CYBER SECURITY

STATEWIDE PROGRAM OF STUDY: CYBER SECURITY

Course	Credits	Class Periods	Grade	Location
Principles of Information Technology	1.0	1	8	Jr High
OR Introduction to Computer Science	1.0	1	9-12	Home Campus
OR Computer Science I	1.0	1	9-12	Home Campus
OR AP Computer Science Principles *Prerequisite: Algebra I*	1.0	1	9-12	Home Campus
OR AP Computer Science A *Prerequisite: Algebra I* *Successful completion of this course awards one advanced math credit and one language other than English credit*	1.0	1	9-12	Home Campus
Cyber Security I & II *Prerequisite: Principles of Information Technology or Introduction to Computer Science or Computer Science I or AP Computer Science Principles or AP Computer Science A*	2.0	2	11-12	MCTC
Practicum in Cyber Security *Prerequisites: Cyber Security I & II*	2.0	2	12	MCTC

CERTIFICATION OPPORTUNITY

- CompTIA Security+

CAREER POSSIBILITIES

- **Chief Information Officer**
- **Cryptographer**
- **IT Security Consultant**
- **IT Security Engineer**
- **Junior IT Auditor/Penetration Tester**
- **Network Administrator**

miller
CAREER & TECHNOLOGY CENTER
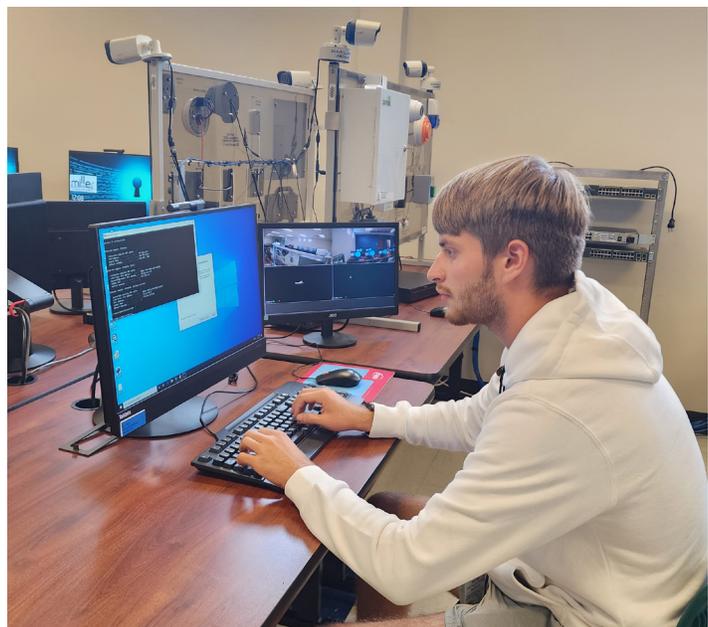
8678V CYBER SECURITY I - FALL SEMESTER
8679V CYBER SECURITY II - SPRING SEMESTER

Grades: 11-12   1 Credit Each Course

Prerequisite: Either Principles of Information Technology or Introduction to Computer Science or Computer Science I or AP Computer Science Principles, or AP Computer Science A.

—

This course provides an understanding of cybersecurity concepts, system vulnerabilities, common cyber-attack mechanisms and tools, intrusion detection systems, and methods to mitigate cybersecurity risks. Simulated and hands-on labs provide experience in various areas including firewall, router, and switch security, cryptography, encryption, VPNs, virtualization, steganography, hashing, security design principles, and social engineering.

8689V PRACTICUM IN CYBER SECURITY

Grade: 12   2 Credits

Prerequisites: Cyber Security I & II

—

This course provides advanced application of previously learned knowledge and skills. Students receive instruction in real-world simulations, tackling security challenges such as ethical hacking, network defense, threat analysis, and data protection. Through collaborative projects, they will gain exposure to industry-standard tools and techniques used to secure computer systems and networks. The course emphasizes problem-solving, critical thinking, and teamwork while preparing students for careers in cybersecurity or further study in the field. By the end of the practicum, students will have built a portfolio of skills and knowledge to advance in cyber defense and IT security roles.

PROGRAM EXPERIENCES

This program provides students knowledge and experience through hands-on lab time, including projects in ethical hacking, cryptography practice, digital forensics, Raspberry Pi projects, and risk management.

Students will also have the opportunity to be exposed to several potential job options within the Cyber industry.

EXPECTATIONS OF STUDENTS

- Ability to learn theory through both lecture and the computer-based lab area.
- Exhibit ability to work independently during lab time.
- Ability to apply learned skills on various simulators including programmable logic controls (PLC), electronics, pneumatics/hydraulics, and computer numerical controls (CNC).