CYBERSECURITY AND NETWORKING (BTC)

Basic Technical Certificate

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

The Cybersecurity and Networking Basic Technical Certificate will teach students proficiency in basic personal computer and small network implementation. It will provide students with knowledge that will allow them to work with computer networks and build their basic cybersecurity skills. Jobs appropriate for this certification include, but are not limited to, cabling technician, computer network support specialist, customer service and technical support, and computer user support. This certificate prepares students for industry-recognized certification exams. Students can also apply credits towards a Network Security Administration or Computer Information Technology Associate of Applied Science Degree.

Contact Information:
Career & Technical 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 and Ethics	3
CITE-152	Networking Essentials	3
	Credits	**11**
Semester 2		
CITE-121	Network Support I	3
CITE-122	Network Support I Projects	3
CITE-142	Information Security Fundamentals	3
	Credits	**9**
	Total Credits	**20**

Course Key

GEM	AAS Institutionally Designated	Gateway	Milestone

Program Outcomes

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

1. Describe devices and services used to support communications and data networks and the Internet.
2. Evaluate various network devices and media and how best to secure them.
3. Analyze captured network/application traffic.
4. Describe why information security is essential in today's IT environment.
5. Describe common security threats and their ramifications.
6. Use a packet sniffer to capture traffic on a network.
7. Determine the factors involved in developing a secure information security strategy.
8. Describe the basics of cryptography.
9. Differentiate between physical security, disaster recover, and business continuity.
10. Demonstrate appropriate and ethical behavior and good work habits.