Information Technology (ISSC)

ISSC621 Computer Forensics (3 semester hours)
This course examines information concealment techniques, technologies, hardware, software, and relevant legislation for cyber forensics to reveal and track legal and illegal activity. The course examines the process for investigation and introduces the tools and procedures required to legally seize and forensically evaluate a suspect machine. Also covered are the rules of evidence, chain of custody, standard operating procedures, and the manipulation of technology to conceal illegal activities, and revealing concealed information using cyber forensics.

ISSC630 Advanced Cybercrime Analysis (3 semester hours)
The global reach of the Internet, the low cost of online activity, and the relative anonymity of users has led to an increase in computer related crimes. This course focuses on cybercrime investigation and prevention; it appraises the legal issues related to on-line criminal conduct, the collection of electronic evidence, and the onslaught of new technology. This course also analyzes the phases, processes, and challenges of cybercrime investigations, and it examines technical, legal, and social issues relating to the search and seizure of digital evidence and computer forensics. Students will encounter the challenges of the latency between technology and the law.

ISSC631 Cyber Ethics: Privacy and Intellectual Property (3 semester hours)
This course is an advanced study of information ethics, cyber privacy, and intellectual property. It examines the ethical, economic, and societal issues that face today’s information-entrenched society; this includes intellectual property rights, privacy, accessibility and censorship. The explosive growth of information technology, the increased competition in the global marketplace, and the surge in the use of information to protect society from terrorism has led to the unintended erosion of fundamental rights and values. This course appraises the current state of information ethics, the dangers and opportunities presented by information technology, and the potential solutions to the inherent risks in today’s information-bound society.

ISSC640 Computer Networks and Data Systems (3 semester hours)
This course is a study of computer networks and the evolution of modern communication systems. It examines the various layers of the basic reference models such as the five-layer IP model or the seven-layer OSI model, by scale, connection method, network architecture, or topology. This course also includes an in-depth analysis of transmission protocols, communications systems, and networks. Prior knowledge of networks and networking is recommended.

ISSC641 Telecommunications and Network Security (3 semester hours)
Telecommunications networks are a critical component of the global economic and social infrastructures. Securing critical infrastructure is an established priority within Information Security Management. This course examines the field of secure telecommunications networks, including emerging threats, system vulnerability, network evolution, and network defense mechanisms.

ISSC642 Intrusion Detection and Incident Handling (3 semester hours)
This course examines the tenets of Intrusion Detection, Intrusion Prevention, and Incident Handling. Intrusion Detection focuses on the methods to detect attempts (attacks or intrusions) to compromise the confidentiality, integrity or availability of an information system. Also included is an analysis of the principles and practices of intrusion detection, intrusion prevention, and incident handling; network-based, host-based, and hybrid intrusion detection; identifying attack patterns; deployment of resources and responses to handle the incident, surveillance, damage assessment, risk assessment, data forensics, data mining, attack tracing, system recovery, and continuity of operation.

ISSC650 Advanced Digital Forensics (3 semester hours)
This course is an advanced study of the models of investigative methods for finding evidence in a wide scope of disparate digital devices such as computers, laptops, netbooks, networks, mobile devices – phones, notepads, PDAs, digital audio and video players, and any device or appliance that carries an electronic circuit board which could potentially store data or information. It also examines the science, the evidence, and the law related to digital forensics, the validation of findings, and determination of acceptable and irrefutable evidence in a court of law. It also evaluates various digital forensics models for data identification, preservation, collection, examination, analysis, preparation, and presentation. (Prerequisite: ISSC621)

ISSC651 Advanced ediscovery (3 semester hours)
This course is an advanced study of the principles and methodologies of the e-discovery process and the increasing importance of digital evidence in litigation. Topics include contemporary investigative methods, legal issues, cost containment, collecting and prioritizing data sets, preservation of digital evidence, document review, metadata and spoliation considerations, comparative assessments, and forensic investigations. Prerequisite: ISSC621.

ISSC660 Information Assurance (3 semester hours)
The course analyzes computer and systems security measures by examining a model for information assurance; it also examines the components of a comprehensive Information Assurance plan. Topics included are: asset identification, human factors, compliance with regulations, personnel security, risk assessment and ethical considerations, IA policy, as well as computer and network security tools.
ISSC661 Information Assurance: Assessment and Evaluation (3 semester hours)
This course is an advanced study of the principles, practices, procedures, and methodologies to assure the protection and availability of vital digital information systems assets. It examines information assurance, incident management and response, and security standards; and it appraises the convergence between information security, information systems security, and information warfare. This course appraises organizational, legal, technical, and ethical issues related to securing vital digital assets. Topics include: the role of the corporate security officer, corporate cybercrime, electronic commerce, cryptography, and international standards, policies, and security acts. Prerequisite: ISSC660.

ISSC662 Information Assurance: Capability Maturity and Appraisals (3 semester hours)
This course examines the phases, processes, standards, the levels, and the process areas of the INFOSEC Assessment Capability Maturity Model (IA-CMM). The IA-CMM minimizes false indications of quality and maturity by relating the IA-CMM process areas to the INFOSEC Assessment Methodology (IAM). This course appraises the principles and methodologies of the IA-CMM; and applies it to develop an organizational ratings profile to provide a measure of maturity. The ratings profile is used to develop strategies to mature the organizational processes. Prerequisite: ISSC660.

ISSC680 Information Security Management (3 semester hours)
Information Security includes an evaluation of the techniques, policies and strategies to ensure that data stored in an organization’s computers cannot be accessed or processed without the consent of the organization. Also included, is an analysis of Information Security & Risk Management, Access Control, Physical Security, Security Architecture & Design, Business Continuity & Disaster Recovery Planning, Telecommunications & Network Security, Application Security, Operations Security, Law, Compliance & Investigations. This course also reviews the building blocks of information systems and cryptography is provided to reinforce the scope of security management.

ISSC698 Cybersecurity Studies: Capstone Practical (3 semester hours)
This Cybersecurity Studies: Capstone Practical course integrates the knowledge, skills, and posture acquired in the program courses. This course is the capstone course of studies completed toward the graduate degree in Cybersecurity Studies. This course will only be offered in 16 week sessions. Students will complete an applied project design that demonstrates mastery and application of advanced research and analytic skills related to the learning outcomes of this degree program. Students must submit a research proposal, preferably two months prior to enrolling in the course to obtain approval from the Cybersecurity Program Director. This course may not be taken until all other courses are COMPLETED and student has a 3.0 GPA.

ISSC699 Cybersecurity Studies Capstone (3 semester hours)
This Master’s degree capstone course in Cybersecurity Studies is an integrative, multi-disciplinary course that applies the knowledge, skills, and attitudes obtained in the core courses. NOTE: This course may not be taken until all other courses are COMPLETED and student has a 3.0 GPA. THIS COURSE IS 16 WEEKS.