ISA 4220: Server Systems Security

3 Credit Hours

Prerequisite: ISA 3010 and ISA 3200

This course is an exploration of server computer system security and vulnerabilities, including server computer architectures, and operating systems. It provides the detailed technical coverage necessary to protect computer information system servers by presenting the knowledge of server platform computer hardware components, server network devices and interfaces, as well as the structure and usage of common server operating system software from an information security perspective. Additional learning regarding ongoing maintenance and operational issues of server computing systems will also be included.

ISA 4330: Incident Response and Contingency Planning

3 Credit Hours

Prerequisite: ISA 3400, 60 credit hours with a minimum GPA of 2.0, and (Admission to the Coles College Undergraduate Professional Program or student in a Coles College Partner Program that includes this course)

An examination of the 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.

ISA 4350: Management of Digital Forensics and eDiscovery

3 Credit Hours

Prerequisite: ISA 3200 and ISA 3210, 60 credit hours with a minimum GPA of 2.0, and Admission to the Coles College Undergraduate Professional Program or student in a Coles College Partner Program that includes this course.

This course focuses on the detection, isolation and response to security breaches and attacks. It provides a detailed examination of the entire computer forensic process and presents specific procedures required to respond to a computer crime incident. Subjects include recognizing unauthorized access, identifying file anomalies, and traffic monitoring.