

Cybersecurity, M.S.

Requirements

The Master of Science in Cybersecurity is intended for individuals who desire to acquire additional cybersecurity knowledge, skills, and abilities in order to pursue new or advance existing careers in cybersecurity. The program is also designed for individuals who plan to pursue doctorate degrees in cybersecurity or related fields. The program focuses on the managerial and technical perspectives of cybersecurity through extensive use of case-studies and hands-on lab exercises.

Total Program Credits: 30

Matriculation Requirements:			
<ol style="list-style-type: none"> Bachelor's degree with a GPA of at least 3.2 on a 4.0 scale from an accredited institution in one of the following fields*: Information Systems, Information Security, Information Technology, Computer Science. Admissions essay. Completed application for admission. Official transcripts from all attended institutions of higher education. Two letters of recommendation 			
Discipline Core Requirements:			21 Credits
	IT 6300	Principles of Cybersecurity	3
	IT 6330	Cybersecurity Operations	3
	IT 6350	Law/Ethics/Privacy in Cybersecurity	3
	IT 6370	Penetration Testing and Vulnerability Assessment	3
	IT 6740	Advanced Network Defense and Countermeasures	3
	IT 6770	Cybersecurity Management	3
	IT 6900	Cybersecurity Capstone	3
Elective Requirements:			9 Credits
Choose 9 credits from the following:			9
	IT 6660	Advanced Network Forensics (3.0)	
	IT 6750	Reverse Engineering and Malware Analysis (3.0)	
	IT 6780	Secure Coding (3.0)	
	INFO 6420	Web and Mobile Application Security (3.0)	
	or other departmental approved electives		

Graduation Requirements:

- Complete all courses with a grade of B- or better with an overall GPA of 3.0 or higher. Courses must be finished within a five-year period. No courses will apply toward graduation that are older than five years.
- Courses must be finished within a five-year period. No courses will apply toward graduation that are older than five years.

Footnote: *Applicants who have bachelor's degrees in other fields may be admitted to the program if they have at least two years of technology or cybersecurity industry experience and have completed undergraduate courses in data communication, programming, and server administration with a grade of C+ or better. Students may

also take a comprehensive exam on these topics to satisfy this admission requirement. These applications will be handled on a case-by-case basis.

Cybersecurity, M.S. Graduation Plan

This graduation plan is a sample plan and is intended to be a guide. Your specific plan may differ based on your Math and English placement and/or transfer credits applied. You are encouraged to meet with an advisor and set up an individualized graduation plan in [Wolverine Track](#).

Milestone courses (pre-requisites for a course in one of the subsequent semesters) are marked in red and italicized.

Semester 1	Course Title	Credit Hours
<i>IT 6300</i>	Principles of Cybersecurity	3
<i>IT 6330</i>	Cybersecurity Operations	3
	Semester total:	6
Semester 2	Course Title	Credit Hours
<i>IT 6740</i>	Advanced Network Defense and Countermeasures	3
<i>IT 6350</i>	Law/Ethics/Privacy in Cybersecurity	3
	Semester total:	6
Semester 3	Course Title	Credit Hours
<i>IT 6370</i>	Penetration Testing and Vulnerability Assessment	3
	Semester total:	3
Semester 4	Course Title	Credit Hours
<i>IT 6770</i>	Cybersecurity Management	3
Elective		3
	Semester total:	6
Semester 5	Course Title	Credit Hours
Elective		3
Elective		3
	Semester total:	6
Semester 6	Course Title	Credit Hours
IT 6900	Cybersecurity Capstone	3
	Semester total:	3
	Degree total:	30