CIT 252: Critical Security Controls

This course provides a foundation for access control and identity management methods used to secure networks, data, and information systems in both the public and private sectors and in organizations large and small. Topics include data classification, identification, authentication, authorization, and accounting protocols and services for information systems whether local, remote, or cloud-based architectures. Security controls for access control including tokens, biometrics, and the use of public key infrastructures (PKI) will also be covered. Prerequisite: CIT 150 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. Define access control, identity management, and appropriate technical solutions to mitigate risk and threats in an IT infrastructure. 2. Implement remote access, PKI, and encryption solutions to ensure confidentiality, integrity, and availability of business communications. 3. Mitigate risk from unauthorized access to IT systems through proper testing and monitoring. 4. Analyze how information classification standards impact IT infrastructure access control requirements and implementation. 5. Develop an access control policy framework consisting of best practices for policies, standards, procedures, and guidelines to mitigate unauthorized access. 6. Assess the consequences of failed access controls and mitigate unauthorized access.

Credits: 3

Program: Computer Information Technology