Maryland
STATE DEPARTMENT OF EDUCATION

Program of Study Guide: Cybersecurity - DRAFT

Comprehensive guidelines and course standards for the Cybersecurity pathway

Office of College and Career Readiness

July 2025

MARYLAND STATE DEPARTMENT OF EDUCATION

Carey M. Wright, Ed.D.
State Superintendent of Schools

Tenette Smith, Ed.D.
Deputy State Superintendent
Office of Teaching and Leading

Richard W. Kincaid
Assistant State Superintendent
Division of College and Career Pathways

Wes Moore
Governor

MARYLAND STATE BOARD OF EDUCATION

Joshua L. Michael, Ph.D.
President, Maryland State Board of Education

Monica Goldson, Ed.D. (Vice President)

Chuen-Chin Bianca Chang, MSN, PNP, RN-BC

Kenny Clash

Clarence C. Crawford (President Emeritus)

Abhiram Gaddam (Student Member)

Susan J. Getty, Ed.D.

Nick Greer

Dr. Irma E. Johnson

Kim Lewis, Ed.D.

Dr. Joan Mele-McCarthy, D.A., CCC-SLP

Rachel L. McCusker

Xiomara V. Medina, M.Ed.

Samir Paul, Esq.

Table of Contents

Document Control Information

Title:	Digital Technology: Cybersecurity CTE Program Guide
Security Level:	Unclassified – For Official Use Only
File Name:	Cybersecurity_Program_Guide

DOCUMENT HISTORY

Document Version	Date	Summary of Change
1.0	October 2024	Initial Document

Purpose

The purpose of this document is to communicate the required Career and Technical Education (CTE) academic standards for the Cybersecurity Program of Study. The academic standards in this document are theoretical and performance based. The standards contain content from multiple state departments of education, the College Board, and the Computer Science Teachers Association (CSTA) and have been reviewed and vetted by members of the Maryland business and industry community.

In addition to academic standards, the Maryland State Department of Education (MSDE) has incorporated into this document Labor Market Information (LMI) definitions and explanations for the Program of Study; program aligned Industry Recognized Credentials; and Work-Based Learning resources and requirements by course level. This document is intended for use by educational administrators and practitioners. A similar document is available for each state-approved CTE Program of Study.

Standards Sources

These sources collectively guide the standards for Cybersecurity I-IV Course Standards, ensuring alignment with national education frameworks, industry-recognized certifications, and security standards essential for developing a skilled cybersecurity workforce.

1. **NICE Framework (National Initiative for Cybersecurity Education)**
   A. **Source:** National Institute of Standards and Technology (NIST)
   B. **Purpose:** The NICE Framework categorizes cybersecurity work roles and defines specific tasks, skills, and knowledge needed for cybersecurity professionals. It's designed to support cybersecurity education and workforce development across various career levels.
   C. **Relevance:** The NICE Framework provides a clear structure for identifying the skills and competencies necessary for students in both foundational and advanced cybersecurity courses. Standards for Cybersecurity I and II align with foundational roles, emphasizing threat detection, incident response, and network security, while Cybersecurity III and IV align with advanced competencies in penetration testing, digital forensics, and security management.
   D. **Access:** NIST NICE Framework: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework

2. **CompTIA Cybersecurity Certifications**
   A. **Source:** Computing Technology Industry Association (CompTIA)
   B. **Purpose:** CompTIA certifications (A+, Network+, Security+, CySA+, PenTest+) provide industry-standard benchmarks for technical skills in IT and cybersecurity, ensuring alignment with current job roles and practices in the field.
   C. **Relevance:** Cybersecurity I and II course standards align with CompTIA A+, Network+, and Security+ certifications, ensuring students gain foundational IT skills, networking knowledge, and an understanding of security fundamentals. Cybersecurity III and IV align with advanced certifications such as CySA+, PenTest+, and CEH, helping students develop competencies in threat analysis, penetration testing, and security operations.
   D. **Access:** CompTIA Certifications: https://www.comptia.org/certifications

3. **National Career Cluster Framework - Digital Technology Cluster**
   A. **Source:** Advance CTE
   B. **Purpose:** The National Career Cluster Framework provides a structure for organizing career and technical education (CTE) around 14 clusters, including Digital Technology, to promote skill development for specific industry sectors.
   C. **Relevance:** The Digital Technology Cluster and its Network Systems and Cybersecurity sub-cluster emphasize the skills needed for careers in network setup, administration, and security. This framework guides the development of Cybersecurity I-IV standards, ensuring that students gain a well-rounded education in network systems, cybersecurity fundamentals, and advanced security measures.
   D. **Access:** Advance CTE Career Clusters: https://careertech.org/career-clusters

4. **National Institute for Standards and Technology (NIST) Cybersecurity Framework**
   A. **Source:** National Institute of Standards and Technology (NIST)
   B. **Purpose:** The NIST Cybersecurity Framework provides a comprehensive set of guidelines for managing and reducing cybersecurity risks in critical infrastructure.

C. **Relevance:** This framework supports standards in Cybersecurity III and IV, where students learn to apply cybersecurity risk management, incident response, and recovery protocols. The framework's guidelines reinforce students' skills in aligning security measures with real-world risk management needs, critical for advanced cybersecurity roles.
D. **Access:** [NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

5. **International Organization for Standardization (ISO) - ISO/IEC 27001**
   A. **Source:** International Organization for Standardization (ISO)
   B. **Purpose:** ISO/IEC 27001 outlines requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).
   C. **Relevance:** Standards for Cybersecurity IV leverage ISO/IEC 27001 to familiarize students with information security management practices, relevant for advanced roles in cybersecurity governance and compliance. Students learn to develop security policies and frameworks, supporting preparation for industry certifications like PenTest+ and CEH.
   D. **Access:** [ISO/IEC 27001 Information Security](https://www.iso.org/isoiec-27001-information-security.html)

6. **National Centers of Academic Excellence in Cybersecurity (CAE-C) Knowledge Units**
   A. **Source:** National Security Agency (NSA) and Department of Homeland Security (DHS)
   B. **Purpose:** The CAE-C Knowledge Units outline specific knowledge and skills that academic programs need to include to be recognized as Centers of Academic Excellence in Cybersecurity.
   C. **Relevance:** Cybersecurity III and IV course standards align with CAE-C Knowledge Units to ensure students gain comprehensive cybersecurity skills recognized at the national level. Advanced concepts such as digital forensics, ethical hacking, and cybersecurity governance in Cybersecurity IV correspond with CAE-C requirements, preparing students for both college-level programs and workforce entry.
   D. **Access:** CAE-C Knowledge Units: https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-resources/knowledge-units/

Course Descriptions

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. Information security analysts plan and carry out security measures to protect an organization's computer networks and systems.

Cybersecurity & Infrastructure Security Agency

Course Level	Course Information	Description
Required Core: Course 1	Cybersecurity I SCED: <XX> Grades: 9-12 Prerequisite: None Credit: 1	Cybersecurity I provides an introduction to the foundational principles of network systems and cybersecurity, emphasizing the essential skills needed to set up, maintain, and protect digital communication networks.
Required Core: Course 2	Cybersecurity II SCED: <XX> Grades: 10-12 Prerequisite: Cybersecurity I Credit: 1	Cybersecurity II builds upon the foundational knowledge gained in Cybersecurity I, advancing students' skills in securing and managing complex network environments. The course focuses on configuring, administering, and troubleshooting network infrastructure, with an emphasis on implementing security protocols and mitigating cybersecurity risks.
Optional Flex: Course 1	Cybersecurity III SCED: <XX> Grades: 11-12 Prerequisite: Cybersecurity I & II Credit: 1	Cybersecurity III advances students' skills in network systems and cybersecurity, focusing on more complex topics in network security, threat mitigation, and digital forensics. Building on foundational knowledge from Cybersecurity I and II, students will explore advanced techniques in network monitoring, vulnerability assessment, and penetration testing.

Course Level	Course Information	Description
Optional Flex: Course 2	Career Connected Learning I SCED: <XX> Grades: 11-12 Prerequisite: Cybersecurity I and II Credit: 1	This flexible, work-based learning course introduces students to real-world applications of classroom knowledge and technical skills through on-the-job experiences and reflective practice. Students engage in career exploration, skill development, and professional networking by participating in youth apprenticeships, registered apprenticeships, pre-apprenticeships, internships, capstone projects, or other approved career-connected opportunities. Variable credit (1–3) accommodates the required on-the-job training hours and related instruction. By integrating industry standards, employability skills, and personalized learning goals, Career Connected Learning I equips students to make informed career decisions, develop a professional portfolio, and build a strong foundation for success in postsecondary education, training, or the workforce.
Optional Flex: Course 3	Career Connected Learning II SCED: <XX> Grades: 11-12 Prerequisite: Career Connected Learning I Credit: 1	Building on the foundational experiences of Career Connected Learning I, this advanced work-based learning course provides students with deeper on-the-job practice, leadership opportunities, and refined career exploration. Students continue to enhance their technical and professional skills, expanding their industry networks and aligning personal goals with evolving career interests. Variable credit (1–3) remains aligned with the required training hours and related instruction. Through elevated responsibilities and skill application, Career Connected Learning II prepares students to confidently transition into higher-level postsecondary programs, apprenticeships, or the workforce.

Dual Enrollment and Career Connected Learning Experiences Must be Aligned to the CTE Core.

Industry-Recognized Credentials and Work-Based Learning

Industry-Recognized Credentials – The standards in this document are aligned to the following certifications:
By the end of Cybersecurity I: CompTIA A+ **By the end of Cybersecurity II:** CompTIA Network+ and CompTIA Security+ **By the end of Cybersecurity III:** Optional Credentials (via the Flex Course options): CompTIA CySA+ (Cybersecurity Analyst)

Work-based Learning Resources		
Cybersecurity I: **Career Awareness**	**Cybersecurity II:** **Career Preparation**	**Flex Courses:** **Career Preparation**
• Industry Visits • Guest Speakers • Participation in Career and Technical Student Organizations • Postsecondary Visits – Program Specific Site Tours • Mock Interviews	• All of Career Awareness plus the following: • Job Shadow • Paid and Unpaid Internships	• Paid and Unpaid Internships • Apprenticeships

Labor Market Information: Definitions and Data

Labor market information (LMI) plays a crucial role in shaping Career and Technical Education (CTE) programs by providing insights into industry demands, employment trends, and skills gaps. This data helps education leaders assess the viability of existing programs and identify opportunities for new offerings. By aligning CTE programs with real-time labor market needs, schools can better prepare students for in-demand careers and ensure that resources are effectively utilized to support pathways that lead to high-quality, sustainable employment.

Standard Occupational Code (SOC) and Aligned Industry:

Indicator	Definition	Pathway Labor Market Data
High Wage[1]	Those occupations that have a 25th percentile wage equal to or greater than the most recent MIT Living Wage Index for one adult in the state of Maryland, and/or leads to a position that pays at least the median hourly or annual wage for the DC-VA-MD-WV Metropolitan Statistical Area (MSA). *Note: A 25th percentile hourly wage of $24.74 or greater is required to meet this definition.*	**Standard Occupational Code:** 15-1212: Information Security Analysts **Hourly Wage/Annual Salary:** 25th Percentile: $32.25 / $67,070.00 50th Percentile: $64.49 / $134,139.00 75th Percentile: $96.74 / $201.219.00
High Skill	Those occupations located within the DC-VA-MD-WV Metropolitan Statistical Area (MSA) with the following education or training requirements: completion of an apprenticeship program; completion of an industry-recognized certification or credential; associate's degree, bachelor's degree, or higher.	**Typical Entry-Level Education:** Information security analysts typically need a bachelor's degree in a computer science field, along with related work experience. Employers may prefer to hire analysts who have professional certifications and work experience, such as an internship or apprenticeship.
In-Demand	Annual growth plus replacement, across all Maryland occupations, is 405 openings between 2024-2029.	**Annual Openings:**

[1] Living Wage Calculator: https://livingwage.mit.edu/states/24

Labor Market Information Data Source

Lightcast Q4 2024 Data Set. Lightcast occupation employment data are based on final Lightcast industry data and final Lightcast staffing patterns. Wage estimates are based on Occupational Employment Statistics (QCEW and Non-QCEW Employees classes of worker) and the American Community Survey (Self-Employed and Extended Proprietors). Occupational wage estimates are also affected by county-level Lightcast earnings by industry. Foundational data for the state of Maryland is collected and reported by the Maryland Department of Labor.

Methodology for High Wage Calculations

To combine labor market data across multiple Standard Occupational Classifications (SOCs), a weighted average approach was used to ensure accurate representation of the marketplace. Median wages for each SOC were weighted based on their respective employment levels, reflecting the relative demand for each occupation. This method ensures that occupations with higher employment contribute proportionately to the overall wage calculation. Additionally, job openings from all relevant SOCs were summed to determine the total projected demand. For example, if Mechanical Engineers account for 67% of total employment and Electrical Engineers for 33%, their respective wages are weighted accordingly, and job openings are aggregated to provide a comprehensive view of labor market opportunities. This approach delivers a balanced and accurate representation of both wages and employment demand for the program.

Methodology for In-Demand Calculations

The baseline for annual job openings, taking into account new positions and replacement positions, was determined by taking the average of all annual job openings between 2024 and 2029 across all 797 career sectors at the 5-digit SOC code level. For the 2024-2029 period, average job openings (growth + replacement) is 405.

Course Standards: Cybersecurity I

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

2. **Introduction.**
   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.

   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.

   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.

   D. The Cybersecurity I course develops students' foundational knowledge and skills in computer networking and security. Students learn to network architecture as well as processes to secure networks, such as: firewalls, VPNs, encryption, and secure communication protocols.

   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.

   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.

3. **Knowledge and Skills.**
   A. **The student demonstrates the necessary skills for career development, maintenance of employability, and successful completion of course outcomes. The student is expected to:**
      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.
      2. Demonstrate positive personal qualities such as flexibility, open-mindedness, initiative, active listening, and a willingness to learn.
      3. Employ effective reading, writing, and technical documentation skills.
      4. Solve problems using critical thinking techniques and structured troubleshooting methodologies.
      5. Demonstrate leadership skills and collaborate effectively as a team member.
      6. Implement safety procedures, including proper handling of hardware and following cybersecurity guidelines.
      7. Exhibit an understanding of legal and ethical responsibilities in the IT field, following data privacy laws and best practices for security.
      8. Demonstrate time-management skills and the ability to prioritize tasks in a technical setting.

   B. **The student identifies various career pathways in the information technology field. The student is expected to:**
      1. Develop a career plan that includes the necessary education, certifications, job skills, and experience for specific roles in IT networking.
      2. Create a professional resume and portfolio that reflect skills, projects, certifications, and recommendations.
      3. Demonstrate effective interview skills for roles in IT and networking.

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

   D. **The student integrates core academic skills into cybersecurity practices. The student is expected to:**
      1. Demonstrate the use of clear communication techniques, both written and verbal, that are consistent with industry standards.
      2. Apply mathematical concepts such as binary conversion, subnetting, and data rate calculations in network configuration and troubleshooting.
      3. Use scientific principles, such as signal properties and electromagnetic interference, in network design and troubleshooting.

E. **The student demonstrates the necessary skills to understand and operate hardware and software systems in a secure environment. The student is expected to:**
   1. Identify and describe the functions of different computer hardware components, including CPUs, memory, storage, and peripheral devices.
   2. Perform basic hardware installation, configuration, and troubleshooting in line with industry standards.
   3. Demonstrate the ability to install and configure operating systems, focusing on system updates, patches, and driver installations.
   4. Explain the importance of and perform regular maintenance and upgrades on hardware and software systems.

F. **The student demonstrates the necessary skills to secure and manage network environments. The student is expected to:**
   1. Understand basic networking concepts, including IP addressing, subnetting, and network protocols, to prepare for configuration and troubleshooting.
   2. Configure and troubleshoot wired and wireless network connections, adhering to industry protocols and standards.
   3. Apply fundamental concepts of network security, including firewalls, antivirus software, and network access controls.
   4. Demonstrate the ability to set up and secure both home and small business networks, emphasizing cybersecurity best practices.

G. **The student demonstrates the necessary skills to implement fundamental security practices for protecting devices and data. The student is expected to:**
   1. Describe common security threats, vulnerabilities, and attacks, including phishing, malware, and social engineering.
   2. Implement basic data security measures, such as data encryption, secure passwords, and data backup strategies.
   3. Demonstrate knowledge of access controls, user permissions, and authentication methods for protecting information systems.
   4. Conduct basic risk assessments and apply strategies to mitigate potential cybersecurity threats.

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

l. **The student integrates core academic skills into cybersecurity practices. The student is expected to:**
   1. Demonstrate clear communication techniques, both written and verbal, consistent with industry standards.
   2. Apply mathematical concepts such as binary conversion, subnetting, and data rate calculations in network configuration and troubleshooting.
   3. Use scientific principles, such as signal properties and electromagnetic interference, in network design and troubleshooting.

Course Standards: Cybersecurity II

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

2. **Introduction.**
   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.

   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.

   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.

   D. The Cybersecurity II course delves into advanced networking concepts, such as subnetting, routing, VPNs, and network security protocols, and students will learn to apply vulnerability scanning, risk assessment, and incident response strategies to protect against unauthorized access and data breaches.

   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.

   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.

3. Knowledge and Skills.
   A. **The student demonstrates the necessary skills for career development, maintenance of employability, and successful completion of course outcomes. The student is expected to:**
      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.
      2. Demonstrate positive personal qualities such as flexibility, open-mindedness, initiative, active listening, and a willingness to learn.
      3. Employ effective reading, writing, and technical documentation skills.
      4. Solve problems using critical thinking techniques and structured troubleshooting methodologies.
      5. Demonstrate leadership skills and collaborate effectively as a team member.
      6. Implement safety procedures, including proper handling of hardware and following cybersecurity guidelines.
      7. Exhibit an understanding of legal and ethical responsibilities in the IT field, following data privacy laws and best practices for security.
      8. Demonstrate time-management skills and the ability to prioritize tasks in a technical setting.

   B. **The student identifies various career pathways in the information technology field. The student is expected to:**
      1. Develop a career plan that includes the necessary education, certifications, job skills, and experience for specific roles in IT networking.
      2. Create a professional resume and portfolio that reflect skills, projects, certifications, and recommendations.
      3. Demonstrate effective interview skills for roles in IT and networking.

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

   D. **The student integrates core academic skills into networking practices. The student is expected to:**
      1. Demonstrate the use of clear communication techniques, both written and verbal, that are consistent with industry standards.
      2. Apply mathematical concepts such as binary conversion, subnetting, and data rate calculations in network configuration and troubleshooting.
      3. Use scientific principles, such as signal properties and electromagnetic interference, in network design and troubleshooting.

E. **The student demonstrates the necessary skills to configure, manage, and troubleshoot complex network infrastructures. The student is expected to:**
   1. Design and implement network topologies and infrastructures, including LANs, WANs, and VPNs, to support secure and efficient data communication.
   2. Configure and troubleshoot routing and switching devices, such as routers and managed switches, according to industry standards.
   3. Utilize subnetting, IP addressing, and network protocols (TCP/IP, DNS, DHCP) to design secure network configurations.
   4. Apply techniques for optimizing network performance and securing network traffic.

F. **The student demonstrates the necessary skills to secure network devices and manage network security protocols. The student is expected to:**
   1. Implement network security controls, such as firewalls, intrusion detection/prevention systems (IDS/IPS), and secure network protocols (e.g., HTTPS, SSL/TLS).
   2. Configure and troubleshoot virtual private networks (VPNs) and other remote access solutions to protect data transmission.
   3. Demonstrate knowledge of wireless security settings, including encryption standards (WPA2, WPA3) and access control.
   4. Monitor network activity and logs to detect and respond to security threats.

G. **The student demonstrates the necessary skills to assess and mitigate cybersecurity threats and vulnerabilities. The student is expected to:**
   1. Identify and analyze security vulnerabilities in network systems using vulnerability scanning tools and penetration testing methods.
   2. Conduct risk assessments and apply best practices for risk mitigation, including patch management, configuration management, and security policies.
   3. Explain and implement access control models, such as role-based access control (RBAC), and multi-factor authentication (MFA).
   4. Perform security audits and apply remediation strategies to strengthen the security posture of network environments.

H. **The student demonstrates the necessary skills to implement organizational security practices and procedures. The student is expected to:**
   1. Create and enforce security policies, procedures, and incident response plans based on organizational needs.
   2. Explain and implement data protection strategies, including data classification, encryption, and secure disposal methods.
   3. Apply principles of social engineering awareness and conduct training to enhance security culture within an organization.
   4. Demonstrate an understanding of regulatory compliance and privacy laws, such as GDPR and HIPAA, and their impact on cybersecurity practices.

I. **The student integrates core academic skills into advanced cybersecurity practices. The student is expected to:**
   1. Demonstrate effective communication skills in documenting and reporting security incidents and resolutions.
   2. Apply advanced mathematical concepts, including probability and statistics, for analyzing network traffic patterns and threat data.
   3. Use scientific and forensic principles to investigate and analyze security incidents in digital systems.

Course Standards: Cybersecurity III

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

2. **Introduction.**
   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.

   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.

   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.

   D. The Cybersecurity III course emphasizes the use of security information and event management (SIEM) tools, network behavior analysis, and ethical hacking practices to protect against sophisticated cyber threats. Students will also gain experience in incident response and risk management, learning to apply cybersecurity frameworks and regulatory standards..

   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.

   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.

3. Knowledge and Skills.
   A. **The student demonstrates the necessary skills for career development, maintenance of employability, and successful completion of course outcomes. The student is expected to:**
      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.
      2. Demonstrate positive personal qualities such as flexibility, open-mindedness, initiative, active listening, and a willingness to learn.
      3. Employ effective reading, writing, and technical documentation skills.
      4. Solve problems using critical thinking techniques and structured troubleshooting methodologies.
      5. Demonstrate leadership skills and collaborate effectively as a team member.
      6. Implement safety procedures, including proper handling of hardware and following cybersecurity guidelines.
      7. Exhibit an understanding of legal and ethical responsibilities in the IT field, following data privacy laws and best practices for security.
      8. Demonstrate time-management skills and the ability to prioritize tasks in a technical setting.

   B. **The student identifies various career pathways in the information technology field. The student is expected to:**
      1. Develop a career plan that includes the necessary education, certifications, job skills, and experience for specific roles in IT networking.
      2. Create a professional resume and portfolio that reflect skills, projects, certifications, and recommendations.
      3. Demonstrate effective interview skills for roles in IT and networking.

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

   D. **The student integrates core academic skills into networking practices. The student is expected to:**
      1. Demonstrate the use of clear communication techniques, both written and verbal, that are consistent with industry standards.
      2. Apply mathematical concepts such as binary conversion, subnetting, and data rate calculations in network configuration and troubleshooting.
      3. Use scientific principles, such as signal properties and electromagnetic interference, in network design and troubleshooting.

E. **The student demonstrates the necessary skills to perform advanced network and system security monitoring. The student is expected to:**
   1. Implement and configure security information and event management (SIEM) tools to monitor and analyze network traffic for potential security threats.
   2. Use network monitoring tools and techniques to detect, respond to, and investigate unusual or unauthorized activity.
   3. Configure alerts and incident logging procedures to support security operations.
   4. Perform network behavior analysis to identify anomalies and potential threats.

F. **The student demonstrates the necessary skills to conduct vulnerability assessments and penetration testing. The student is expected to:**
   1. Plan and execute vulnerability assessments using tools like Nessus, Nmap, or OpenVAS, documenting and reporting findings.
   2. Explain and apply methodologies for penetration testing, including reconnaissance, scanning, and exploitation.
   3. Develop skills in ethical hacking techniques to identify and mitigate security vulnerabilities.
   4. Evaluate and implement remediation actions based on vulnerability assessment reports and best practices in cybersecurity.

G. **The student demonstrates the necessary skills to manage incident response and recovery procedures. The student is expected to:**
   1. Describe and apply incident response processes, including preparation, detection, containment, eradication, recovery, and post-incident analysis.
   2. Utilize digital forensics tools to collect, analyze, and preserve evidence in response to cybersecurity incidents.
   3. Coordinate and document incident handling procedures, creating post-incident reports with recommended improvements.
   4. Apply disaster recovery and business continuity planning practices to ensure data integrity and operational resilience.

H. **The student demonstrates the necessary skills to assess and apply organizational security controls and compliance standards. The student is expected to:**
   1. Identify and interpret industry regulations and compliance standards, such as PCI-DSS, GDPR, and HIPAA, and apply appropriate security controls.
   2. Implement security frameworks (such as NIST or ISO/IEC 27001) to establish organizational cybersecurity policies and procedures.
   3. Develop risk management strategies that assess and mitigate potential business impacts of security threats.
   4. Conduct audits to ensure compliance with organizational policies and regulatory requirements, documenting any corrective actions.

I. **I. The student integrates core academic skills into advanced cybersecurity practices. The student is expected to:**
   1. Demonstrate advanced technical communication skills in documenting complex cybersecurity processes and protocols.
   2. Apply statistical analysis to evaluate and interpret security data from logs, alerts, and other monitoring tools.
   3. Use principles of digital forensics to analyze and reconstruct events related to security incidents.

Course Standards: Career Connected Learning I and II

Career connected learning is an educational approach that integrates classroom instruction with real-world experiences, enabling high school students to explore potential careers and develop relevant skills before graduation. By participating in work-based learning opportunities—such as apprenticeships, internships, capstone projects, and school-based enterprises—students apply academic concepts in authentic settings, gain practical industry knowledge, and build professional networks. This hands-on engagement helps students connect their studies to future career paths, strengthens their problem-solving and communication skills, and supports a smoother transition into college, vocational programs, or the workforce.

All Career and Technical Education Programs of Study include aspects of work-based learning, and almost all of the programs include two Career Connected Learning (CCL) courses. Below are the course descriptions for CCL I and CCL II. The CCL standards can be found via this link: