course will cover the fundamentals of website layout and build a website using programming languages HTML and CSS. Students will learn how to implement responsive design and search engine optimization into their web pages. Students will also learn about best practices in website security.

CIS 208 Database Management (4 Credits)
This course focuses on database management system (DBMS) concepts and applying them to practical business situations. Topics include database environments, relational database modeling, logical and physical design, Structure Query Language (SQL), and database administration. Students will use a relational DBMS, employ associated tools, and write programs to manipulate tables.

CIS 212 Microsoft Windows Operating System (3 Credits)
The course helps learners to gain the knowledge and skills to install, configure, customize, optimize, and troubleshoot the Microsoft Windows operating system in a stand-alone and network environment.

CIS 216 Impl MS Network Infrastructure (3 Credits)
This course helps learners who will be responsible for configuring, managing, and troubleshooting a network infrastructure that uses the Microsoft Windows Server products. Students will learn how to install and manage a Microsoft Server and it roles. DHCP, DNS, RRAS, and File and Print services will be explored along with other roles and services in both physical and cloud computing environments.
Prerequisite: CIS 212

CIS 220 Linux Fundamentals (3 Credits)
This course introduces students to the fundamental concepts of Linux/UNIX operating systems. Students will be trained in Linux command line utilities, file systems, text processing, and shell scripting. Open source software will be utilized in exploring cybersecurity concepts. This course prepares students for the CompTIA Linux+ certification exams.

CIS 255 Computer and Network Security (3 Credits)
This course introduces students to technologies and practices used to secure computers and networks. Topics covered include cryptography, secure authentication, logging, device security, and other aspects of enterprise security. Students will discuss current cybersecurity events and breaches. This is the second of two courses that prepares students for the CompTIA Security+ certification.
Prerequisite: CIS 147

CIS 284 Incident Response & Disaster Recove (3 Credits)
This course examines detailed aspects of incident response and contingency planning consisting of incident response planning; disaster recovery planning; and business continuity planning. Developing and executing plans to deal with incidents in the organization is a critical function in information security. This course focuses on the planning processes for all three areas of contingency planning; incident response; disaster recovery and business continuity; and the execution of response to human and non-human incidents in compliance with these policies.

CIS 297 CIT Internship (3 Credits)
The internship experience is to integrate classroom learning from the Computer Information Technology (CIT) courses with practical experience in the information technology industry. The intern will complete a 45-hour internship in an IT field and 16 hours of classroom sessions. The intern will be mentored by the employer and supervised by the Computer Information Technology instructor.