CIT 150: Cybersecurity Principles

This course introduces the principles and practices of information systems security in computer networks. It covers the foundation of securing computer networks, including cryptography models, authentication, communications security, infrastructure security, operational and organization security. Students learn the risks, threats, and vulnerabilities of computer networks and countermeasure strategies. Topics include definition of terms, concepts, elements, and goals of incorporating industry standards and practices with a focus on confidentiality, integrity, and availability aspects of information systems. This course prepares students to sit for the current CompTIA Security+ certification exam. Prerequisite: CIS 134 Networking Technologies or permission of the instructor. Three lecture hours per week. Instructional support fee applies. Gen. Ed. Competencies Met: Critical Thinking, Information Literacy, and Scientific Reasoning and Discovery.

Course Student Learning Outcomes

1. Explain information systems security, why it is important, and its effect on people and businesses. 2. Describe the principles of risk management, risk assessments, and contingency planning to mitigate threats and vulnerabilities in an IT infrastructure. 3 .Describe networking principles, security mechanisms, cryptography models, and the role of access control in an IT infrastructure. 4. Describe the impact of malware on an organization's systems and how to prevent and detect attacks. 5. Explain the role of security operations in an IT infrastructure including testing, monitoring, and incident handling. 6. Apply information security standards, professional certifications, and compliance laws to real-world applications in both the private and public sectors.
Credits: 3
Program: Computer Information Technology