CYBERSECURITY AND INFORMATION SECURITY ADMINISTRATION (ATC)

Advanced Technical Certificate

Career-Technical Program
Interest Areas:
Business Admin. and Management

This Cybersecurity Information Security (INFOSEC) Administration Advanced Technical Certificate program will prepare students for a career in the cybersecurity industry. The technical courses in this certificate program combine both networking concepts and security fundamentals with a focus on best practices required to implement and administer secure network environments. The program integrates knowledge from communication, social sciences, and math with the theory and practice of information technology to prepare students for employment in the industry. It will also provide opportunities for those employed in the information technology field to enhance their knowledge and credentials and advance in their careers.

During the program students are encouraged to work toward a varieinstitutional certificate. Students will graduate with a Cybersecurity Information Security (INFOSEC) Administration Advanced Technical Certificate upon successful completion of this program. Entry-level position responsibilities in cybersecurity include, but are not limited to: maintaining computer network infrastructure and security; securing computer assets connected to the Internet; installing, configuring and securing PC systems and mobile devices; configuring and securing remote access networks; providing technical support and configuring and repairing endpoint devices.

Career opportunities for Cyber Security professionals are varied and immediate. The National Initiative for Cyber Security Education (NICE) has identified dozens of job titles that require security skills. See www.nist.gov (https://www.nist.gov/) and search for Cybersecurity Workforce Framework Resource Center for more information on cybersecurity skills needed today. Additionally, projections are that by the end of the decade, all or nearly all intermediate level computer technical, developmental or implementation careers will require some level of security training.

This is a selective enrollment program. Successful completion of each semester or permission of the instructor is required to continue to the next semester. Successful completion of the technical certificate or permission of the instructor is required for enrollment in the third and fourth semester courses.

For requirements and admission procedures, go to the program website below or contact the Career and Technical Education Advisor at (208) 769-3371.

Contact Information:
Business & Professional Programs Division
Hedlund Building, Room 101
Phone: (208) 769-3226
Program Website (https://www.nic.edu/programs/cybersecurity-and-networking/)

Program Requirements

Course	Title	Credits
Semester 1		
CITE-118	Computer Information Technology Essentials	2
CITE-140	Introduction to Cybersecurity	3
CITE-145	Cybersecurity Law Ethics	3
CITE-152	Networking Essentials	3
ENGL-101	Writing and Rhetoric I	3
Select one of the following:		3-5
MCTE-101	Technical Mathematics	
GEM 3 - A.A.S. Mathematical Ways of Knowing		
	Credits	**17-19**
Semester 2		
CITE-121	Network Support I	3
CITE-122	Network Support I Projects	3
CITE-142	Information Security Fundamentals	3
CITE-155	Linux Essentials	3
COMM-101	Fundamentals of Oral Communication	3
	Credits	**15**
Semester 3		
CITE-165	Linux System Administration	3
CITE-235	Network Security Fundamentals	3
CITE-243	Command Line and Scripting Fundamentals	3
CITE-275	Intrusion Detection/Prevention Systems Fundamentals	3
	Credits	**12**
Semester 4		
CITE-104	Systems Administration I	3
CITE-105	Systems Administration I Projects	3
CITE-237	Ethical Hacking and Systems Defense	3
CITE-258	Cyber Operations	3
Select one of the following:		2-3
ATEC-117	Occupational Relations and Job Search	
CITE-289	Cyber Competitions	
CITE-296	Cybersecurity Internship	
	Credits	**14-15**
	Total Credits	**58-61**

Course Key

GEM | AAS Institutionally Designated | Gateway | Milestone

Program Outcomes

Upon completion of the program, students will be able to:

1. Evaluate various network devices and media and how best to secure them.
2. Determine the factors involved in developing a secure information technology strategy.
3. Describe and identify common security threats and attacks and describe how to safeguard against them.

4. Perform vulnerability assessment on a network.
5. Monitor and analyze multiple sources of data to identify changes in circumstances or events.
6. Access a computer system's security vulnerabilities using appropriate resources.
7. Apply software patches to operating systems and applications.
8. Explain how to use current forensic tools.
9. Use standard software tools to detect attempted security breaches of computer systems. Implement computer network security defenses.
10. Demonstrate sensitivity to and sound judgment on ethical issues as they arise in information security and cyber defense.
11. Demonstrate professionalism through acceptable attitudes, organization and time management skills, and attire.