Undergraduate Certificate - Information Systems Security Essentials

The undergraduate certificate in Information Systems Security Essentials focuses on protecting information assets by ensuring availability, confidentiality, integrity, authenticity, and non-repudiation of information systems. This program concentrates on five key aspects of information security: hardware, software, networks, people, and policies. Security threats increase in number and severity at a faster rate than qualified security professionals can fill the necessary gap. Knowledgeable security professionals are needed even in a troubled economy, as businesses are forced to prioritize to invest in a secure digital environment.

Courseware in this online program is designed to prepare you for the Security+ certification. It meets the topical requirements of the DoD Directive 8570.1M Information Assurance Management (IAM) Technical III, 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:

- Evaluate information security strategies, architectures and plans to counteract intruders in an information system.
- Appraise national and federal laws, policies, and guidance related to information assurance; also develop an awareness of the social, psychological, ethical, and legal policies and requirements in the field of information assurance.
- Examine and profile the various types of security attacks and exploits; also appraise various security technologies, such as: packet filtering, Stateful Packet Inspection (SPI), proxy technology, Network Address Translation (NAT), Public Key Infrastructure (PKI) authentication, and encryption.
- Analyze the concept and the functionality of firewalls, routers, Virtual Private Networks (VPN), and Intrusion Detection Systems (IDS).
- Appraise the role of security assessments, penetration testing, and security plans in establishing network security; also evaluate the components of a network security assessment methodology.
- Investigate methods of mitigating risk by minimizing the exposure of information to hackers and the techniques hackers use to avoid detection and to cover their electronic footprints.
- Develop an assessment methodology that identifies, attacks, and penetrates IP based network systems.
- Define public key cryptography, the purpose of digital certificates, and risk analysis and explain ways to securely manage operations.

Certificate Requirements (18 semester hours)

Code	Title	Semester Hours
ISSC361	Information Assurance	3
ISSC262	Red and Blue Team Security	3
ISSC363	IT Security: Risk Management	3
ISSC421	Computer and Network Security	3
ISSC422	Information Security	3
ISSC461	IT Security: Countermeasures	3
Total Semester Hours		18