CYBERSECURITY ENGINEERING (M.S.)

https://manchester.unh.edu/program/ms/cybersecurity-engineering

Description

This program is offered in Manchester.

Cybersecurity touches nearly every facet of an organization. From marketing to legal to finance, employees across the industry are more aware of the flow of data and the measures needed to keep it secure. Technical systems need technical solutions—which is why the University of New Hampshire has launched a Master of Science in Cybersecurity Engineering.

Designed for working professionals and those with a strong interest in cybersecurity, the program combines in-class and online learning on how to develop, engineer and operate secure information systems. You will learn the theoretical underpinnings of information security and have opportunities to apply your knowledge and skills to real-world scenarios and authentic project experiences.

With a greater emphasis on the collection and storage of big data, information security and cloud computing, the demand for cybersecurity engineers has never been higher. The M.S. in Cybersecurity Engineering gives you the technical skills and experience to meet that demand, preparing you to secure information, communications, networks and control systems for any organization.

Career Opportunities

Graduates of the Cybersecurity Engineering program are able to identify, analyze and respond to the complex information security threats that are increasingly common in today's digital landscape. You'll learn skills in core and advanced information security, preparing you to develop, integrate and evaluate secure IT systems and services for any organization.

Requirements

The M.S. in Cybersecurity Engineering program has two options for completion:

- **Master's Project Option**: 30 credits course work and 3 credits Master's Project course (total of 33 credits).
- **Master's Thesis Option**: 24 credits course work and 6 credits Master's Thesis course (total of 30 credits).

Code	Title	Credits
Required Core Courses		
COMP 815	Information Security	3
COMP 835	Secure Networking Technologies	3
COMP 855	Digital Forensics	3
COMP 865	Secure Software Principles	3
COMP 885	Applied Cryptography	3
Select one policy course from the following:		3
CPRM 810	Foundations of Cybersecurity Policy	
CPRM 830	Security Measures I	
CPRM 850	Security Measures II	
CPRM 870	Cybersecurity Risk Management	
CPRM 880	Cybersecurity Metrics and Evaluation	
Professional Experience		
COMP 801	Integrated Computing Practice [1]	3
Internship Experience [2]		
Select from the following:		3
COMP 890	Internship and Career Planning	
COMP 891	Internship Practice	
COMP 892	Applied Research Internship	
COMP 893	Team Project Internship	
Elective Courses		
Master's Project Option - Elective Coursework		6
Master's Thesis Option - Elective Coursework		0
Culminating Experience		
Select one of the following:		
COMP 898	Master's Project	3
COMP 899	Master's Thesis	6

[1] Students are required to enroll in COMP 801 within their first nine credits in the program.

[2] Students are required to enroll in at least 1 credit of Internship Experience upon successful completion of nine credits in the program. COMP 891, COMP 892, or COMP 893 may be repeated for a maximum of 6 credits.

Accelerated Master's

This graduate program is approved to be taken on an accelerated basis in articulation with certain undergraduate degree programs.

General Accelerated Master's policy, note that some programs have additional requirements (e.g. higher grade expectations) compared to the policy.

Please see the Graduate School website and contact the department directly for more information.

Student Learning Outcomes

Program Learning Outcomes

- Analyze complex computing problems and identify solutions by applying principles of computing.
- Design, implement, and evaluate computing solutions that meet computing requirements with focus on security aspects.
- Communicate effectively in a variety of professional contexts.
- Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
- Function effectively as a member or leader of a team engaged in IT activities.
- Apply security principles and practices to maintain operations in the presence of risks and threats.