Cybersecurity, Graduate Certificate

The Graduate Certificate in Cybersecurity at Utah Valley University is a post-baccalaureate program for students who wish to complete advanced studies in the field of cybersecurity. This program is designed to provide students with advanced technical and managerial knowledge of cybersecurity, preparing them for senior technical and leadership roles in the field. Coursework includes a balanced approach, combining critical analysis of cybersecurity theory with hands-on education for essential applied cybersecurity techniques and tools. The program takes two semesters to complete the 18 credits of graduate level courses. Courses include cybersecurity operations, advanced network defense, cybersecurity management, case studies, secure coding, ethical hacking, and the legal and privacy implications of cybersecurity. To be successful, students should have a strong background in technology. Students should have completed undergraduate work in a related field or have applicable work experience. For those who do not meet this requirement, select undergraduate courses are available to provide the foundational knowledge needed. Please contact the academic advisor for more information.

Matriculation Requirements

1. Application for admission to the program.
2. Bachelor's degree required, preferably in Information Systems, Information Security, Information Technology, or Computer Science.
3. 2 years of IT or IT security industry experience (if Bachelor's degree in non-related field).
4. Completion of undergraduate courses in data communication, programming and servers.

Program Requirements

Code	Title	Credit Hours
Total Credit Hours		**18**
Discipline Core Requirements		**12 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
Elective Requirements		**6 Credits**
Complete 6 credits from the following:		6
IT 6660	Advanced Network Forensics (3)	
IT 6740	Advanced Network Defense and Countermeasures (3)	
IT 6760	Case Studies in Cybersecurity (3)	
IT 6770	Cybersecurity Management (3)	
IT 6780	Secure Coding (3)	
or other departmental approved electives		

Graduation Requirements

1. Completion of a minimum of 18 credits.
2. Overall grade point average of 3.0 (B) or above.
3. Residency hours -- minimum of 5 credit hours through course attendance at UVU.
4. Courses and project requirements must be finished within a five-year period. No courses will apply toward graduation which are older than five years.

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 (http://www.uvu.edu/wolverinetrack/).

First Year		
Semester 1		**Credit Hours**
IT 6300	Principles of Cybersecurity	3
IT 6330	Cybersecurity Operations	3
	Credit Hours	**6**

Semester 2		
IT 6350	Law/Ethics/Privacy in Cybersecurity	3
IT 6370	Penetration Testing and Vulnerability Assessment	3
	Credit Hours	**6**
Second Year		
Semester 3		
IT 6370	Penetration Testing and Vulnerability Assessment	3
Elective		3
	Credit Hours	**6**
	Total Credit Hours	**18**

Program Learning Outcomes

1. Clearly explain complex technical cyber security concepts in written and verbal forms.
2. Describe and explain how to mitigate cyber security threats to enterprise, government, and individuals.
3. Explain the role of cyber security in the enterprise and how to integrate cyber security principles into existing processes.
4. Be aware of their responsibility to behave ethically in their professional lives (e.g., clients, customers, employers, society, profession, environment, and community).
5. Have a global perspective on legal and ethical issues surrounding cyber security and technology.