Cybersecurity (ATC)

HIGH WAGE
DC CAREER AND TECHNICAL EDUCATION

HIGH SKILL
DC CAREER AND TECHNICAL EDUCATION

IN-DEMAND
DC CAREER AND TECHNICAL EDUCATION

Updated January 17, 2022

Office of the State Superintendent of Education
Postsecondary and Career Education Division
Career and Technical Education Department

Christina Grant, Ed.D.
State Superintendent of Education

Antoinette Mitchell, Ph.D.
Assistant Superintendent, Postsecondary and Career Education

Kilin Boardman-Schroyer
Deputy Assistant Superintendent, Postsecondary and Career Education

Richard W. Kincaid
State Director, Career and Technical Education

The purpose of this document is to communicate the required Career and Technical Education (CTE) academic standards for the Cybersecurity. The academic standards in this document are theoretical and performance based. The standards contain content from Colorado, Maryland, Tennessee, and Texas and were validated by D.C. business and industry partners. All content is used with permission.
In addition to academic standards, OSSE 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.

Updated January 17, 2022

Cybersecurity (ATC)

Table of Contents

Course Descriptions: Cybersecurity

Course Level	Course Information	Description
Level I	**Foundations of Cybersecurity** **OSSEID:** 5110601-1 **Grades:** 9-12 **Prerequisite:** None **Credit:** 1	In the Foundations of Cybersecurity course, students will develop the knowledge and skills needed to explore fundamental concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will review and explore security policies designed to mitigate risks. The skills obtained in this course prepare students for additional study in cybersecurity. A variety of courses are available to students interested in this field. Foundations of Cybersecurity may serve as an introductory course in this field of study.
Level II	**Internetworking Technologies** **OSSEID:** 5110602-1 **Grades:** 10-12 **Prerequisite:** Foundations of Cybersecurity **Credit:** 1	The Internetworking Technologies course is normally comprised of the courses called Cisco CCNA R&S: Introduction to Networks (CCNA 1) and Cisco CCNA R&S: Routing and Switching Essentials (CCNA 2). The course introduces the concept of networking, using various analogies to help the student understand the movement of packets throughout the Internet, and the protocol standards used. The Routing and Switching course moves the student into the theory of “moving packets.” The concepts of routing and switching “packets” to the correct destination is covered, and how a network administrator.
Level III	**Digital Forensics** **OSSEID:** 5110603-1 **Grades:** 11-12 **Prerequisite:** Internetworking Technologies **Credit:** 1	Digital Forensics is an evolving discipline concerned with analyzing anomalous activity on computers, networks, programs, and data. As a discipline, it has grown with the emergence of a globally-connected digital society. As computing has become more sophisticated, so too have the abilities of malicious agents to access systems and private information. By evaluating prior incidents, digital forensics professionals have the ability to investigate and craft appropriate responses to disruptions to corporations, governments, and individuals. Whereas cybersecurity takes a proactive approach to information assurance to minimize harm, digital forensics takes a reactive approach to incident response.
Level IV	**Cybersecurity Capstone** **OSSEID:** 5110604-1 **Grades:** 12 **Prerequisite:** Digital Forensics **Credit:** 1	In the Cybersecurity Capstone course, students will develop the knowledge and skills needed to explore advanced concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will develop security policies to mitigate risks. The skills obtained in this course

		prepare students for additional study toward industry certification. A variety of courses are available to students interested in the cybersecurity field. Cybersecurity Capstone may serve as a culminating course in this field of study.

Industry Certifications

At the end of Networking II:
Cisco Certified Entry Networking Technician (CCENT)
CompTIA A+
CompTIA Network+

Work-Based Learning Examples and Resources

Level I Course	Level II Course	Level III Course	Level IV Course
Career Exploration Industry Visits Guest Speakers Participate in a CTSO	**Career Awareness** *All of Level I, plus:* Postsecondary Visits Program-Specific Site Tours Mock Interviews	**Career Preparation** *All of Level I and II, plus:* Job Shadow Paid/Unpaid Internships	**Career Preparation** Paid/Unpaid Internships Apprenticeships

Several resources are available to help instructors meet the Level I and Level II WBL requirements, including:

Career Coach DC (http://careercoachdc.emsicc.com). Online site designed to help students find and connect to a career pathway by providing the most current local data on wages, employment, job postings, and associated education and training. The resource includes a Career Assessment for students.

Nepris (https://dc.nepris.com/). Connects educators and learners with a network of industry professionals virtually, bringing real-world relevance and career exposure to all students. Nepris also provides a skills-based volunteering platform for business and industry professionals to extend their educational outreach.

Virtual Job Shadow (https://virtualjobshadow.com). Provides interactive tools which empower students to discover, plan, and pursue their dreams. Rich video library presents a “day in the life of” view for thousands of occupations.

Labor Market Information Definitions and Data

Career and Technical Education programs of study in the District of Columbia must meet at least one of the High Wage, High Skill, and In-Demand definitions below to be considered appropriate for our students and the regional labor market. These definitions were created in collaboration with Career and Technical Education leaders from District of Columbia LEA's, the University of the District of Columbia Community College, and national guidance from Research Triangle International (RTI) and Education Northwest. Additionally, previous work was consulted from researchers at MIT's Labor Wage Index Project and the DC CTE Task Force's 2012 Strategic Plan for the District of Columbia.

Indicator	Definition	Data for the Networking Program of Study (source: EMSI, August 2021)
High Wage	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 District of Columbia, and/or leads to a position that pays at least the median hourly or annual wage for the Washington, DC, metropolitan statistical area. *Note: A 25th percentile hourly wage of $20.49 or greater is required to meet this definition.*	**Standard Occupational Code (SOC):** 15-1241.00 Computer Network Architects 15-1244.00 Network and Computer Systems Administrators **Hourly Wages** **25th Percentile:** $33.97 **50th Percentile:** $57.23 **75th Percentile:** $84.10
High Skill	Those occupations located within the Washington, DC, metropolitan statistical area with the following education or training requirements: completion of an apprenticeship program; completion of an industry-recognized certification or credential; associate's degree, or higher.	**Typical Entry-Level Education:** Bachelor's degree
In-Demand	Those occupations in the Washington, DC, metropolitan statistical area having more than the median number of total **(growth plus replacement)** annual openings over a five-year period. *Note: An occupation is required to have an annual growth plus replacement rate of 105 openings, or greater, between 2020-25 to meet this definition.*	**Annual Openings:** 847

Model Six-Year Plan: Cybersecurity

College: University of the District of Columbia Community College
Program/CIP:
Plan:

Entity: Office of the State Superintendent of Education
Career Cluster: Information Technology
Program of Study: Cybersecurity

High School					College			
Subject	**9th Grade**	**10th Grade**	**11th Grade**	**12th Grade**	**Semester I**	**Semester II**	**Semester III**	**Semester IV**
English (4)	English I	English II	English III	English IV				
Math (4)	Algebra I	Geometry	Algebra II	Math				
Science (4)	Biology	Lab Science	Anatomy and Physiology	Science				
Social Studies (4)	World History and Geography I: Middle Ages	World History and Geography II: Modern World	U.S. History	U.S. Government (.5) and D.C. History (.5)				
Health (.5) and Physical Ed (1)	Health (.5) Physical Ed (.5)	Physical Ed (.5)						
World Languages (2)			World Language I	World Language II				
Art (.5)		Art (.5)						
Music (.5)		Music (.5)						
Elective / Major Courses	Foundations of Cybersecurity	Internetworking Technology	Digital Forensics	Cybersecurity Capstone				
Total possible college credits completed in high school: XX					***Credit hours required to complete the AAS program: XX***			

Course Standards

Foundations of Cybersecurity

1. **General requirements.** This course is recommended for students in Grades 9-12. Students shall be awarded one credit for successful completion of 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 Information Technology (IT) Career Cluster focuses on building linkages in IT occupations for entry level, technical, and professional careers related to the design, development, support, and management of hardware, software, multimedia, and systems integration services.

   C. In the Foundations of Cybersecurity course, students will develop the knowledge and skills needed to explore fundamental concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will review and explore security policies designed to mitigate risks. The skills obtained in this course prepare students for additional study in cybersecurity. A variety of courses are available to students interested in this field. Foundations of Cybersecurity may serve as an introductory course in this field of study.

   D. Students will participate in at least two Career Exploration Work-Based Learning experiences in this course, which might include guest speakers and work-place tours relevant to the program of study.

   E. Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.

3. **Knowledge and skills.**

   A. **Employability skills. The student demonstrates necessary skills for career development and successful completion of course outcomes. The student is expected to:**

      1. Identify and demonstrate employable work behaviors such as regular attendance, punctuality, maintenance of a professional work environment, and effective written and verbal communication;
      2. Identify and demonstrate positive personal qualities such as authenticity, resilience, initiative, and a willingness to learn new knowledge and skills;
      3. Solve problems and think critically;
      4. Demonstrate leadership skills and function effectively as a team member; and
      5. Demonstrate an understanding of ethical and legal responsibilities in relation to the field of cybersecurity.

B. **Employability skills. The student identifies various employment opportunities and requirements in the cybersecurity field. The student is expected to:**
   1. Identify job and internship opportunities as well as accompanying duties and tasks;
   2. Research careers in cybersecurity and information assurance along with the education and job skills required for obtaining a job in both the public and private sectors;
   3. Identify and discuss certifications for cybersecurity-related careers; and
   4. Research and develop resumes, digital portfolios, or professional profiles in the cybersecurity field.

C. **Ethics and laws. The student understands ethical and current legal standards, rights and restrictions governing technology, technology systems, digital media, and the use of social media. The student is expected to:**
   1. Demonstrate and advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers;
   2. Research local, state, national, and international cyber law such as the PATRIOT Act of 2001, General Data Protection Regulation, and Digital Millennium Copyright Act;
   3. Research historic cases or events regarding cyber;
   4. Demonstrate an understanding of ethical and legal behavior when presented with various scenarios related to cyber activities;
   5. Define and identify techniques such as hacking, phishing, social engineering, online piracy, spoofing, and data vandalism; and
   6. Identify and use appropriate methods for citing sources.

D. **Ethics and laws. The student identifies the consequences of ethical versus malicious hacking. The student is expected to:**
   1. Identify motivations for hacking;
   2. Identify and describe the impact of cyberattacks on the global community, society, and individuals;
   3. Distinguish between a cyber attacker and a cyber defender;
   4. Differentiate types of hackers such as black hats, white hats, and gray hats;
   5. Determine possible outcomes and legal ramifications of ethical versus malicious hacking practices; and
   6. Debate the varying perspectives of ethical versus malicious hacking.

E. **Ethics and laws. The student identifies and defines cyberterrorism and counterterrorism. The student is expected to:**
   1. Define cyberterrorism, state-sponsored cyberterrorism, and hacktivism;
   2. Compare and contrast physical terrorism and cyberterrorism, including domestic and foreign actors
   3. Define and explain intelligence gathering and counterterrorism
   4. Identify the role of cyber defenders in protecting national interests and corporations; (E) identify the role of cyber defense in society and the global economy; and (F) explain the importance of protecting public infrastructures such as electrical power grids, water systems, pipelines, transportation, and nuclear plants.

F. **Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding significant issues related to digital technology, digital hygiene, and cyberbullying. The student is expected to:**
   1. Identify and understand the nature and value of privacy;
   2. Analyze the positive and negative implications of a digital footprint and the maintenance and monitoring of an online presence;

3. Discuss the role and impact of technology on privacy;
4. Identify the signs, emotional effects, and legal consequences of cyberbullying and cyberstalking; and
5. Identify and discuss effective ways to prevent, deter, and report cyberbullying.

G. **Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:**

1. Define information security and cyber defense;
2. Identify basic risk management and risk assessment principles related to cybersecurity threats and vulnerabilities;
3. Explain the fundamental concepts of confidentiality, integrity, availability, authentication, and authorization;
4. Describe the inverse relationship between privacy and security;
5. Identify and analyze cybersecurity breaches and incident responses;
6. Identify and analyze security concerns in areas such as physical, network, cloud, and web;
7. Define and discuss challenges faced by cybersecurity professionals;
8. Identify common risks, alerts, and warning signs of compromised computer and network systems;
9. Understand and explore the vulnerability of network-connected devices; and
10. Use appropriate cybersecurity terminology.

H. **Cybersecurity skills. The student understands and explains various types of malicious software (malware). The student is expected to:**

1. Define malware, including spyware, ransomware, viruses, and rootkits;
2. Identify the transmission and function of malware such as Trojans, worms, and viruses;
3. Discuss the impact malware has had on the cybersecurity landscape;
4. Explain the role of reverse engineering for detecting malware and viruses;
5. Compare free and commercial antivirus software alternatives; and
6. Compare free and commercial anti-malware software alternatives.

I. **Cybersecurity skills. The student understands and demonstrates knowledge of techniques and strategies to prevent a system from being compromised. The student is expected to:**

1. Define system hardening;
2. Demonstrate basic use of system administration privileges;
3. Explain the importance of patching operating systems;
4. Explain the importance of software updates;
5. Describe standard practices to configure system services;
6. Explain the importance of backup files; and
7. Research and understand standard practices for securing computers, networks, and operating systems.

J. **Cybersecurity skills. The student understands basic network operations. The student is expected to:**

1. Identify basic network addressing and devices, including switches and routers;
2. Analyze incoming and outgoing rules for traffic passing through a firewall;
3. Identify well known ports by number and service provided, including port 22 (ssh), port 80 (http), and port 443 (https);
4. Identify commonly exploited ports and services, including ports 20 and 21 (ftp) and port 23 (telnet); and
5. Identify common tools for monitoring ports and network traffic.

K. **Cybersecurity skills. The student identifies standard practices of system administration. The student is expected to:**
   1. Define what constitutes a secure password;
   2. Create a secure password policy, including length, complexity, account lockout, and rotation;
   3. Identify methods of password cracking such as brute force and dictionary attacks; and
   4. Examine and configure security options to allow and restrict access based on user roles.

L. **Cybersecurity skills. The student demonstrates necessary steps to maintain user access on the computer system. The student is expected to:**
   1. Identify the different types of user accounts and groups on an operating system;
   2. Explain the fundamental concepts and standard practices related to access control, including authentication, authorization, and accounting;
   3. Compare methods for single- and dual-factor authentication such as passwords, biometrics, personal identification numbers (PINs), and security tokens;
   4. Define and explain the purpose of an air-gapped computer; and
   5. Explain how hashes and checksums may be used to validate the integrity of transferred data.

M. **Cybersecurity skills. The student explores the field of digital forensics. The student is expected to:**
   1. Explain the importance of digital forensics to law enforcement, government agencies, and corporations;
   2. Identify the role of chain of custody in digital forensics;
   3. Explain the four steps of the forensics process, including collection, examination, analysis, and reporting;
   4. Identify when a digital forensics investigation is necessary;
   5. Identify information that can be recovered from digital forensics investigations such as metadata and event logs; and
   6. Analyze the purpose of event logs and identify suspicious activity.

N. **Cybersecurity skills. The student explores the operations of cryptography. The student is expected to:**
   1. Explain the purpose of cryptography and encrypting data;
   2. Research historical uses of cryptography; and
   3. Review simple cryptography methods such as shift cipher and substitution cipher.

O. **Risk assessment. The student understands information security vulnerabilities, threats, and computer attacks. The student is expected to:**
   1. Define and describe vulnerability, payload, exploit, port scanning, and packet sniffing as they relate to hacking;
   2. Define and describe cyberattacks, including man-in-the-middle, distributed denial of service, and spoofing;
   3. Explain how computer vulnerabilities leave systems open to cyberattacks;
   4. Identify threats to systems such as back-door attacks and insider threats;
   5. Differentiate types of social engineering attacks such as phishing, shoulder surfing, hoaxes, and dumpster diving;
   6. Explain how users are the most common vehicle for compromising a system at the application level; and
   7. Identify various types of application-specific attacks.

P. **Risk assessment. The student understands, identifies, and explains the strategies and techniques of both ethical and malicious hackers. The student is expected to:**
   1. Identify internal and external threats to computer systems;
   2. Identify the capabilities of vulnerability assessment tools, including open source tools; and
   3. Explain the concept of penetration testing, tools, and techniques.
   4. Risk assessment. The student evaluates the risks of wireless networks. The student is expected to:
   5. Compare risks associated with connecting devices to public and private wireless networks;
   6. Explain device vulnerabilities and security solutions on a wireless network;
   7. compare wireless encryption protocols;
   8. debate the broadcasting or hiding of a wireless service set identifier (SSID); and
   9. research and discuss wireless threats such as MAC spoofing and war driving.

Q. **Risk assessment. The student analyzes threats to computer applications. The student is expected to:**
   1. Define application security;
   2. Identify methods of application security such as secure development practices;
   3. Discuss methods of online spoofing such as web links in email, instant messaging, social media, and other online communication with malicious links;
   4. Explain the purpose and function of vulnerability scanners;
   5. Explain how coding errors may create system vulnerabilities; and
   6. Analyze the risks of distributing insecure programs.

R. **Risk assessment. The student understands the implications of sharing information and access with others. The student is expected to:**
   1. Describe the impact of granting applications unnecessary permissions;
   2. Describe the risks of granting third parties access to personal and proprietary data on social media and systems; and
   3. Describe the risks involved with accepting Terms of Service (ToS) or End User License Agreements (EULA) without a basic understanding of the terms or agreements.

S. **The student develops technology skills. The student is expected to:**
   1. Use technology as a tool to research, organize, evaluate, and communicate information.
   2. Use digital technologies (computers, PDAs, media players, GPSs, etc.); communication/networking tools, and social networks appropriately to access, manage; integrate, evaluate, and create information to successfully function in a knowledge economy;
   3. Demonstrate using current and new technologies specific to the program of study, course; and/or industry; and
   4. Apply a fundamental understanding of the ethical/legal issues surrounding the access and use of information technologies.

Internetworking Technologies

1. **General requirements.** This course is recommended for students in Grades 10-12. Prerequisites: Foundations of Cybersecurity.

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 Information Technology (IT) Career Cluster focuses on building linkages in IT occupations for entry level, technical, and professional careers related to the design, development, support, and management of hardware, software, multimedia, and systems integration services.

   C. The Internetworking Technologies course is normally comprised of the courses called Cisco CCNA R&S: Introduction to Networks (CCNA 1) and Cisco CCNA R&S: Routing and Switching Essentials (CCNA 2). The course introduces the concept of networking, using various analogies to help the student understand the movement of packets throughout the Internet, and the protocol standards used. The Routing and Switching course moves the student into the theory of "moving packets." The concepts of routing and switching "packets" to the correct destination is covered, and how a network administrator.

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

   E. Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.

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, attention to proper attire, maintenance of a clean and safe work environment, appropriate voice, and pride in work;
      2. identify and demonstrate positive personal qualities such as flexibility, open-mindedness, initiative, listening attentively to speakers, and willingness to learn new knowledge and skills;
      3. employ effective reading and writing skills;
      4. solve problems and think critically;
      5. demonstrate leadership skills and function effectively as a team member;
      6. identify and implement proper safety procedures;
      7. demonstrate an understanding of legal and ethical responsibilities in relation to the field of information technology; and
      8. demonstrate planning and time-management skills.

B. **The student identifies various employment opportunities in the information technology field. The student is expected to:**

   1. improve on a personal career plan along with education, job skills, and experience necessary to achieve career goals;
   2. develop a resume and portfolio appropriate to chosen career plan, including letters of recommendation; and
   3. illustrate interview skills for successful job placement.

C. **The student develops technology skills. The student is expected to:**

   1. Use technology as a tool to research, organize, evaluate, and communicate information.
   2. Use digital technologies (computers, PDAs, media players, GPSs, etc.), communication/networking tools, and social networks appropriately to access, manage, integrate, evaluate, and create information to successfully function in a knowledge economy.
   3. Demonstrate utilizing current and new technologies specific to the program of study, course, and/or industry.
   4. Apply a fundamental understanding of the ethical/legal issues surrounding the access and use of information technologies.

D. **The student applies communication, mathematics, English language arts, and science knowledge and skills to research and develop projects. The student is expected to:**

   1. demonstrate proper use of written, verbal, and visual communication techniques consistent with networking industry standards;
   2. demonstrate proper use of mathematics concepts in the development of networking technologies; and
   3. demonstrate proper use of science principles in the development of networking technologies.

E. **The student understands the operation of data networks. The student is expected to:**

   1. describe the purpose and functions of various network devices;
   2. describe the components required for network and Internet communications;
   3. select the correct components required to meet a given network specification;
   4. describe the purpose and basic operation of the protocols in the Open Systems Interconnection (OSI) and Transmission Control Protocol (TCP) models and their associated protocols;
   5. describe the impact of common networking applications Voice Over Internet Protocol (VOIP) and Video Over IP (VIP) on a network;
   6. interpret network diagrams;
   7. predict the path between two hosts across a network; and
   8. differentiate between Local Area Networks/Wide-Area Networks (LAN/WAN) operation and features.

F. **The student configures, verifies and troubleshoots switching. The student is expected to:**

   1. select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts;
   2. explain the technology and media access control method for Ethernet technologies;
   3. explain network segmentation and basic traffic management concepts;
   4. explain the operation and concepts of basic switching;

5. perform, save and verify initial switch configuration including Switched Virtual Interfaces (SVI) and Default Gateway;
6. verify network status and switch operation using basic utilities;
7. implement and verify basic security for a switch;
8. identify, prescribe, and resolve common switched network media issues, configuration issues, auto negotiation, and switch hardware failures;
9. describe the function and operation of Virtual Local Area Networks (VLANs); and
10. configure, verify, and troubleshoot VLANs and trunking.

G. **The student implements Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) addressing schemes and services to meet network requirements. The student is expected to:**

1. describe the need and role of addressing in a network;
2. compare and contrast IPv4 and IPv6;
3. create and apply appropriate IP addressing schemes to a network;
4. assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment;
5. explain the basic uses and operation of Network Address Translation (NAT) in IPv4;
6. describe and verify Domain Name Service (DNS) operation;
7. describe the operation and benefits of using private and public IPv4 addressing;
8. implement static and dynamic addressing services for hosts in a LAN environment; and
9. identify and correct IP addressing issues.

H. **The student configures, verifies, and troubleshoots routing. The student is expected to:**

1. describe basic routing concepts;
2. describe the operation of routers;
3. compare and contrast methods of routing and routing protocols;
4. configure, verify, and troubleshoot routing protocols;
5. connect, configure, and verify operation status of a device interface;
6. verify device configuration and network connectivity using ping, traceroute, telnet, Secure Shell (SSH) or other utilities;
7. perform and verify routing configuration tasks for a static or default route given specific routing requirements;
8. manage Internetwork Operating System (IOS) and configuration files including save, edit, upgrade, backup, and restore;
9. implement password and physical security;
10. configure and verify interVLAN routing;
11. configure and verify Access Control Lists (ACLs);
12. configure and verify Domain Host Configuration Protocol (DHCP) and Network Address Translation (NAT); and
13. troubleshoot and correct network and configuration issues.

T. **The student develops technology skills. The student is expected to:**

5. Use technology as a tool to research, organize, evaluate, and communicate information.

6. Use digital technologies (computers, PDAs, media players, GPSs, etc.); communication/networking tools, and social networks appropriately to access, manage; integrate, evaluate, and create information to successfully function in a knowledge economy;
7. Demonstrate using current and new technologies specific to the program of study, course; and/or industry; and
8. Apply a fundamental understanding of the ethical/legal issues surrounding the access and use of information technologies.

Digital Forensics

1. **General requirements.** This course is recommended for students in Grades 11-12. Prerequisites: Internetworking Technologies.

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 Information Technology (IT) Career Cluster focuses on building linkages in IT occupations for entry level, technical, and professional careers related to the design, development, support, and management of hardware, software, multimedia, and systems integration services.

   C. Digital Forensics is an evolving discipline concerned with analyzing anomalous activity on computers, networks, programs, and data. As a discipline, it has grown with the emergence of a globally-connected digital society. As computing has become more sophisticated, so too have the abilities of malicious agents to access systems and private information. By evaluating prior incidents, digital forensics professionals have the ability to investigate and craft appropriate responses to disruptions to corporations, governments, and individuals. Whereas cybersecurity takes a proactive approach to information assurance to minimize harm, digital forensics takes a reactive approach to incident response.

   D. Students will participate in a Career Preparation Work-Based Learning experience in this course, which might include paid or unpaid internship experiences relevant to the program of study.

   E. Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.

3. **Knowledge and skills**
   A. **Employability skills. The student identifies necessary skills for career development and employment opportunities. The student is expected to:**
      1. Investigate the need for digital forensics;
      2. Research careers in digital forensics along with the education and job skills required for obtaining a job in both the public and private sector;
      3. Identify job and internship opportunities as well as accompanying duties and tasks;
      4. Identify and discuss certifications for digital forensics careers;
      5. Explain ethical and legal responsibilities in relation to the field of digital forensics;
      6. Identify and describe businesses and government agencies that use digital forensics;
      7. Identify and describe the kinds of crimes investigated by digital forensics specialists; and
      8. Solve problems and think critically.

B. **Employability skills. The student communicates and collaborates effectively. The student is expected to:**
   1. Apply effective teamwork strategies;
   2. Collaborate with a community of peers and professionals;
   3. Create, review, and edit a report summarizing technical findings; and
   4. Present technical information to a non-technical audience.

C. **Ethics and laws. The student recognizes and analyzes ethical and current legal standards, rights, and restrictions related to digital forensics. The student is expected to:**
   1. Develop a plan to advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers;
   2. Research local, state, national, and international law such as the Electronic Communications Privacy Act of 1986, Title III (Pen Register Act); USA PATRIOT Act of 2001; and Digital Millennium Copyright Act;
   3. Research historic cases or events regarding digital forensics or cyber;
   4. Examine ethical and legal behavior when presented with confidential or sensitive information in various scenarios related to cyber activities;
   5. Analyze case studies of computer incidents;
   6. Use the findings of a computer incident investigation to reconstruct the incident;
   7. Identify and discuss intellectual property laws, issues, and use;
   8. Contrast legal and illegal aspects of information gathering;
   9. Contrast ethical and unethical aspects of information gathering;
   10. Analyze emerging legal and societal trends affecting digital forensics; and
   11. Discuss how technological changes affect applicable laws.

D. **Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding digital technology, safety, digital hygiene, and cyberbullying. The student is expected to:**
   1. Identify and use digital information responsibly;
   2. Use digital tools responsibly;
   3. Identify and use valid and reliable sources of information; and
   4. Gain informed consent prior to investigating incidents.

E. **Digital forensics skills. The student locates, processes, analyzes, and organizes data. The student is expected to:**
   1. Identify sources of data;
   2. Analyze and report data collected;
   3. Maintain data integrity;
   4. Examine metadata of a file; and
   5. Examine how multiple data sources can be used for digital forensics, including investigating malicious software (malware) and email threats.

F. **Digital forensics skills. The student understands software concepts and operations as they apply to digital forensics. The student is expected to:**
   1. Compare software applications as they apply to digital forensics;
   2. Describe the purpose of various application types such as email, web, file sharing, security applications, and data concealment tools;

3. Identify the different purposes of data formats such as pdf, wav, jpeg, and exe;
4. Describe how application logs and metadata are used for investigations;
5. Describe digital forensics tools;
6. Select the proper software tool based on appropriateness, effectiveness, and efficiency for a given digital forensics scenario; and
7. Describe components of applications such as configurations settings, data, supporting files, and user interface.

G. **Digital forensics skills. The student understands operating systems concepts and functions as they apply to digital forensics. The student is expected to:**

1. Compare various operating systems;
2. Describe file attributes, including access and creation times;
3. Describe how operating system logs are used for investigations;
4. Compare and contrast the file systems of various operating systems;
5. Compare various primary and secondary storage devices; and
6. Differentiate between volatile and non-volatile memory.

H. **Digital forensics skills. The student understands networking concepts and operations as they apply to digital forensics. The student is expected to:**

1. Examine networks, including Internet Protocol (IP) addressing and subnets;
2. Describe the Open Systems Interconnection (OSI) model;
3. Describe the Transmission Control Protocol/Internet Protocol (TCP/IP) model;
4. Use network forensic analysis tools to examine network traffic data from sources such as firewalls, routers, intrusion detection systems (IDS), and remote access logs; and
5. Identify malicious or suspicious network activities such as mandatory access control (MAC) spoofing and rogue wireless access points.

I. **Digital forensics skills. The student explains the principles of access controls. The student is expected to:**

1. Define the principle of least privilege;
2. Describe the impact of granting access and permissions;
3. Identify different access components such as passwords, tokens, key cards, and biometric verification systems;
4. Explain the value of an access log to identify suspicious activity;
5. Describe the risks of granting third parties access to personal and proprietary data on social media and systems;
6. Describe the risks involved with accepting Terms of Service (ToS) or End User License Agreements (EULA) without a basic understanding of the terms or agreements; and
7. Identify various access control methods such as MAC, role-based access control (RBAC), and discretionary access control (DAC).

J. **Incident response. The student objectively analyzes collected data from an incident. The student is expected to:**

1. Identify the role of chain of custody in digital forensics;
2. Describe safe data handling procedures;

3. Explain the fundamental concepts of confidentiality, integrity, availability, authentication, and authorization;
4. Identify and report information conflicts or suspicious activity;
5. Identify events of interest and suspicious activity by examining network traffic; and
6. Identify events of interest and suspicious activity by examining event logs.

K. **Incident response. The student analyzes the various ways systems can be compromised. The student is expected to:**

1. Analyze the different signatures of cyberattacks; and
2. Identify points of weakness and attack vectors such as online spoofing, phishing, and social engineering.

L. **Incident response. The student follows a methodological approach to prepare for and respond to an incident. The student is expected to:**

1. Define the components of the incident response cycle, including preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity;
2. Describe incident response preparation;
3. Discuss incident response detection and analysis;
4. Discuss containment and eradication of and recovery from an incident;
5. Describe post-incident activities such as reflecting on lessons learned, using collected incident data, and retaining evidence of an incident;
6. Develop an incident response plan; and
7. Describe ways a user may compromise the validity of existing evidence.

M. **The student develops technology skills. The student is expected to:**

1. Use technology as a tool to research, organize, evaluate, and communicate information.
2. Use digital technologies (computers, PDAs, media players, GPSs, etc.); communication/networking tools, and social networks appropriately to access, manage; integrate, evaluate, and create information to successfully function in a knowledge economy;
3. Demonstrate using current and new technologies specific to the program of study, course; and/or industry; and
4. Apply a fundamental understanding of the ethical/legal issues surrounding the access and use of information technologies.

Cybersecurity Capstone

1. **General requirements.** Students shall be awarded one credit for successful completion of this course. This course is recommended for students in Grades 11 and 12. Recommended prerequisite: Digital Forensics.

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 Information Technology (IT) Career Cluster focuses on building linkages in IT occupations for entry level, technical, and professional careers related to the design, development, support, and management of hardware, software, multimedia, and systems integration services.

   C. In the Cybersecurity Capstone course, students will develop the knowledge and skills needed to explore advanced concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will develop security policies to mitigate risks. The skills obtained in this course prepare students for additional study toward industry certification. A variety of courses are available to students interested in the cybersecurity field. Cybersecurity Capstone may serve as a culminating course in this field of study.

   D. Students will participate in a Career Preparation Work-Based Learning experience in this course, which includes paid or unpaid internship, pre-apprenticeship, or apprenticeship experiences relevant to the program of study.

   E. Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.

3. **Knowledge and skills.**
   A. **Employability skills. The student demonstrates necessary skills for career development and successful completion of course outcomes. The student is expected to:**
      1. **I**dentify and demonstrate employable work behaviors such as regular attendance, punctuality, maintenance of a professional work environment, and effective written and verbal communication;
      2. Identify and demonstrate positive personal qualities such as authenticity, resilience, initiative, and a willingness to learn new knowledge and skills;
      3. Solve problems and think critically;
      4. Demonstrate leadership skills and function effectively as a team member; and
      5. Demonstrate an understanding of ethical and legal responsibilities in relation to the field of cybersecurity.

   B. **Employability skills. The student identifies various employment opportunities in the cybersecurity field. The student is expected to:**
   Develop a personal career plan along with the education, job skills, and experience necessary to achieve career goals;
   Develop a resume or a portfolio appropriate to a chosen career plan; and
   Illustrate interview skills for successful job placement.

C. **Ethics and laws. The student evaluates ethical and current legal standards, rights and restrictions governing technology, technology systems, digital media and information technology, and the use of social media in the context of today's society. The student is expected to:**
   1. Analyze and apply to a scenario local, state, national, and international cyber law such as David's Law and Digital Millennium Copyright Act;
   2. valuate historic cases or events regarding cyber; and
   3. **E**xplore compliance requirements such as Section 508 of the Rehabilitation Act of 1973, Family Educational Rights and Privacy Act of 1974 (FERPA), Health Insurance Portability and Accountability.

D. **Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding significant issues relating to digital technology, safety, digital hygiene, and cyberbullying. The student is expected to:**
   1. Debate the relationship between privacy and security; and
   2. Identify ethical or unethical behavior when presented with various scenarios related to cyber activities.

E. **Cybersecurity skills. The student explains the importance and process of penetration testing. The student is expected to:**
   1. Define the phases of penetration testing, including plan, discover, attack, and report;
   2. Develop a plan to gain authorization for penetration testing;
   3. Identify commonly used vulnerability scanning tools such as port scanning, packet sniffing, and password crackers;
   4. Develop a list of exploits based on results of scanning tool reports; and
   5. Prioritize a list of mitigations based on results of scanning tool reports.

F. **Cybersecurity skills. The student understands common cryptographic methods. The student is expected to:**
   1. Evaluate symmetric and asymmetric algorithms such as substitution cipher, Advanced Encryption Standard (AES), Diffie-Hellman, and Rivest-Shamir-Adleman (RSA);
   2. Explain the purpose of hashing algorithms, including blockchain;
   3. Explain the function of password salting;
   4. Explain and create a digital signature; and
   5. Explain steganography.

G. **Cybersecurity skills. The student understands the concept of cyber defense. The student is expected to**:
   1. Explain the purpose of establishing system baselines;
   2. Valuate the role of physical security;
   3. Valuate the functions of network security devices such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and intrusion detection prevention systems (IDPS);
   4. Evaluate the functions of network security devices such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and intrusion detection prevention systems (IDPS);
   5. Analyze log files for anomalies; and
   6. Develop a plan demonstrating the concept of defense in depth.

H. **Cybersecurity skills. The student demonstrates an understanding of secure network design. The student is expected to:**
   1. Explain the benefits of network segmentation, including sandboxes, air gaps, and virtual local area networks (VLAN);
   2. Investigate the role of software-managed networks, including virtualization;
   3. Discuss the role of honeypots and honeynets in networks; and
   4. Create an incoming and outgoing network policy for a firewall.

I. **Cybersecurity skills. The student integrates principles of digital forensics. The student is expected too:**
   1. Identify cyberattacks by their signatures;
   2. Explain proper data acquisition;
   3. Examine evidence from devices for suspicious activities; and
   4. Research current cybercrime cases involving digital forensics.

J. **Cybersecurity skills. The student explores emerging technology. The student is expected to:**
   1. Describe the integration of artificial intelligence and machine learning in cybersecurity;
   2. Investigate impacts made by predictive analytics on cybersecurity; and
   3. Research other emerging trends such as augmented reality and quantum computing.

K. **Cybersecurity skills. The student uses various operating system environments. The student is expected to:**
   1. Issue commands via the command line interface (CLI) such as ls, cd, pwd, cp, mv, chmod, ps, sudo, and passwd;
   2. Describe the file system structure for multiple operating systems;
   3. Manipulate and edit files within the CLI; and
   4. Determine network status using the CLI with commands such as ping, ifconfig/ipconfig, traceroute/tracert, and netstat.

L. **Cybersecurity skills. The student clearly and effectively communicates technical information. The student is expected to:**
   1. Collaborate with others to create a technical report;
   2. Create, review, and edit a report summarizing technical findings; and
   3. Present technical information to a non-technical audience.

M. **Risk assessment. The student analyzes various types of threats, attacks, and vulnerabilities. The student is expected to:**
   1. Differentiate types of attacks, including operating systems, software, hardware, network, physical, social engineering, and cryptographic;
   2. Explain blended threats such as combinations of software, hardware, network, physical, social engineering, and cryptographic;
   3. Discuss risk response techniques, including accept, transfer, avoid, and mitigate;
   4. Develop a plan of preventative measures to address cyberattacks;
   5. Describe common web vulnerabilities such as cross-site scripting, buffer overflow, injection, spoofing, and denial of service;

6. Describe common data destruction and media sanitation practices such as wiping, shredding, and degaussing; and
7. Develop an incident response plan for a given scenario or recent attack.

N. **Risk assessment. The student understands risk management processes and concepts. The student is expected to:**
   1. Describe various access control methods such as mandatory access control (MAC), role-based access control (RBAC), and discretionary access control (DAC);
   2. Develop and defend a plan for multi-factor access control using components such as biometric verification systems, key cards, tokens, and passwords; and
   3. Review a disaster recovery plan (DRP) that includes backups, redundancies, system dependencies, and alternate sites.

O. **Risk assessment. The student investigates the role and effectiveness of environmental controls. The student is expected to:**
   1. Explain commonly used physical security controls, including lock types, fences, barricades, security doors, and mantraps; and
   2. Describe the role of embedded systems such as fire suppression; heating, ventilation, and air conditioning (HVAC) systems; security alarms; and video monitoring.

P. **The student develops technology skills. The student is expected to:**
   1. Use technology as a tool to research, organize, evaluate, and communicate information.
   2. Use digital technologies (computers, PDAs, media players, GPSs, etc.); communication/networking tools, and social networks appropriately to access, manage; integrate, evaluate, and create information to successfully function in a knowledge economy;
   3. Demonstrate using current and new technologies specific to the program of study, course; and/or industry; and
   4. Apply a fundamental understanding of the ethical/legal issues surrounding the access and use of information technologies.