Master of Science in Cybersecurity (MSC)

2025-2026 Catalog Year

Discipline Core Requirements (21 Credits)			
Course No.	**Course Title**	**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 Vunerability Assessment	3	
IT 6740	Advanced Network Defense and Countermeasures	3	
IT 6770	Cybersecurity Management	3	
IT 6900	Cybersecurity Capstone	3	
Elective Requirements (9 Credits)			
Complete 3 of the following:			
IT 6660	Advanced Network Forensics	3	
INFO 6420	Web and Mobile Application Security	3	
IT 6750	Reverse Engineering and Malware Analysis	3	
IT 6780	Secure Coding	3	
	Total Credits Required for Degree	**30**	

NOTES:

***The MS Cybersecurity is a two year, part time program. Classes will be held two evenings a week and are livestreamed (classes are also recorded to be viewed at the student's convenience)**

Not all courses are taught every semester.

Admission requirements:

1. To be accepted into the MS in Cybersecurity applicants must hold an undergraduate degree in a computing-related field (such as Information Systems, Information Security, Information Technology, or Computer Science) with a minimum overall GPA of 3.0 on a 4.0 scale. If your bachelor's degree is not in one of these fields, please contact Julie Marr at julie.marr@uvu.edu for further assistance.
2. Applicants with bachelor's degrees in other fields may still be considered for admission if they have at least two years of relevent technology or cybersecurity industry experience and have completed undergraduate courses in data communication, programming, and server administration. The following UVU courses or their equivelents meet the prerequisites:
   * Data Communication: IT 2600: Data Communication Fundamentals or CS 2600: Computer Network I
   * Programming: INFO 1200: Computer Programming I for IS IT or CS 1400: Fundamentals of Programming
   * Server Administration: IT 1510: Introduction to System Administration--Linux/UNIX or IT 2530: Introduction to System Administration--Windows Client
3. Resumé
4. Two Letters of Recommendation
5. Essay answering the following two questions: How does completing a Cybersecurity degree relate to your career and life goals? What would you like the committee to know about you that is not reflected elsewhere in your application materials?

Graduation Requirements:

1. Completion of all courses with a grade of B- or better.
2. Completion of all required courses and elective courses for a total of 30 credit hours with an average GPA of 3.0 or higher.

Contact information:

UVU Program director:
Basil Hamdan
Basil.hamdan@uvu.edu

UVU Graduate Program Coordinator/Advisor:
Julie Marr
julie.marr@uvu.edu
https://appointments.uvu.edu/juliemarr

IT 6300 Principles of Cybersecurity

implementation. Includes networking and system fundamentals, cryptography, malware, authentication, authorization, access control, physical security, attacker profiles, appropriate threat responses, and the human elements of cybersecurity. Introduces multiple aspects of cybersecurity and various career paths within the field.

IT 6330 Cybersecurity Operations

Focuses on operational aspects of cybersecurity. Includes incident response, network monitoring, change management, configuration management, and resource protection. Emphasizes the role of cybersecurity in the enterprise. Integrates sound cybersecurity principles into various aspects of IT operations. Includes information on secure server administration and open source security software. Teaches cybersecurity standards for government and industry sources and the application of those standards.

IT 6350 Law/Ethics/Privacy in Cybersecurity

security and use policies, and the government's role in cybersecurity. Emphasizes the roles and responsibilities of individual cybersecurity practitioners as well as corporate entities, including vulnerability disclosure and correcting software defects. Teaches privacy policies and regulations as they relate to cybersecurity and information systems.

IT 6370 Penetration Testing and Vunerability

Explores advanced topics in ethical hacking, penetration testing, vulnerability assessment, and other offensive network and system techniques. Teaches network scanning, target identification, application exploitation, antivirus evasion, physical security, social engineering, phishing, and privilege escalation. Contains hands-on labs providing experience from the perspective of an attacker.

IT 6740 Advanced Network Defense and Countermeasures

Explores advanced topics in network defense, server hardening, vulnerability assessment, and mitigation scanning. Teaches students about network scanning, asset identification, Linux and Windows server hardening, anti-malware tools, intrusion detection, physical security, perimeter security, and cybersecurity awareness training. Contains hands-on labs providing experience from the perspective of a defender.

IT 6770 Cybersecurity Management

management, organizational security, cybersecurity life cycle management, and interactions between information technology and business units. Focuses on policies, procedures, and guidelines based on industry and government standards to fulfill legal, regulatory, and operational requirements.

IT 6900 Cybersecurity Capstone

Provides culmination of cybersecurity in a self-directed research or practical project that showcases student's mastery of cybersecurity topics. Provides an opportunity to conduct research and/or implement systems that incorporate topics from previous courses. Requires students to present their work at the end of the semester.

IT 6750 Reverse Engineering and Malware Analysis

standard methodology for reverse engineering and eradicating malware. Includes setting up isolated malware labs and utilizing a selected set of forensic tools, such as system and network monitoring utilities, disassemblers, and debuggers for analyzing malware characteristics and the impact that malware may have on compromised systems.

INFO 6420 Web and Mobile Application Security

Examines Web application vulnerabilities and remediation techniques. Explores various tools and techniques used to perform Web application assessments. Includes cross-site scripting, SQL injection, session management, and Web server configuration. Emphasizes practical skills developed through extensive hands-on exercises.

IT 6660 Advanced Network Forensics

forensic principles and development of an understanding of the technologies, protocols, laws, regulations, ethics, and procedures for network forensics. Incorporates demonstrations and laboratory exercises covering the identification, acquisition, authentication, preservation, analysis, and reporting of evidence for prosecution purposes.

IT 6780 Secure Coding

lifecycle principles, identifying and mitigating issues in existing applications, and common security issues. Covers the most frequently encountered application security risks and how to address each of them. Includes web applications, mobile applications, and traditional desktop applications.