Our Master of Science in Information Assurance and Cybersecurity combines an understanding of information security technology with relevant knowledge from law, the social sciences, criminology, and management. The MS program is designed for working professionals and recent graduates who want knowledge they can apply in their workplaces to assess and manage information security risks effectively.

Learning Outcomes:
- Build core knowledge surrounding computer system security and network security practices
- Plan and implement security strategies to reduce risk and enhance protection of information assets and systems
- Understand legal and ethical issues associated with information security, privacy, and digital rights.
- Enhance communication skills for effective interaction with corporate management on information assurance/cybersecurity-related issues.

Program Requirements

General Requirements

Foundations
IA 5010 Foundations of Information Assurance 4

Technical Courses
Complete 8 semester hours from the following: 8
IA 5120 Applied Cryptography
IA 5130 Computer System Security
IA 5150 Network Security Practices
IA 6120 Software Security Practices

Contextual Courses
Complete 8 semester hours from the following: 8
IA 5200 Security Risk Management and Assessment
IA 5210 Information System Forensics
IA 5240 Cyberlaw: Privacy, Ethics, and Digital Rights
IA 5250 Decision Making for Critical Infrastructure

Capstone
IA 7900 Capstone Project/Seminar 4

Electives
Complete 8 semester hours from the following: 8
IA 5040 Introduction to Cyberspace Programming
IA 5050 Data Mining in Cyberspace
IA 5120 Applied Cryptography
IA 5130 Computer System Security
IA 5150 Network Security Practices
IA 5200 Security Risk Management and Assessment
IA 5210 Information System Forensics
IA 5240 Cyberlaw: Privacy, Ethics, and Digital Rights
IA 6120 Software Security Practices
CS 5200 Database Management Systems
CS 5500 Managing Software Development
CS 5600 Computer Systems
CS 5700 Fundamentals of Computer Networking
CS 5770 Software Vulnerabilities and Security
CS 6540 Foundations of Formal Methods and Software Analysis
CS 6710 Wireless Network
CS 6740 Network Security ¹
CS 6750 Cryptography and Communications Security
CS 7805 Theory of Computation
CRIM 7224 Law and Psychology
CRIM 7242 Terrorism and International Crime
CRIM 7252 White-Collar Crime
CRIM 7312 Special Topics in Criminology and Public Policy
PPUA 6503 Public Personnel Administration
PPUA 6505 Public Budgeting and Financial Management
PPUA 6507 Institutional Budgeting and Financial Management
POLS 7341 Security and Resilience Policy

Program Credit/GPA Requirements
32 total semester hours required
Minimum 3.000 GPA required

¹ This course can only be taken for credit if the student has NOT also taken Network Security Practices (IA 5150). These courses cannot both be taken for credit.