Ph.D. Cyber Defense Course Descriptions

Required Courses

Prefix Number	Course Title	Credit Hours
INFA 701	**Principles of Information Assurance** This course covers key bodies of knowledge and specializations in security, privacy, and compliance associated with enterprise information systems. The course explores defense-in-depth techniques of layering people, process and technology controls to secure the enterprise. Topics include information security law, ethics, security concepts and mechanisms; security technologies; authentication mechanisms; mandatory and discretionary controls; basic cryptography and its applications; digital forensics, biometrics database security, intrusion detection and prevention, anonymity and privacy issues for information systems. Emerging frameworks and tools are explored to complete the student's foundational understanding of information assurance.	3
INFA 702	**Principles of Data Privacy** This course provides a comprehensive overview of foundational privacy compliance, management and engineering. Students will learn about international privacy regulations, management frameworks and design methodologies. Assessment will be a combination of hands-on exercises, classroom discussions and a 2-part Privacy Impact Assessment “use case.” Although course content may change as it is taught, students can expect the following topics to receive significant treatment: Privacy Foundations, Privacy Compliance, Privacy Management, Privacy by Design and Privacy Engineering.	3
INFA 710	**Cybersecurity Program Design and Implementation** Technology is being deployed at dramatic rates and changing business models. Security programs must be designed and implemented to support this technological revolution. This course is a study of the cybersecurity frameworks, models, processes and tools to equip students with the theory, science and practical knowledge to operationalize an information security program in an organization or government agency. Topics include security strategy, risk management, asset management, security documentation, network testing, disaster recovery, incident response, and security education, training and awareness programs.	3
INFA 713	**Managing Security Risks** Information technology holds the potential to create strategic, operational, financial, and reputational issues for an organization. Information technology risk management science provides decision-makers with the information needed to determine information security risk so decisions can be made regarding risk mitigation. This course is a study of the existing risk management frameworks, models, processes and tools to equip students with the theory, science and practical knowledge to operationalize risk management in an organization or government agency. Topics include outsourcing and off-shoring risks, and their mitigation through third party risk management programs. Students will examine cutting-edge risk management science to understand the future of information technology risk management.	3
INFA 720	**Incident Response** This course provides theoretical and practical aspects of incident response. Students will learn how to respond to information security incidents and understand how the incident occurred. Response, mitigation, and policy will be included in this course with both an applied and managerial approach. A focus on current tools and methodologies will be stressed.	3
INFA 731	**Personnel Security** People are often considered the weakest layer in security defense. This	1

	course will teach students the Security Education, Training and Awareness (SETA) techniques available to promote good security knowledge in employees, customers and communities. Special topics analyzed include the NIST Cybersecurity Framework and Department of Defense (DoD) Personnel Security Program (PSP) and Personnel Security Investigation (PSI).	
INFA 732	**Physical Security** Cyber and physical security are converging, and cyber/physical systems research is growing. Organizations are understanding that they cannot have good cybersecurity without good physical security. This course introduces security issues relating to various cyber-physical systems including industrial control systems and those considered critical infrastructure systems. This course provides the student with an understanding of the various levels of security that can be employed for the protection of people, property, and data housed in physical facilities.	1
INFA 733	**Vendor Management** you will learn the skills needed to effectively manage vendors. Through hands-on exercises, you'll develop an integrated understanding of how vendors are chosen, motivated and managed. Third party management is under regulatory scrutiny due to increase outsourcing, cloud computing, high profile breaches and additional guidance being issued from governments and agencies. These factors are increasing demand for Vendor Management professionals with regulatory knowledge and specialized expertise in building, implementing and managing compliant Vendor Management programs. This course provides students with the regulatory and compliance knowledge, program implementation methodology and the best practices required to build and manage a ***compliant*** program.	1
INFA 754	**Intrusion Detection** Students will learn threat hunting and detection techniques through the use of cyber threat intelligence and popular intrusion detection and data collection platforms. Topics will include signature, anomaly, and emerging detection methods on a network and host level, threat intelligence collection, classification, and sharing, and the creation of indicators of compromise.	3
INFA 758	**Security Metrics** This course provides a deep dive into Security Metrics and Measurements and Security Standards and Measurement Systems. Students will learn: • Deep understanding of design, implementation and evaluation of capability maturity models for security. • Designing and building key performance indicators (KPI) to measure the security and privacy of data. • Designing, building and implementing standard measurement systems to promote and measure the security and privacy of data.	3

Required Research Core

Prefix Number	Course Title	Credit Hours
CSC 803	**An Introduction to Cyber Security Research** An introduction to cyber security research where students will gain knowledge in identifying research sources, gathering applicable research materials, and how to best categorize and analyze the current state of research. Students will gain knowledge in transitioning from gathered research artifacts to authorizing sections of research papers applicable for submission to journals and conferences. Special attention will be paid to citation standards, anti-plagiarism and scientific writing styles	3
CSC 804	**Cyber Security Research Methodologies** This course develops skills needed in quantitative, qualitative and design	3

	science research methodologies. Students will acquire skills in the development of research proposals for each of the three methodologies normally used in cybersecurity research	
CSC 807	**Cyber Security Research** This course focuses on research issues pertaining to Cyber Security Research. During this seminar course, students will examine and evaluate the research literature from a wide variety of sources, both academic and applied. Students will also identify various research frontiers associated with cyber security.	3

Dissertation

Prefix Number	Course Title	Credit Hours
CSC 809	**Dissertation Preparation** Students will formalize, present, and defend a dissertation proposal with guidance from a faculty dissertation chair. By working closely with a faculty member, each student should have a developed dissertation proposal in a specific research field of cyber security that is agreed upon by both student and faculty member. Pre-Requisites: CSC 807	3
CSC 890	**Dissertation Seminar 1** A highly focused and topical course. The format includes student presentations and discussions of reports based on literature, practices, problems, and research. Seminars may be conducted over electronic media, such as internet, and are at the upper division or graduate levels. Enrollment is generally limited to 20 or fewer students	3
CSC 898D	**Dissertation** A formal treatise presenting the results of study submitted in partial fulfillment of the requirements for the applicable degree. The process requires extensive and intensive one-on-one interaction between the candidate and professor with more limited interaction between and among the candidate and other members of the committee.	11-21

Elective Courses:

Prefix Number	Course Title	Credit Hours
BADM 765	Management and Leadership This course is a study of general management, including the planning, directing, controlling, and coordinating of activities involved in operating a business, government, or not-for-profit organization, with special emphasis on leadership. Pre-Requisites: BADM 360	3
CSC 748	Software Exploitation This course is designed to expose students to advanced exploitation techniques. Topics include the use of automated exploitation tools as well as the process of exploitation discovery and development. Vulnerability analysis, debugging, fuzzing, shellcode, and mitigation techniques will be explored. Both Windows and Linux platforms will be covered.	3
INFA 715	Data Privacy This course explores computational techniques for releasing information in such a way that data privacy cannot be violated and provides a formal framework for privacy-enhancing technologies and models of privacy protection. It explores privacy enhancements from economic, legal and policy perspectives and introduces cutting-edge, privacy-preserving frameworks for data-mining systems	3
INFA 716	**Privacy Enhancing Technologies** Enormous data collection has emerged to support today's digitized world. How can we ensure that the collected user data are not	3

	misused, and privacy policies not violated? How can we protect user privacy while simultaneously allowing effective data sharing and utilization? This course aims at providing students with advanced concepts and latest progress on emerging techniques in information privacy. Topics will be adjusted to reflect the latest trends and the interests of students. Exemplary topics include, but not limited to, IoT privacy considerations, cloud privacy, cryptocurrency and decentralized ledger technologies, machine learning and privacy, data anonymization, and encrypted databases.	
INFA 721	**Computer Forensics** Identifying, acquiring, preserving, and analyzing electronic evidence from single machines, networks, and internet. It will explore both technical and legal issues of computer forensics investigations. Topics include forensics law and regulation issues, incidence response, open and commercial tools, evidence recovery theory and practice of computer file systems, memory, registry, network logs and communications. Special focus will be given to windows systems and networks	3
INFA 723	**Cryptography** This course covers fundamentals of cryptography and its applications, classical and contemporary ciphers, encryption and decryption and breaking ciphers. Cryptographic applications, protocols, applications of cryptography and automated tools to analyze cryptographic protocols are examined.	3
INFA 735	**Offensive Security** This course provides theoretical and practical aspects of network and web application penetration testing. The course includes in-depth details and hands-on labs for each phase of an ethical hack including, but not limited to: reconnaissance, vulnerability assessment, exploitation, maintaining access, and covering tracks. An applied approach with a focus on current tools and methodologies will be stressed.	3
INFA 742	**Ethics and Information Technology** Ethics and Information Technology concerns the ethical dilemmas that exist where human beings, information objects, and social computing technologies interact. The course explores emerging ethical models from historical and cross-cultural perspectives and then applies these models to a variety of new and emerging technologies that are inherently social in their construction and use. The course challenges students to explore ethics by using a case-study format in which technologists and information custodians must decide what to do.	3
INFA 745	**Compliance and Audit** This course examines fundamental concepts in IT security audit and control processes for the financial industry, including the control framework, attendant control objectives and reporting systems for an organization. Students learn to create a control structure, audit an IT infrastructure against it, and establish systematic remediation procedures. As part of the learning process, students have an opportunity to be certified as a CISA (Certified Information System Auditor).	3
INFA 751	**Wireless Security** A technical perspective on maintaining the availability, integrity, and confidentiality of wireless networks. Covers a wide range of technical issues, including wireless communication fundamentals, wireless network configuration, security standards, wireless vulnerabilities, attacks and countermeasures.	3