# CIT 250: Cyber Defense and Firewall Security

This course offers an introduction to firewalls and virtual private networks (VPNs) for securing a network. Various network security-related issues, such as threats and business challenges, are introduced and examined. The course addresses firewall functionality and how to select, construct, configure, and manage a firewall. Different types of VPNs for securing data in an organization are also addressed including the benefits, various architectures, and implementation considerations. In addition, students will learn the essentials of secure network design and management. 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. Explain the fundamental concepts of network security and the impact of risks, threats, and vulnerabilities. 2. Describe common network topologies, network infrastructures, and incorporate them into a secure network design. 3. Describe the fundamental functions performed by firewalls, common firewall technologies, and the elements of firewall implementation and configuration. 4. Describe the fundamental functions of virtual private networks (VPNs), common VPN technologies, and associated authentication methods. 5. Implement firewalls and VPNs to protect a network from various types of attacks and exploits. 6. Identify firewall and network security management best practices.

**Credits:** 3

**Program:** Computer Information Technology