Undergraduate Certificate - Information Security Planning

The undergraduate certificate in Information Security Planning examines the principles of information systems attack and defense, and applies that knowledge to protect the information assets of an organization. You'll be taught how to design secure networks, develop security policies, use cryptography, and perform business continuity planning.

Courses in this program meet the topical requirements of the DoD Directive 8570.1M Information Assurance Management (IAM) Technical II, Technical III, Management I, Management II, and Management III categories. Additionally, the National Security Agency (NSA) Information Assurance Courseware Evaluation (IACE) has certified some courses for this program.

Certificate Objectives

Upon successful completion of this certificate, the student will be able to:

- Assess the laws (national and federal), policies (including Sarbanes-Oxley Act), issues (social, psychological, legal, and management), risks, and controls related to information assurance and network security.
- Appraise the principles and concepts behind computer network defense (CND) methodology, robust codes, cryptography, authentication, authorization, non-repudiation, and commercially available security packages (PKI, PGP, Kerberos, SSL, VPN).
- Examine the processes, roles and responsibilities of management and security professionals in risk assessment, risk mitigation, security validation, policy enforcement, and personnel indoctrination.
- Assess the key components of the Physical Security Policy, Internet Security Policy, Email Security Policy, Encryption Security Policy, Software Development Security Policy, Authentication Security Policy, Network Security Policy, Acceptable Use Policy, and the policy that addresses viruses, worms, and Trojan horses.
- Assess the engineering discipline, process, techniques, tools, and technologies used by hackers to gain unauthorized access to the systems and appraise counter measures to mitigate this risk.
- Examine the plans, procedures, practices, and tools to ensure business continuity and to recover rapidly after an incident.

Certificate Requirements (18 semester hours)

Code	Title	Semester Hours
ISSC361	Information Assurance	3
ISSC262	Red and Blue Team Security	3
ISSC422	Information Security	3
ISSC471	IT Security: Auditing	3
ISSC481	IT Security: Planning and Policy	3
ITMG281	Law, Privacy, and Digital Data	3
Total Semester Hours		18