
Cybersecurity – Certificate of Achievement

Units: 30

(State Code: 38827; TOP Code: 070800; Academic Plan: C038827D)

The Cybersecurity certificate of achievement prepares students for a career in a sector of technology that is growing rapidly and will continue to grow for the foreseeable future. The curriculum teaches students to recognize threats and procedures to be proactive against cybersecurity threats and/or respond to cybersecurity incidents, how to protect and defend against intrusions through the use of advanced techniques used by cybercriminals, and how to create innovative solutions to prevent hackers from stealing critical information or causing problems for computer networks. Students also learn about the ethics of security and hacking and the geopolitical ramifications of cyber-attacks. The Cybersecurity Certificate is comprised of a group of industry-recognized CompTIA certifications and computer forensics and ethical hacking certification programs which will enhance a student's ability to pursue a career in cybersecurity.

PROGRAM STUDENT LEARNING OUTCOMES

1. Gain an understanding of computer technologies, such as, hardware, software, and networking technologies, as well as troubleshooting, methods of signaling and encoding, interfaces, transmission media, and the most important protocols involved in moving data over a communication network.
2. Understand concepts of cybersecurity, network security, risk assessment, disaster recovery, threat assessment, computer forensics, privacy, and ethics as it relates to security, law, civil compliance, and criminal activity.
3. Gain the skills necessary to apply knowledge of concepts, tools, and procedures to react to cybersecurity incidents and guard against cybersecurity attacks.
4. Understand how hardware, software, and networks interact and how to protect and defend against intrusions using advanced techniques that are used by cybercriminals.
5. Create innovative solutions to prevent hackers from stealing critical information or cause problems for computer networks.
6. Understand the ethical implications of working to protect organizations or countries against a cyberattack.

PROGRAM REQUIREMENTS

Requirements for the Cybersecurity certificate of achievement may be met by completing 30 units of required courses with a grade of "C" or better.

REQUIRED COURSES (30 UNITS)

CS 101	(Formerly CO SCI 103) INTRODUCTION TO COMPUTER SCIENCE	3
OR		
CS 111	(Formerly CO SCI 108) PROGRAMMING IN VISUAL BASIC	
CIS 210	(Formerly COTECH 004) INTRODUCTION TO COMPUTER NETWORKING	3
CIS 212	(Formerly COTECH 012) INTRODUCTION TO COMPUTER-HARDWARE	3
CIS 213	(Formerly COTECH 014) INTRODUCTION TO COMPUTER-SOFTWAREWARE	3
CIS 214	(Formerly CO TECH 015) INTRODUCTION TO NETWORK +	3
CIS 211	(Formerly CO TECH 016) SECURITY+ CERTIFICATION PREPARATION	3
CIS 170	(Formerly CO TECH 031) INTRODUCTION TO ETHICAL HACKING	3
CIS 112	(Formerly CO TECH 018) OPERATING SYSTEMS-BEGINNING LINUX	3
CIS 166	(Formerly CO TECH 029) COMPUTER FORENSICS I	3
CS 119	(Formerly CO SCI 124) PROGRAMMING IN PYTHON	3