Cybersecurity, MS

Our Master of Science in 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:

- Building core knowledge surrounding computer system security and network security theory, processes, and practices
- Planning and implementing security strategies to reduce risk and enhance protection of information assets and systems
- Identifying and addressing legal and ethical issues associated with information security, privacy, and digital rights and identifying how they inform specific IA plan/decisions
- Communicating effectively, verbally and in writing, with corporate management on IA-related issues

GORDON INSTITUTE OF ENGINEERING LEADERSHIP

Master's Degree in Cybersecurity with Graduate Certificate in Engineering Leadership

Students may complete a Master of Science in Cybersecurity in addition to earning a Graduate Certificate in Engineering Leadership. Students must apply and be admitted to the Gordon Engineering Leadership Program in order to pursue this option. The certificate program requires fulfillment of the 16-semester-hour curriculum required to earn the Graduate Certificate in Engineering Leadership, which includes an industry-based challenge project with multiple mentors. The integrated 40-semester-hour master's degree and certificate require 24 hours of information assurance course work.

Engineering Leadership (http://catalog.northeastern.edu/graduate/engineering/leadership/engineering-leadership-graduate-certificate/#text)

Program Requirements

Core Requirement

Code	Title	Hours
Foundations		
IA 5010	Foundations of Information Assurance	4
Technical Track		
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 Track		
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

Code	Title	Hours
Complete 8 semester hours from the following:		8
IA 5040	Introduction to Cyberspace Programming	
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 6710	Wireless Network	
CS 6740	Network Security [1]	
CS 6750	Cryptography and Communications Security	
CS 7805	Theory of Computation	
CRIM 7312	Special Topics in Criminology and Public Policy	
PPUA 6503	Public Personnel Administration	
PPUA 6505	Public Budgeting and Financial Management	
PPUA 6507	Institutional Leadership and the Public Manager	
POLS 7341	Security and Resilience Policy	

Program Credit/GPA Requirements

32 total semester hours required
Minimum 3.000 GPA required

[1] Students who took Network Security Practices (IA 5150) (technical track) and are interested in taking Network Security (CS 6740) (approved elective, non–IA course) should inform the network security instructor and the director/associate director of IA.