

Courses Offered

CNG 131 – Principles of Information Assurance

Provides students with the skills and knowledge required to survey key issues associated with protecting information assets, determine the levels of protection and response to security incidents, and design a consistent, reasonable information security system, with appropriate intrusion detection and reporting features. Students will learn to inspect and protect your experience you, detect and react to threats to information assets, and examine pre- and post-incident procedures, and technical and managerial responses. Students will learn about information security planning and staffing functions.

CNG 132 – Network Security Fundamentals

Delivers a comprehensive overview of network security, including general security concepts. Communication Security is studied, including remote access, e-mail, the Web, directory and file transfer, and wireless data. Common network attacks are introduced. Cryptography basics are incorporated, and operational/organizational security is discussed as it relates to physical security, disaster recovery, and business continuity. Computer forensics is introduced.

CNG 133 – Fire Walls/Network Security

Teaches students the basics of network firewall security. It covers basic installation techniques, discusses how to make an intelligent choice of firewall technology, and presents basic firewall troubleshooting.

CNG 136 – Guide to IT Disaster Recovery

Presents methods to identify technology and communication infrastructure vulnerabilities and appropriate countermeasures to prevent and mitigate failure risks for an organization. The course will take an enterprise-wide approach to developing a disaster recovery plan.

CNG 257 – Network Defense and Counter Measures

Examines the tools, techniques and technologies used in the technical securing of information assets. This course provides in-depth information of the software and hardware components of Information Security and Assurance. Topics include firewall configurations, hardening UNIX and NT servers, Web and distributed systems security and specific implementation of security modes and architectures. The curriculum maps to the Security Certified Network Professional (SCP) Network Defense and Countermeasures exam.

CNG 258 – Computer Forensics

Exposes the student to the field of digital computer forensics and investigation. This class provides the student with methods to properly conduct a digital forensics investigation including a discussion of ethics. Topics covered include fundamental concepts, history of computer forensics, file structures, data recovery techniques, computer forensic tools and analyses

CNG 259 – Enterprise Security

This course challenges students to combine the skills learned in previous coursework (or work experience) and apply them in whole to a mock business IT environment. Students will work in their own virtualized server environment, complete with servers, routers, firewalls, VPN, IDS/IPS, wireless and other current technologies to develop a security policy and framework using risk analysis and risk management techniques.

CIS 222 – UNIX System Administration

Provides students with knowledge and skills to configure, administer and secure data, users, and services in a UNIX/Linux server environment.

CNG 280 – Internship

Provides students with the opportunity to supplement coursework with practical work experience related to their educational program. Students work under the immediate supervision of experienced personnel at the business location and with the direct guidance of the instructor.