Undergraduate Certificate - Cybersecurity

The undergraduate certificate in Cybersecurity examines the digital forensics tools, techniques, and methods used by cyber analysts to detect cybercrime, cyber terrorism, cyber war, cyberstalking, and cyberbullying. This online program offers both introductory and advanced forensic science courses, along with an understanding of the social and legal impacts of cyber terrorism and cyber bullying. The curriculum for this program maps to the general objectives of the International Association of Computer Investigative Specialists (IACIS) certification.

Cybersecurity experts are needed to keep systems and sensitive information secure and out of the hands of cyber criminals in government and the public safety sectors, as well as commercial industries. This certificate program is intended for undergraduate students who seek to heighten their knowledge of cybersecurity without committing to an academic degree program.

Certificate Objectives

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

- Demonstrate an understanding of the processes and goals of cyber forensics investigations.
- Assess and select Federal and State laws and legal concepts that affect how governments and organizations think about information security.
- Support the importance of search warrants and chain of custody in a forensic investigation.
- Apply the field of Cybersecurity and the regulatory standards and compliances.
- Gain the foundational knowledge and technologies needed to detect, investigate, and prevent computer-related crimes.

Certificate Requirements (18 semester hours)

Code	Title	Semester Hours
ISSC331	Legal Issues in Information Security	3
ISSC351	Computer Forensics	3
ISSC451	Cybercrime	3
ISSC452	Cybersecurity	3
ISSC457	Digital Forensics: Investigating Network Intrusions and Cybercrime Security	3
ITMG281	Law, Privacy, and Digital Data	3
Total Semester Hours		18