Maryland CTE Programs of Study

Cybersecurity I (2025)

General requirements. This course is recommended for students in Grades 9-12. Students shall be awarded one credit for successfully completing this course. 1

1 General requirements. This course is recommended for students in Grades 9-12. Students shall be awarded one credit for successfully completing this course. 1

Introduction. 2

A Career and technical education instruction provides content aligned with challenging academic standards and relevant technical knowledge and skills for students to further their education and succeed in current or emerging professions. 2.A

B The Digital Technology (DT) Career Cluster focuses on building linkages in IT occupations for entry level, technical, and professional careers related to securing and protecting network systems. 2.B

C The Cybersecurity Career and Technical Education (CTE) Program of Study emphasizes pathways related to securing computer and information networks, including local area networks (LAN), wide area networks (WAN), intranets, extranets, and other data communication systems. 2.C

D The Cybersecurity I course introduces and applies the confidentiality, integrity, and availability (CIA) triad while emphasizing foundational security skills aligned to entry-level certification objectives. Students develop foundational knowledge and skills in computer networking and security. Students learn network architecture as well as processes to secure networks, such as: firewalls, VPNs, encryption, and secure communication protocols. 2.D

E Students will participate in at least two Career-Connected Education and Work-Based Learning experiences in this course, which might include informational interviews or job shadowing relevant to the program of study. 2.E

F Students are encouraged to participate in extended learning experiences through aligned Career and Technical Student Organizations (CTSOs). CTSOs are a cocurricular requirement in the Carl D. Perkins Act, and alignment to CTSO activities is an expectation for CTE programs in the state of Maryland. 2.F

Kn Skip to main content **he student demonstrates the necessary skills for career development, maintenance of employability, and successful completion of course outcomes. The**

student is expected to: 3.A

1. Identify and demonstrate positive work behaviors that enhance employability and job advancement, such as regular attendance, promptness, proper attire, maintenance of a clean and safe work environment, and pride in work. 3.A.1
2. Demonstrate positive personal qualities such as flexibility, open-mindedness, initiative, active listening, and a willingness to learn. 3.A.2
3. Employ effective reading, writing, and technical documentation skills. 3.A.3
4. Solve problems using critical thinking techniques and structured troubleshooting methodologies. 3.A.4
5. Demonstrate leadership skills and collaborate effectively as a team member. 3.A.5
6. Implement safety procedures, including proper handling of hardware and following cybersecurity guidelines. 3.A.6
7. Exhibit an understanding of legal and ethical responsibilities in the IT field, following data privacy laws and best practices for security. 3.A.7
8. Demonstrate time-management skills and the ability to prioritize tasks in a technical setting. 3.A.8

B **The student identifies various career pathways in the information technology field. The student is expected to:** 3.B

1. Develop a career plan that includes the necessary education, certifications, job skills, and experience for specific roles in IT networking. 3.B.1
2. Create a professional resume and portfolio that reflect skills, projects, certifications, and recommendations. 3.B.2
3. Demonstrate effective interview skills for roles in IT and networking. 3.B.3

C **The student develops technology and digital literacy skills. The student is expected to:** 3.C

1. Use technology as a tool for research, organization, communication, and problem-solving. 3.C.1
2. Use digital tools, including computers, mobile devices, collaboration platforms, and cloud services, to access, manage, and create information. 3.C.2
3. Demonstrate proficiency in using emerging and industry-standard technologies, including virtualization tools, network management software, and cybersecurity applications. 3.C.3
4. Understand ethical and legal considerations for technology use, including the principles of data protection, copyright, and responsible technology use. 3.C.4

D **The student integrates core academic skills into cybersecurity practices. The student is expected to:** 3.D

1. Demonstrate the use of clear communication techniques, both written and verbal, that are consistent with industry standards. 3.D.1

Skip to main content

2 Apply mathematical concepts such as binary conversion, subnetting, and data rate calculations in network configuration and troubleshooting. 3.D.2

3 Use scientific principles, such as signal properties and electromagnetic interference, in network design and troubleshooting. 3.D.3

E The student demonstrates the necessary skills to understand and operate hardware and software systems in a secure environment. The student is expected to: 3.E

1 Identify and describe the functions of different computer hardware components, including CPUs, memory, storage, and peripheral devices. 3.E.1

2 Perform basic hardware installation, configuration, and troubleshooting in line with industry standards. 3.E.2

3 Demonstrate the ability to install and configure operating systems, focusing on system updates, patches, and driver installations. 3.E.3

4 Explain the importance of and perform regular maintenance and upgrades on hardware and software systems. 3.E.4

F The student demonstrates the necessary skills to secure and manage network environments. The student is expected to: 3.F

1 Understand basic networking concepts, including IP addressing and network protocols, to prepare for configuration and troubleshooting. 3.F.1

2 Configure and troubleshoot wired and wireless network connections, adhering to industry protocols and standards. 3.F.2

3 Apply fundamental concepts of network security, including firewalls, antivirus software, and network access controls. 3.F.3

4 Demonstrate the ability to set up and secure both home and small business networks, emphasizing cybersecurity best practices. 3.F.4

G The student demonstrates the necessary skills to implement fundamental security practices for protecting devices and data. The student is expected to: 3.G

1 Describe common security threats, vulnerabilities, and attacks, including phishing, malware, and social engineering. 3.G.1

2 Identify basic data security measures, such as data encryption, secure passwords, and data backup strategies. 3.G.2

3 Demonstrate knowledge of access controls, user permissions, and authentication methods for protecting information systems. 3.G.3

4 Describe the core cybersecurity frameworks including the CIA Triad, Defense in Depth, and Authentication, Authorization, and Accounting (AAA) and how they influence cybersecurity policies and practices. 3.G.4

5 Conduct basic risk assessments and apply strategies to mitigate potential cybersecurity threats. 3.G.5

Skip to main content

H The student demonstrates the necessary skills to manage and troubleshoot technical issues in a professional environment. The student is expected to: 3.H

1. Identify and troubleshoot common hardware, software, and network issues using systematic diagnostic methods. 3.H.1
2. Document technical issues, troubleshooting steps, and solutions in line with industry documentation practices. 3.H.2
3. Demonstrate the use of technical support tools, such as remote assistance, for resolving user issues. 3.H.3
4. Apply customer service skills in technical support scenarios, practicing professional communication and problem-solving techniques. 3.H.4

I The student demonstrates the necessary skills to implement secure baseline configurations on endpoints. The student is expected to: 3.I

1. Harden operating systems (local policies, secure services, update/patch cadence) and configure endpoint protection (AV/EDR). 3.I.1
2. Apply least-privilege and standard user policies; manage local groups and permissions. 3.I.2
3. Configure basic logging and review event logs to identify suspicious activity. 3.I.3
4. Create and test a simple data backup/restore plan for endpoints. 3.I.4

J The student demonstrates the necessary skills in computational thinking and basic scripting to automate security tasks. The student is expected to: 3.J

1. Use decomposition, pattern recognition, abstraction, and algorithms to plan solutions. 3.J.1
2. Write and run simple scripts (e.g., Python, Bash, or PowerShell) to parse logs, hash files, or query system info. 3.J.2
3. Use regular expressions and command-line tools to filter and transform data. 3.J.3
4. Document scripts with comments and basic error handling. 3.J.4

K The student demonstrates AI literacy for cybersecurity contexts. The student is expected to: 3.K

1. Explain what modern AI/ML systems do (at a high level) and their limitations (e.g., hallucinations, bias, data leakage). 3.K.1
2. Use AI tools responsibly for research and drafting (prompt hygiene, citation, privacy-safe inputs). 3.K.2
3. Identify security risks of AI systems (e.g., prompt injection, model poisoning, data exfiltration) in age-appropriate scenarios. 3.K.3

L The student demonstrates the necessary skills to monitor emerging cybersecurity roles and technologies. The student is expected to: 3.L

1. Track current industry news and summarize quarterly trends (e.g., AI, cloud, OT). 3.L.1
2. Map evolving roles to skills/credentials (e.g., Security Operations, GRC, Cloud Security, OT Security) and update an individual learning plan. 3.L.2

Skip to main content

M **The student demonstrates the necessary skills to participate in practical, challenge-based cybersecurity activities. The student is expected to:** 3.M

1. Complete beginner capture-the-flag (CTF) labs (e.g., password cracking basics, log triage, web challenges) in a safe, isolated environment. 3.M.1
2. Reflect on problem-solving approaches and document write-ups in a portfolio. 3.M.2
3. Engage with recognized gamified platforms (e.g., SANS BootUp CTF, NetWars Skill Quest) or equivalent, as available and approved. 3.M.3

N **The student demonstrates the necessary skills to install, configure, and maintain common operating systems and devices. The student is expected to:** 3.N

1. Perform basic OS installation or imaging and initial configuration (accounts, updates, drivers). 3.N.1
2. Configure user profiles and local authentication settings on Windows, Linux, or macOS. 3.N.2
3. Connect and troubleshoot common peripherals and printers at a basic level. 3.N.3
4. Describe safe tool use and ESD precautions during basic hardware service. 3.N.4