Florida Department of Education
Curriculum Framework

Program Title: **Applied Cybersecurity**
Program Type: **Career Preparatory**
Career Cluster: **Information Technology**

Career Certificate Program		
Program Number	Y100300	
CIP Number	0511100302	
Grade Level	30, 31	
Program Length	750 hours	
Teacher Certification	Refer to the **Program Structure** section.	
CTSO	PBL, BPA	
SOC Codes (all applicable)	Please see the CIP to SOC Crosswalk located at the link below.	
CTE Program Resources	http://www.fldoe.org/academics/career-adult-edu/career-tech-edu/program-resources.stml	
Basic Skills Level	Computation (Mathematics) 9	Communications (Reading and Language Arts): 9

Purpose

This program offers a sequence of courses that provides coherent and rigorous content aligned with challenging academic standards and relevant technical knowledge and skills needed to prepare for further education and cybersecurity-related careers in the Information Technology career cluster; provides technical skill proficiency, and includes competency-based applied learning that contributes to the academic knowledge, higher-order reasoning and problem-solving skills, work attitudes, general employability skills, technical skills, and occupation-specific skills, and knowledge of all aspects of cybersecurity.

The content includes but is not limited to foundational knowledge and skills in computer and network security, security vulnerabilities, attack mechanisms and techniques, intrusion detection and prevention, cryptographic systems, system hardening, risk identification, incidence response, penetration testing, key management, access control, and recovery. Specialized courses focus on database security, planning and analysis, software, and web security.

Additional Information relevant to this Career and Technology (CTE) program is provided at the end of this document.

Program Structure

This program is a planned sequence of instruction consisting of two occupational completion points (OCPs). To complete this program, students must complete OCP A plus one of the subsequent courses in OCP B.

This program is comprised of courses that have been assigned course numbers in the SCNS (Statewide Course Numbering System) in accordance with Section 1007.24 (1), F.S. Career and Technical credit shall be awarded to the student on a transcript in accordance with Section 1001.44 (3)(b), F.S.

To teach the courses listed below, instructors must hold at least one of the teacher certifications indicated for that course.

The following table illustrates the postsecondary program structure:

OCP	Course Number	Course Title	Teacher Certification	Length
A	CTS0018	Cybersecurity Associate	BUS ED 1 @2 COMPU SCI 6 CYBER TECH 7G INFO TECH 7G	600 hours
B	CTS0019	Information Security Manager **OR**		150 hours
	CTS0021	Data Security Specialist **OR**		150 hours
	CTS0060	Software Security Specialist **OR**		150 hours
	CTS0085	Web Security Specialist **OR**		150 hours
	CTS0089	Information Security Administrator		150 hours

Common Career Technical Core – Career Ready Practices

Career Ready Practices describe the career-ready skills that educators should seek to develop in their students. These practices are not exclusive to a Career Pathway, program of study, discipline or level of education. Career Ready Practices should be taught and reinforced in all career exploration and preparation programs with increasingly higher levels of complexity and expectation as a student advances through a program of study.

1. Act as a responsible and contributing citizen and employee.

2. Apply appropriate academic and technical skills.

3. Attend to personal health and financial well-being.

4. Communicate clearly, effectively and with reason.

5. Consider the environmental, social and economic impacts of decisions.

6. Demonstrate creativity and innovation.

7. Employ valid and reliable research strategies.

8. Utilize critical thinking to make sense of problems and persevere in solving them.

9. Model integrity, ethical leadership and effective management.

10. Plan education and career path aligned to personal goals.

11. Use technology to enhance productivity.

12. Work productively in teams while using cultural/global competence.

Standards

After successfully completing this program, the student will be able to perform the following:

01.0 Demonstrate knowledge, skill, and application of computer systems.
02.0 Demonstrate knowledge of different operating systems.
03.0 Develop a familiarity with the information technology industry.
04.0 Develop an awareness of microprocessors and digital computers.
05.0 Develop an awareness of programming languages.
06.0 Develop an awareness of emerging technologies.
07.0 Demonstrate an understanding of the Open Systems Interconnection (OSI) models.
08.0 Demonstrate an understanding of the TCP/IP model.
09.0 Identify computer components and their functions.
10.0 Demonstrate proficiency using the Internet to locate information.
11.0 Demonstrate an understanding of Internet safety and ethics.
12.0 Demonstrate proficiency using common software applications.
13.0 Perform email activities.
14.0 Demonstrate proficiency in using presentation software and equipment.
15.0 Perform decision-making activities in a multimedia environment.
16.0 Demonstrate an understanding of cybersecurity, including its origins, trends, culture, and legal implications.
17.0 Describe the national agencies and supporting initiatives involved in cybersecurity.
18.0 Discuss the underlying concepts of terms used in cybersecurity.
19.0 Demonstrate an understanding of basic computer components, their functions, and their operation.
20.0 Demonstrate knowledge of different operating systems.
21.0 Demonstrate an understanding of the Open Systems Interconnection (OSI) model. The student will be able to
22.0 Demonstrate an understanding of the TCP/IP model.
23.0 Describe the services and protocols that operate in the application, transport, network, and data link layers of the OSI Model.
24.0 Demonstrate proficiency using computer networks.
25.0 Describe and differentiate between serial, digital subscriber line (DSL), Metro Ethernet, and cable modem WAN connections.
26.0 Demonstrate an understanding of basic security concepts.
27.0 Demonstrate an understanding of legal and ethical issues in cybersecurity.
28.0 Demonstrate an understanding of virtualization technology.
29.0 Recognize and understand the administration of the following types of remote access technologies.
30.0 Understand the application of the following concepts of physical security.
31.0 Securely configure and maintain the following types of devices.
32.0 Understand the societal and security challenges of emerging technologies.
33.0 Recognize and be able to differentiate and explain the following access control models.
34.0 Understand the security concerns for the following types of media.
35.0 Explain the following security topologies as they relate to cybersecurity.
36.0 Describe the roles within teams, work units, departments, organizations, inter-organizational systems, and the larger environment.

37.0 Demonstrate an understanding of the technical underpinnings of cybersecurity and its taxonomy, terminology, and challenges.
38.0 Demonstrate an understanding of common information and computer system security vulnerabilities.
39.0 Demonstrate an understanding of common cyber attack mechanisms, their consequences, and motivation for their use.
40.0 Be able to identify and explain the following different kinds of cryptographic algorithms.
41.0 Demonstrate an understanding of the following kinds of steganographic techniques and their use in cybersecurity.
42.0 Understand how cryptography and digital signatures address the following security concepts.
43.0 Understand and be able to explain the following concepts of PKI (Public Key Infrastructure).
44.0 Demonstrate an understanding of certificates and their role in cybersecurity.
45.0 Demonstrate an understanding of intrusion, the types of intruders, their techniques, and their motivation.
46.0 Demonstrate an understanding of Intrusion Detection Systems (IDS).
47.0 Describe host-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature).
48.0 Describe network-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature).
49.0 Demonstrate an understanding of IDS applications.
50.0 Demonstrate an understanding of port scanning and network traffic monitoring employed as intrusion detection techniques.
51.0 Demonstrate an understanding of firewalls and other means of intrusion prevention.
52.0 Demonstrate an understanding of vulnerabilities unique to virtual computing environments.
53.0 Demonstrate an understanding of social engineering and its implications to cybersecurity.
54.0 Demonstrate an understanding of fundamental security design principles and their role in limiting points of vulnerability.
55.0 Demonstrate an understanding of how to configure host systems to guard against cyber intrusion.
56.0 Demonstrate an understanding of authentication methods and strategies.
57.0 Demonstrate an understanding of methods and strategies for controlling access to computer networks.
58.0 Demonstrate an understanding of key network services, their operation, vulnerabilities, and ways in which they may be secured.
59.0 Demonstrate an understanding of the processes involved in hardening a computer system or network.
60.0 Demonstrate an understanding of Public Key Infrastructure (PKI) management functions, key states, and life cycle/transition considerations.
61.0 Demonstrate an understanding of the processes associated with assessing vulnerabilities and risks within an organization.
62.0 Demonstrate an understanding of penetration testing, the types of tests and metrics, testing methodologies, and reporting processes.
63.0 Demonstrate an understanding of the Incident Response Life Cycle and the activities comprising each phase.
64.0 Demonstrate proficiency in cybersecurity risk mitigation planning.
65.0 Demonstrate proficiency in establishing a risk management framework.
66.0 Demonstrate proficiency in creating a corporate security policy.
67.0 Demonstrate proficiency in addressing process risks.
68.0 Demonstrate proficiency in addressing physical security risks.
69.0 Demonstrate proficiency in cybersecurity contingency planning.
70.0 Demonstrate proficiency in cybersecurity disaster recovery planning.
71.0 Demonstrate proficiency in cybersecurity business continuity planning.
72.0 Demonstrate proficiency in the essential elements of forensic analysis.
73.0 Demonstrate an understanding of database design, structure, and operation.
74.0 Demonstrate a fundamental understanding of Structured Query Language (SQL).
75.0 Demonstrate an understanding of database security policies.
76.0 Demonstrate an understanding of database access control, functions, methods, and verification.

77.0 Demonstrate an understanding of database vulnerabilities, attack vectors, and associated countermeasures.
78.0 Demonstrate an understanding of pre- and post-intrusion actions to facilitate database recovery.
79.0 Demonstrate an understanding of software design, structure, and operation.
80.0 Demonstrate a fundamental understanding of common software attack vectors.
81.0 Demonstrate an understanding input syntax validation.
82.0 Demonstrate an understanding of best practices for processing input data to ensure safe and secure program code.
83.0 Demonstrate an understanding of the role of environment variables in the operation of software applications.
84.0 Demonstrate an understanding of program design strategies for inhibiting elevated privilege attacks.
85.0 Demonstrate an understanding of the primary security services used in Internet and intranet environments.
86.0 Demonstrate a fundamental understanding of the SSL protocol stack and its elements.
87.0 Demonstrate an understanding of IPsec, including its uses, elements, and mechanisms.
88.0 Demonstrate an understanding of S/MIME, including its uses, functions, cryptographic algorithms, and key certificates.
89.0 Demonstrate an understanding of Kerberos and its role in third-party authentication in a distributed network.
90.0 Demonstrate an understanding of identity management and ways in which secure identify information is exchanged across different domains.
91.0 Complete a safety skills inventory.
92.0 Demonstrate acceptable project values.
93.0 Demonstrate the ability to detect and resolve system vulnerabilities.
94.0 Plan, organize, and carry out a penetration-testing plan.
95.0 Demonstrate proficiency in conducting forensic analysis.
96.0 Successfully work as a member of a team.
97.0 Manage time according to a plan.
98.0 Keep acceptable records of progress problems and solutions.
99.0 Manage resources.
100.0 Use tools, materials, and processes in an appropriate and safe manner.
101.0 Research content related to the project and document the results.
102.0 Use presentation skills, and appropriate media to describe the progress, results and outcomes of the experience.
103.0 Demonstrate competency in the area of expertise related to the Applied Cybersecurity education program previously completed that this project is based upon.

Florida Department of Education
Student Performance Standards

Program Title: **Applied Cybersecurity**
Career Certificate Program Number: **Y100300**

Course Number: CTS0018 **Occupational Completion Point: A** **Cybersecurity Associate – 600 Hours**	
01.0	Demonstrate knowledge, skill, and application of computer systems. The student will be able to:
01.01	Describe and use current and emerging computer technology and software to perform personal and business related tasks.
01.02	Describe the types of communications and networking systems used in workplace environments.
01.03	Locate and use software application reference materials such as on-line help, vendor bulletin boards, tutorials, and manuals.
01.04	Troubleshoot problems with computer hardware peripherals.
01.05	Describe ethical, privacy, and security issues and problems associated with computers and information systems.
01.06	Demonstrate proficiency in using the basic features of GUI browsers.
01.07	Configure computer systems to protect against various low-level attacks.
02.0	Demonstrate knowledge of different operating systems. The student will be able to:
02.01	Identify the most common computer operating systems.
02.02	Describe and use industry accepted file naming conventions, particularly in NTFS, ext4, FAT, and ReFS file systems.
02.03	Demonstrate proficiency with file management tasks (e.g., folder creation, file creation, backup, copy, delete, open, save).
02.04	Demonstrate a working knowledge of standard file formats.
02.05	Compare and contrast various operating systems (e.g., Android iOS, Windows, Mac, Linux).
02.06	Differentiate between different operating systems and applications.
02.07	Compare and contrast open source and proprietary software.
02.08	Explain how system utilities are used to maintain computer performance.
02.09	Evaluate criteria for selecting an operating system.
02.10	Configure various operating systems from their default settings to low, medium, and high security level settings.
03.0	Develop a familiarity with the information technology industry. The student will be able to:
03.01	Explain how information technology impacts the operation and management of business and society.

	03.02 Identify and describe the various ways of segmenting the IT industry (e.g., hardware vs. software, server vs. client, business vs. entertainment, stable vs. mobile).
	03.03 Describe how digital technologies (social media) are changing both work and personal lifestyles.
	03.04 Demonstrate an understanding of configuring social media used for business to meet various business requirements.
	03.05 Demonstrate an awareness of Cloud based infrastructure including SaaS (Software as a Service) and their impact on the IT industry.
04.0	Develop an awareness of microprocessors and digital computers. The student will be able to:
	04.01 Explain software hierarchy and its impact on microprocessors as it relates to the limitation and/or increase in security.
	04.02 Explain the need for and use of peripherals and how they can compromise security.
	04.03 Demonstrate proficiency installing and using plug-and-play peripherals and explain their associated security risks.
	04.04 Identify the basic concepts of computer maintenance and upgrades and their relevance as it relates to security.
05.0	Develop an awareness of programming languages. The student will be able to:
	05.01 Explain the need for and use of compilers.
	05.02 Identify the three types of programming design approaches (e.g., top-down, structured, object-oriented).
	05.03 Compare the various types or classes of programming languages (e.g., compiled, interpretive).
	05.04 Differentiate among source code, machine code, interpreters, and compilers.
	05.05 Characterize the major categories of programming languages and how they are used.
	05.06 Create a model flowchart for a computer program using software applications like RAPTOR or MS VISIO.
	05.07 Describe the stages in the software development life cycle and explain how to successfully implement them.
	05.08 Compare security and vulnerabilities of various programming languages.
06.0	Develop an awareness of emerging technologies. The student will be able to:
	06.01 Compare and contrast emerging technologies and describe how they impact the security of business in the global marketplace (e.g., wireless, wireless web, cell phones, portables/handhelds, vehicles, home networks, peer-to-peer, IoT, embedded systems, AI).
	06.02 Adhere to published best practices for protecting personal identifiable information when using the Internet.
	06.03 Identify trends related to the secure use of information technology in people's personal and professional lives.
	06.04 Characterize how the rapid pace of change in information technology impacts our society's ability to keep the appropriate level of security.
07.0	Demonstrate an understanding of the Open Systems Interconnection (OSI) models. The student will be able to:
	07.01 Explain the interrelations of the seven layers of the Open Systems Interconnection (OSI) as it relates to hardware and software.

	07.02 Describe the purpose of the OSI model and each of its layers.
	07.03 Explain specific functions belonging to each OSI model layer.
	07.04 Understand how two network nodes communicate through the OSI model.
	07.05 Discuss the structure and purpose of data packets and frames.
	07.06 Describe the two types of addressing covered by the OSI model.
08.0	Demonstrate an understanding of the TCP/IP model. The student will be able to:
	08.01 Explain the interrelations of the four layers of the TCP/IP model as it relates to hardware and software.
	08.02 Describe the purpose of the TCP/IP model and each of its layers.
	08.03 Explain specific functions belonging to each TCP/IP model layer.
	08.04 Understand how two network nodes communicate through the TCP/IP model.
	08.05 Describe the two types of addressing covered by the TCP/IP model.
09.0	Identify computer components and their functions. The student will be able to:
	09.01 Identify the internal components of a computer (e.g., power supply, hard drive, mother board, I/O cards/ports, cabling).
	09.02 Use common computer and programming terminology.
10.0	Demonstrate proficiency using the Internet to locate information. The student will be able to:
	10.01 Identify and describe web terminology.
	10.02 Define Universal Resource Locators (URLs) and associated protocols (e.g., http, ftp, telnet, mailto) and their associated secure protocols (e.g. https, ftps, ssh).
	10.03 Compare and contrast the types of Internet domains (e.g., .com, .org, .edu, .gov, .net, .mil).
	10.04 Demonstrate proficiency using search engines, including Boolean search strategies.
	10.05 Demonstrate proficiency using various secure web tools (e.g., downloading of files, transfer of files, SSH, PDF).
	10.06 Compare and contrast the roles of web servers and web browsers.
	10.07 Compare and contrast MS Web Servers and Linux Web Servers.
11.0	Demonstrate an understanding of Internet safety and ethics. The student will be able to:
	11.01 Describe cyber-bullying and its impact on perpetrators and victims.
	11.02 Differentiate between viruses and malware, specifically their sources, ploys, and impact on personal privacy and computer operation, and ways to avoid infection.
	11.03 Describe risks associated with sexting, including related legal issues, social engineering aspects, prevention methods, and reporting of offenses.

	11.04 Describe the risks associated with online gaming and ways to reduce these risks.
	11.05 Describe the intellectual property rights, ethics and legalities of downloading music or videos from the Internet.
	11.06 Describe various risks associated with social networking sites and ways to reduce these risks.
	11.07 Describe the risks associated with various conferencing programs and ways to reduce these risks.
	11.08 Adhere to cyber safety practices with regard to conducting Internet searches, email, chat rooms, and other social network websites.
12.0	Demonstrate proficiency using common software applications. The student will be able to:
	12.01 Compare and contrast the appropriate use of various software applications (e.g., word processing, desktop publishing, graphics design, web browser, email, presentation, database, scheduling, financial management, Java applet, music).
	12.02 Demonstrate proficiency in the use of various software applications (e.g., word processing, desktop publishing, graphics design, web browser, email, presentation, database, scheduling, financial management, Java applet, music).
13.0	Perform email activities. The student will be able to:
	13.01 Describe email capabilities and functions.
	13.02 Identify components of an email message.
	13.03 Identify the components of an email address.
	13.04 Identify when to use different email options.
	13.05 Attach a file to an email message.
	13.06 Forward an email message.
	13.07 Use an address book if an address book is available via the school's Outlook server for the student to use.
	13.08 Reply to an email message.
	13.09 Use the Internet to perform email activities.
	13.10 Identify the appropriate use of email and demonstrate related email etiquette.
	13.11 Recognize a fraudulent email and deal with it appropriately.
	13.12 Identify common problems associated with widespread use of email.
	13.13 Create folders to organize email.
14.0	Demonstrate proficiency in using presentation software and equipment. The student will be able to:
	14.01 Produce a presentation that includes music, animation, and digital photography and present it using appropriate technology.
	14.02 Using presentation software, create a multimedia presentation that incorporates shot and edited video, animation, music, narration and adheres to good design principles, use of transitions, and effective message conveyance.
	14.03 Demonstrate knowledge of the roles and responsibilities of a multimedia production team (e.g. project manager, creative or design director, content experts, writers, graphic designers, animators, sound designers, videographer, interface designers/programmers).

	14.04 Collaborate with team members to plan, edit, evaluate, and present a multimedia presentation where individuals on the team function in specific production roles.
	14.05 Create a self-running presentation with synchronized audio, convert presentation slides (e.g., PowerPoint) into streaming ASF files for use on the web.
15.0	Perform decision-making activities in a multimedia environment. The student will be able to:
	15.01 Determine work priorities, the audience, project budgets, project specifications and the production schedule.
	15.02 Evaluate and select appropriate software packages and multimedia tools to complete assigned tasks.
	15.03 Present and defend design projects.
16.0	Demonstrate an understanding of cybersecurity, including its origins, trends, culture, and legal implications. The student will be able to:
	16.01 Define cybersecurity.
	16.02 Describe how information security evolved into cybersecurity and the impact of the Internet on the pace and nature of the evolution.
	16.03 Describe the individual elements that comprise the CIA triad (i.e., Confidentiality, Integrity, Availability).
	16.04 Define and explain the various types of hackers and the role each plays in cybersecurity.
	16.05 Describe various methodologies used by hackers and the basis for their employment.
	16.06 Describe the individual elements of the AAA model (Authentication, Authorization and Accounting).
17.0	Describe the national agencies and supporting initiatives involved in cybersecurity. The student will be able to:
	17.01 Describe the role of the National Security Agency.
	17.02 Describe current trends in cyber-attacks and strategies for combating them.
	17.03 Describe the legal implications of computer hacking and other forms of cyber-attacks.
	17.04 Understand the importance of the weekly bulletins distributed by the United States Computer Emergency Readiness Team (US-CERT).
	17.05 Determine if any software or hardware on a given network has vulnerabilities outlined in the most recent US-CERT bulletin.
18.0	Discuss the underlying concepts of terms used in cybersecurity. The student will be able to:
	18.01 Differentiate between cybersecurity and information assurance.
	18.02 Define confidentiality and give examples of security breaches.
	18.03 Define integrity and give examples of security breaches.
	18.04 Define authenticity and give examples of security breaches.
	18.05 Define accountability (non-repudiation) and give examples of security breaches.
19.0	Demonstrate an understanding of basic computer components, their functions, and their operation. The student will be able to:

	19.01	Describe the internal components of a computer (e.g., power supply, hard drive, mother board, I/O cards/ports, cabling).
	19.02	Demonstrate and understanding of common computer and programming terminology.
	19.03	Explain the physical and logical architecture of a microcomputer system.
	19.04	Describe the file types used in the operation of a computer.
	19.05	Compare and contrast memory technologies (e.g., RAM, ROM, virtual memory, memory management).
20.0	Demonstrate knowledge of different operating systems. The student will be able to:	
	20.01	Compare operating system file naming conventions.
	20.02	Describe the common elements that comprise the architecture of an operating system (e.g., kernel, file manager, memory manager, device manager, network manager).
	20.03	Demonstrate proficiency with file management and structure (e.g., folder creation, file creation, backup, copy, delete, open, save).
	20.04	Demonstrate a working knowledge of standard file formats.
	20.05	Describe the purpose of various operating systems (e.g., Windows, Mac, iOS, Android and Linux).
	20.06	Describe the difference between client and network operating systems.
	20.07	Differentiate between different operating systems and applications and Macros.
	20.08	Explain the basics of boot sequences, methods and startup utilities.
	20.09	Compare and contrast open source and proprietary software.
	20.10	Describe common system utilities used in performing computer maintenance.
21.0	Demonstrate an understanding of the Open Systems Interconnection (OSI) model. The student will be able to	
	21.01	Explain the interrelations of the seven layers of the Open Systems Interconnection (OSI) as it relates to hardware and software.
	21.02	Describe the purpose of the OSI model and each of its layers.
	21.03	Explain specific functions belonging to each OSI model layer.
	21.04	Understand how two network nodes communicate through the OSI model.
	21.05	Discuss the structure and purpose of data packets and frames.
	21.06	Describe the two types of addressing covered by the OSI model.
22.0	Demonstrate an understanding of the TCP/IP model. The student will be able to:	
	22.01	Explain the interrelations of the four layers of the TCP/IP model as it relates to hardware and software.
	22.02	Describe the purpose of the TCP/IP model and each of its layers.
	22.03	Explain specific functions belonging to each TCP/IP model layer.

	22.04 Understand how two network nodes communicate through the TCP/IP model.
	22.05 Describe the two types of addressing covered by the TCP/IP model.
23.0	Describe the services and protocols that operate in the application, transport, network, and data link layers of the OSI Model. The student will be able to:
	23.01 Describe the services and protocols used in the OSI Application Layer (i.e., DHCP, DNS, FTP, HTTP, SMTP, Telnet, IMAP).
	23.02 Describe the services and protocols used in the OSI Transport Layer (i.e., TCP, TLS/SSL, UDP).
	23.03 Describe the services and protocols used in the OSI Network Layer (i.e., IP, ICMP, IGMP, IPsec).
	23.04 Describe the services and protocols used in the OSI Data Link Layer (i.e., ARP, OSPF, L2TP, PPP).
24.0	Demonstrate proficiency using computer networks. The student will be able to:
	24.01 Define networking and describe the purpose of a network.
	24.02 Describe the conceptual background of digital networks and cloud computing including terminology and basics.
	24.03 Describe various types of networks and the advantages and disadvantages of each (e.g. peer-to-peer, client/server, ROI).
	24.04 Describe the use, advantages, and disadvantages of various network media (e.g. coaxial, twisted pair, fiber optics).
	24.05 Describe the function of various network devices (e.g. hub, switched hub or switch, router, bridge, gateway, access points).
	24.06 Describe how network devices are identified (i.e., IP addressing).
	24.07 Explain the protocols commonly used in a network environment.
	24.08 Differentiate between public and private IP addresses.
	24.09 Describe the common ports and corresponding protocols used in a network.
	24.10 Describe the difference between the Internet and intranet.
	24.11 Compare and contrast IP Version 4 (IPv4) and IP Version 6 (IPv6).
	24.12 Compare and contrast the different methods for network connectivity (e.g. broadband, wireless, Bluetooth, cellular).
	24.13 Discuss the differences between Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), Virtual Local Area Network (VLAN), and Virtual Private Network (VPN).
25.0	Describe and differentiate between serial, digital subscriber line (DSL), Metro Ethernet, and cable modem WAN connections. The student will be able to:
	25.01 Describe the various types of cloud computing (IaaS, PaaS, SaaS) and modes of delivery (Public, Private, Community, Hybrid).
	25.02 Describe practices that aid in protecting the Hybrid cloud model.
	25.03 Describe the challenges and solutions associated with securing embedded devices.
26.0	Demonstrate an understanding of basic security concepts. The student will be able to:

	26.01	Distinguish between vulnerability and a threat.
	26.02	Discuss the different types of attacks (e.g., active, passive).
	26.03	Define security policy and explain its role in cybersecurity.
	26.04	Describe the basic methods of authentication (e.g., password, biometrics, smart cards, two-factor authentication, multifactor authentication).
	26.05	Describe the various forms of encryption methodologies (e.g., symmetric, asymmetric, block cipher, stream cipher).
	26.06	Describe hash functions and their role in authentication.
	26.07	Describe various method of access control used in computer security (e.g., policies, groups, Access Control List (ACL)).
	26.08	Understand the concept of malware (i.e., ransomware, worms, viruses, adware) and how attackers use it to steal sensitive or confidential information.
27.0	Demonstrate an understanding of legal and ethical issues in cybersecurity. The student will be able to:	
	27.01	Define cybercrime and discuss the challenges facing law enforcement.
	27.02	Identify the key legislative acts that impact cybersecurity.
	27.03	Describe the Federal criminal code related to computers and give examples of cybercrimes and penalties, particularly those involving inappropriate access.
	27.04	Discuss the concept of digital forensics and its place in cybercrime investigations and incident response.
	27.05	Distinguish among the Intellectual Property Rights of trademark, patent, and copyright.
	27.06	Explain digital rights management and the implications of the Digital Millennium Copyright Act (DMCA).
	27.07	Describe the implications of various social media on the safeguarding of personal or sensitive information.
	27.08	Describe various safeguards that can be employed to help ensure that sensitive or confidential information is not inadvertently divulged or obtained.
28.0	Demonstrate an understanding of virtualization technology. The student will be able to:	
	28.01	Define virtual computing.
	28.02	Explain the benefits of virtual computing.
	28.03	Differentiate between guest and host operating systems.
	28.04	Install desktop virtualization software.
	28.05	Describe the role of the hypervisor.
	28.06	Create and upgrade a virtual machine.
	28.07	Optimize the performance of a virtual machine.
	28.08	Preserve the state of a virtual machine.

	28.09	Clone, move and share virtual machines.
	28.10	Use basic(static) and dynamic virtual disks and disk drives.
	28.11	Configure a virtual network.
	28.12	Connect devices to a virtual machine.
	28.13	Enable security settings on a virtual machine.
29.0	Recognize and understand the administration of the following types of remote access technologies. The student will be able to:	
	29.01	Configure 802.1x authentication for a given scenario.
	29.02	Connect clients to a VPN.
	29.03	Understand Authentication, Authorization and Accounting (AAA) management.
	29.04	Differentiate between TACACS+ (Terminal Access Controller Access Control System) and RADIUS.
	29.05	Differentiate between Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) protocols as they apply to VPN options.
	29.06	Implement the use of SSH (Secure Shell).
	29.07	Implement the use of IPsec (Internet Protocol Security).
	29.08	Identify vulnerabilities associated with authentication.
	29.09	Understand ways to implement VoIP technologies.
	29.10	Demonstrate the use and purpose of Kerberos.
30.0	Understand the application of the following concepts of physical security. The student will be able to:	
	30.01	Configure access controls including biometric devices, keypads and security tokens.
	30.02	Recognize social engineering attempts.
	30.03	Evaluate environmental controls (e.g., EMI shielding, temperature, humidity and fire suppression).
	30.04	Develop a method of training users to recognize, report and avoid social engineering attempts.
	30.05	Identify components of physical security including: mantraps, motion detection, alarm systems, locks, video surveillance, and fences/barricades.
	30.06	Install a camera for a video surveillance system.
	30.07	Configure an alarm system including a keypad and motion detector.
	30.08	Recognize vulnerabilities associated with physical security.
	30.09	Explain how a mantrap is used as a counter measure against tailgating.
31.0	Securely configure and maintain the following types of devices. The student will be able to:	

	31.01 Configure and maintain software and hardware firewalls.
	31.02 Configure and secure routers.
	31.03 Apply security settings to switches.
	31.04 Configure and secure wireless devices.
	31.05 Secure a LAN connected to a DSL/cable modem.
	31.06 Configure a RAS (Remote Access Server) for remote connectivity.
	31.07 Securely deploy a PBX (Private Branch Exchange).
	31.08 Explain the benefits of implementing a VPN (Virtual Private Network).
	31.09 Deploy IDS (intrusion detection system) and IPS (intrusion prevention systems).
	31.10 Analyze the performance, efficiency and security of the network based on network monitoring and diagnostic software.
	31.11 Employ techniques used to lock down workstations.
	31.12 Configure and secure servers for a given scenario.
	31.13 Understand and assess the security of mobile devices including but not limited to those using the Android, iOS and Windows platforms.
32.0	Understand the societal and security challenges of emerging technologies. The student will be able to:
	32.01 Explain the security implications of the Internet of Things (IoT) (e.g., understand the efforts to address authentication and updates to IoT devices).
	32.02 Explain societal and security challenges associated with robotics.
	32.03 Explain security challenges associated with serverless computing.
	32.04 Explain societal and security challenges associated with the implementation of 5G.
	32.05 Describe and explain the security challenges of Autonomous vehicles (i.e., the significance of vehicular cybersecurity and its relation to: computer vision, artificial intelligence, machine learning and Deep learning.)
33.0	Recognize and be able to differentiate and explain the following access control models. The student will be able to:
	33.01 Understand access control as it applies to MAC (Mandatory Access Control).
	33.02 Understand access control as it applies to DAC (Discretionary Access Control).
	33.03 Understand access control as it applies to RBAC (Role Based Access Control).
34.0	Understand the security concerns for the following types of media. The student will be able to:
	34.01 Understand and identify security concerns with the use of Coaxial Cable.
	34.02 The student should be able to identify and understand security concerns for UTP/STP (Unshielded Twisted Pair / Shielded Twisted Pair).

	34.03 Identify and understand security concerns fiber optic cable.
	34.04 Identify security concerns associated with removable media.
	34.05 Address pitfalls associated with tape backups.
	34.06 Apply drive encryption to hard drives.
	34.07 Secure flash drives.
	34.08 Smartcards and secure USB memory.
35.0	Explain the following security topologies as they relate to cybersecurity. The student will be able to:
	35.01 Determine Security Zones.
	35.02 Point out vulnerabilities on a DMZ (Demilitarized Zone).
	35.03 Explain the security benefits of using an intranet.
	35.04 Explain the security benefits of using an extranet.
	35.05 Secure a VLAN (Virtual Local Area Network).
	35.06 Describe the security benefits associated with NAT (Network Address Translation).
	35.07 Justify the implementation of tunneling, for security purpose.
36.0	Describe the roles within teams, work units, departments, organizations, inter-organizational systems, and the larger environment. The student will be able to:
	36.01 Describe the nature and types of business organizations.
	36.02 Explain the effect of key organizational systems on performance and quality.
	36.03 List and describe quality control systems and/or practices common to the workplace.
	36.04 Explain the impact of the global economy on business organizations.
	36.05 Display proficiency in using team-oriented collaboration and video teleconferencing software (e.g. Teams, Zoom).
37.0	Demonstrate an understanding of the technical underpinnings of cybersecurity and its taxonomy, terminology, and challenges. The student will be able to:
	37.01 Explain the various elements that make up the security taxonomy used by the U.S. Computer Emergency Readiness Team (CERT).
	37.02 Describe the challenges associated with achieving and maintaining computer security.
	37.03 Discuss the range of potential consequences of various forms of security breaches.
	37.04 Describe various defense mechanisms, techniques, and methodologies (e.g., antivirus, anti-malware, protocol analyzers and scans, analyzing email headers, patch management).
	37.05 Compare and contrast mechanisms employed in passive and active cyber-attacks.

	37.06	Describe vulnerabilities associated with each element of the CIA Triad.
	37.07	Explain the differences between hardware, software, data, and network assets susceptible to cyber-attack.
	37.08	Describe the tools and technologies used in cybersecurity.
	37.09	Define intrusion detection and discuss its role in cybersecurity (e.g., HIDS and NIDS).
	37.10	Explain what is meant by the term countermeasures (e.g., NIPS and HIPS).
	37.11	Describe the role recovery plays in cybersecurity (e.g., Business Continuity Plan).
38.0	Demonstrate an understanding of common information and computer system security vulnerabilities. The student will be able to:	
	38.01	Describe the basic categories of vulnerabilities associated with cybersecurity (i.e., hardware, software, network, human, physical, organizational).
	38.02	Describe the ways in which various social networks are cybersecurity targets.
	38.03	Describe footprinting and explain how it is used to reveal system vulnerabilities.
	38.04	Explain why default values and technical controls are points of vulnerability and describe the hardening efforts being taken by government and industry.
	38.05	Describe the process of port scanning and explain why it is so prevalent in cybersecurity.
	38.06	Describe what is meant by password strength and explain its relationship to vulnerability.
	38.07	Distinguish between a weak and a strong password.
	38.08	Describe some of the ways in which intruders can cover their tracks.
	38.09	Describe the circumstances under which a computer system is vulnerable to a denial of service attack.
39.0	Demonstrate an understanding of common cyber-attack mechanisms, their consequences, and motivation for their use. The student will be able to:	
	39.01	Describe spoofing as an attack mechanism and discuss its consequences and common motivating factors for its use.
	39.02	Describe the introduction of malware or spyware as an attack mechanism and discuss its consequences and common motivating factors for its use.
	39.03	Describe the use of grayware as an attack mechanism and discuss its consequences and common motivating factors for its use.
	39.04	Describe the use of computer viruses or worms as an attack mechanism and discuss its consequences and common motivating factors for its use.
	39.05	Describe Logic Bombs as an attack mechanism and discuss its consequences and common motivating factors for its use.
	39.06	Describe botnet and rootkit as an attack mechanism and discuss its consequences and common motivating factors for its use.
	39.07	Describe the introduction of a Trojan Horse as an attack mechanism and discuss its consequences and common motivating factors for its use.
	39.08	Describe DNS poisoning as an attack mechanism and discuss its consequences and common motivating factors for its use.

	39.09 Describe buffer overflow as an attack mechanism and discuss its consequences and common motivating factors for its use.
	39.10 Understand the risk associated with a zero-day exploit.
	39.11 Understand risks associated with P2P networking including the Gnutella protocol and Torrents.
	39.12 Describe the use of ransomware as an attack mechanism and discuss its consequences and common motivating factors for its use.
40.0	Be able to identify and explain the following different kinds of cryptographic algorithms. The student will be able to:
	40.01 Hashing Functions.
	40.02 Symmetric Keys.
	40.03 Asymmetric Keys.
41.0	Demonstrate an understanding of the following kinds of steganographic techniques and their use in cybersecurity. The student will be able to:
	41.01 Network steganographic methods (e.g., WLAN).
	41.02 Digital steganographic methods (e.g., image encryption, audio, mimic functions, video, packet manipulation).
	41.03 Understand how steganographic methods are used in malware.
42.0	Understand how cryptography and digital signatures address the following security concepts. The student will be able to:
	42.01 Confidentiality.
	42.02 Integrity.
	42.03 Authentication.
	42.04 Non-Repudiation.
	42.05 Access Control.
43.0	Understand and be able to explain the following concepts of PKI (Public Key Infrastructure). The student will be able to:
	43.01 Certificates (e.g., policies, practice statements).
	43.02 Revocation.
	43.03 Trust Models.
44.0	Demonstrate an understanding of certificates and their role in cybersecurity. The student will be able to:
	44.01 Describe the role of a Certificate Authority (CA).
	44.02 Describe Registration Authority (RA) and its relevance to security certificates.
	44.03 Compare and contrast SSL/TSL X.509-compliant certificates with PGP-compliant certificates.
	44.04 Describe the events that make up the lifecycle of a certificate.

	44.05 Describe how root certificate distribution works.
	44.06 Describe the role of a Certificate Revocation List (CRL).
	44.07 Describe the role of the Online Certificate Status Protocol (OCSP).
45.0	Demonstrate an understanding of intrusion, the types of intruders, their techniques, and their motivation. The student will be able to:
	45.01 Define intrusion.
	45.02 Describe the classes of intruders (i.e., masquerader, misfeasor, clandestine user).
	45.03 Describe what is meant by a hacker and discuss their role in cybersecurity.
	45.04 Compare and contrast the “black hat”, “white hat”, “blue hat”, and “grey hat” hacker cultures (i.e., computer criminal versus computer security expert).
	45.05 Describe various techniques used by hackers to achieve intrusion.
	45.06 Describe the difference between an inside and an outside attack.
46.0	Demonstrate an understanding of Intrusion Detection Systems (IDS). The student will be able to:
	46.01 Describe the three logical components of IDS (i.e., sensors, analyzers, user interface).
	46.02 Explain how user behavior relates to the detection of an intruder.
	46.03 Describe the essential requirements for any IDS.
47.0	Describe host-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature). The student will be able to:
	47.01 Describe anomaly detection, specifically threshold and profile-based approaches.
	47.02 Describe the types of audit records employed in intrusion detection (i.e., native, detection-specific).
	47.03 Describe signature detection, specifically rule-based anomaly and penetration identification approaches.
48.0	Describe network-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature). The student will be able to:
	48.01 Describe the primary approach for intrusion detection in a network.
	48.02 Compare and contrast inline and passive sensors.
	48.03 Discuss typical placement of sensors in a network-based IDS environment and explain the rationale for each.
49.0	Demonstrate an understanding of IDS applications. The student will be able to:
	49.01 Describe the operation, typical activities, and outputs of an intrusion detection system.
	49.02 Describe some of the limitations of intrusion detection systems.
	49.03 Differentiate between an intrusion detection system (passive) and an intrusion prevention (reactive) system.
	49.04 Compare and contrast several of the intrusion detection systems available on the current market.

50.0	Demonstrate an understanding of port scanning and network traffic monitoring employed as intrusion detection techniques. The student will be able to:
	50.01 Describe the process of monitoring/detecting port scanning attacks and associated patterns.
	50.02 Explain how the monitoring and analysis of network traffic can be used to detect intrusion.
	50.03 Utilize network monitoring and analysis tools to detect intrusion and anomalies.
51.0	Demonstrate an understanding of firewalls and other means of intrusion prevention. The student will be able to:
	51.01 Describe the purpose and limitations of firewalls.
	51.02 Describe the four types of firewalls (i.e., packet filtering, stateful inspection, application-level gateway, circuit-level gateway).
	51.03 Describe the use of honeypots as an intrusion prevention technique.
	51.04 Explain how security policies are used to prevent intruders.
	51.05 Explain how Access Control Lists (ACLs) are used to prevent intrusion.
52.0	Demonstrate an understanding of vulnerabilities unique to virtual computing environments. The student will be able to:
	52.01 Describe the limitations of traffic monitoring within virtual networks.
	52.02 Discuss the primary vulnerability of virtual operating systems.
	52.03 Describe the “hypervisor” and explain its role in securing a virtual environment.
53.0	Demonstrate an understanding of social engineering and its implications to cybersecurity. The student will be able to:
	53.01 Define social engineering and describe its role in cybersecurity.
	53.02 Discuss common mechanisms that constitute social engineering (e.g., phishing, baiting, quid pro quo, pretexting).
	53.03 Describe the variety of attacks targeting the human element.
	53.04 Describe countermeasures that can be used to counter social engineering attacks.
54.0	Demonstrate an understanding of fundamental security design principles and their role in limiting points of vulnerability. The student will be able to:
	54.01 Discuss the three over-arching security design principles (i.e., only necessary, simple, ease of use).
	54.02 Describe the principle of least privilege as it relates to computer security.
	54.03 Describe the principle of separation of duties as it relates to computer security.
	54.04 Describe the principle of defense in depth as it relates to computer security.
	54.05 Describe the principle of fail secure or fail safe and false positive or false negative as it relates to computer security.
	54.06 Describe the principle of economy of mechanism as it relates to computer security.
	54.07 Describe the principle of complete mediation as it relates to computer security.

	54.08 Describe the principle of open design as it relates to computer security.
	54.09 Describe the principle of least common mechanism as it relates to computer security.
	54.10 Describe the principle of psychological acceptability as it relates to computer security.
	54.11 Describe the principle of leveraging existing components as it relates to computer security.
	54.12 Describe the principle of weakest link as it relates to computer security.
	54.13 Describe the principle of single point of failure as it relates to computer security.
55.0	Demonstrate an understanding of how to configure host systems to guard against cyber intrusion. The student will be able to:
	55.01 Describe the security features and options available for configuring network routers to prevent intrusion.
	55.02 Describe the various types of firewalls (i.e., packet filtering, stateful, application-level gateway, circuit-level gateway) and how each can be used to prevent intrusion.
	55.03 Explain the configuration and operation of a Demilitarized Zone (DMZ) host, including the key services contained within the zone.
	55.04 Describe the role of security zones, content filters, subnets, and trusted zones in configuring a network infrastructure.
56.0	Demonstrate an understanding of authentication methods and strategies. The student will be able to:
	56.01 Describe the strengths, vulnerabilities, and countermeasures related to the use of passwords for authentication.
	56.02 Describe ways in which passwords are compromised and techniques/models for strengthening.
	56.03 Explain token authentication methods (e.g., memory cards, smart cards) and limitations.
57.0	Demonstrate an understanding of methods and strategies for controlling access to computer networks. The student will be able to:
	57.01 Compare and contrast the three primary categories of access control (i.e., discretionary, mandatory, role-based).
	57.02 Describe the underlying principles of authorization as an access control mechanism applicable to individuals, system services, subjects, objects.
	57.03 Discuss the key features of an access control system (i.e., reliable input, granularity, least privilege, separation of duty, open/close policies, conflict resolution, administration).
	57.04 Describe the three elements of access control (i.e., subject, object, rights).
	57.05 Describe access rights (i.e., read, write, execute, delete, create, search) and their use in establishing individual and group access control policies.
	57.06 Compare and contrast the use, operation, and limitations of Access Control Matrix (ACM), Access Control Lists (ACLs), and Capability Tickets in a network environment.
	57.07 Describe the UNIX file access control schema.
	57.08 Explain the relationship between security policies and access control.
	57.09 Describe the use and conceptual operation of formal security policy models (e.g., Bell-La Padula (BLP), Chinese Wall Model (CWM), Harrison Ruzzo Ullman (HRU)).

	57.10	Describe the use, strengths, and vulnerabilities of group policies in access control and strategies for ensuring safety.
	57.11	Describe the key entities, relationships, and functions that comprise Role-Based Access Control (RBAC), including privilege management considerations.
58.0	Demonstrate an understanding of key network services, their operation, vulnerabilities, and ways in which they may be secured. The student will be able to:	
	58.01	Describe the operation of Dynamic Host Configuration Protocol (DHCP), its vulnerabilities, typical cyber-attacks, and potential countermeasure strategies.
	58.02	Describe the operation of the Domain Name System (DNS) service, its role in a network environment, its vulnerabilities, typical cyber-attacks, and potential countermeasure strategies.
	58.03	Describe the operation of the Simple Mail Transport Protocol (SMTP), its role in a network environment, its vulnerabilities, typical cyber-attacks, and potential countermeasure strategies.
	58.04	Describe the operation of the File Transfer Protocol (FTP) and Telnet, their role in a network environment, their vulnerabilities, typical cyber-attacks, and potential countermeasure strategies.
59.0	Demonstrate an understanding of the processes involved in hardening a computer system or network. The student will be able to:	
	59.01	Describe hardening and some of the general approaches for securing a computer network.
	59.02	Describe and apply the process by which a web server is hardened against their typical cyber-attacks.
	59.03	Describe and apply the process by which a mail server is hardened against their typical cyber-attacks.
	59.04	Describe and apply the process by which a FTP server is hardened against their typical cyber-attacks.
	59.05	Describe and apply the process by which a file/print server is hardened against their typical cyber-attacks.
	59.06	Describe and apply the process by which data repositories are hardened against their typical cyber-attacks.
	59.07	Describe and apply the process by which Directory Services is hardened against their typical cyber-attacks.
	59.08	Describe and apply the process by which various network appliances are hardened against their typical cyber-attacks.
60.0	Demonstrate an understanding of Public Key Infrastructure (PKI) management functions, key states, and life cycle/transition considerations. The student will be able to:	
	60.01	Compare and contrast the forms, limitations, and vulnerabilities associated with centralized and decentralized key management schemas, including the PKI web of trust model.
	60.02	Describe key escrow, its role in key management, its advantages, and its risks.
	60.03	Differentiate between key backup and key escrow.
	60.04	Explain the role of a key's expiration date, its implications on the key's validity, and its relationship to deactivation.
	60.05	Describe the circumstances under which a key might be revoked, who has authority to revoke a key, and how revocation is communicated.
	60.06	Compare and contrast key suspension and key revocation.
	60.07	Describe ways in which key recovery might be achieved, who is authorized to recover keys, and associated vulnerabilities to attack.

	60.08	Compare and contrast key renewal and key replacement, who is authorized to initiate renewal or replacement, and associated vulnerabilities to attack.
	60.09	Describe the circumstances under which a key might be destroyed, the considerations prior to destruction, and associated vulnerabilities to compromise or attack.
61.0	Demonstrate an understanding of the processes associated with assessing vulnerabilities and risks within an organization. The student will be able to:	
	61.01	Describe the process of asset identification relative to risk assessment and the considerations or criteria used in identifying assets requiring protection and understand how to leverage a configuration management database (CMDB) for asset management.
	61.02	Describe the process of threat identification, including identifying the types of threats, asset vulnerabilities, and threat sources.
	61.03	Describe the process of risk assessment, including determination of attack probability, attack consequences, and assignment of risk priorities.
	61.04	Evaluate an existing security posture and identify gaps and vulnerabilities in security.
	61.05	Describe the role of governance, risk, and compliance in achieving a more secure organization.
	61.06	Describe the concepts of Key Performance Indicators and Risk Measurement. (e.g., annualized loss expectancy (ALE), annual rate of occurrence (ARO), single loss expectancy (SLE), Exposure Factor (EF).)
	61.07	Analyze and apply data and measurements to solve business problems and relate it to IT risk and business continuity.
62.0	Demonstrate an understanding of penetration testing, the types of tests and metrics, testing methodologies, and reporting processes. The student will be able to:	
	62.01	Describe the types of penetration tests (i.e., human, physical, wireless, data networks, telecommunications), the goals of each type, the metrics tested, and the value of their results.
	62.02	Compare and contrast the processes of black box versus white box penetration testing, including their characteristics, limitations, and appropriateness.
	62.03	Define attack vector and explain its relationship and importance to penetration testing.
	62.04	Describe common testing methodologies and standards used in penetration testing.
	62.05	Describe the salient points, structure, detail, and documentation typically addressed in reporting and debriefing the results of penetration testing.
	62.06	Detect malicious and abnormal activities through logs, intrusion detection systems, and other utilities and appliances.
	62.07	Reproduce methods that intruders use to gain unauthorized access to a network system for purposes of compromising information assets.
	62.08	Deploy proprietary and/or open source tools to test known technical vulnerabilities in networked systems.
	62.09	Determine which vulnerabilities are exploitable and estimate the risk and impact of potential exploitations.
	62.10	Recommend appropriate mitigation procedures against discovered vulnerabilities and security gaps.
	62.11	Model the ethics of a licensed Penetration Tester or Computer Security Specialist.
63.0	Demonstrate an understanding of the Incident Response Life Cycle and the activities comprising each phase. The student will be able to:	

63.01	Describe the activities that make up the Preparation Phase of the Incident Response Life Cycle (e.g., identification of useful tools and resources, setting up a war room, securing communications, creating a governance team, identifying key stakeholders for response activities.)
63.02	Describe the activities that make up the Detection and Analysis Phase of the Incident Response Life Cycle, including identification of indication sources, analysis of resulting signs of an intrusion event, documentation and notification of the incident.
63.03	Describe the factors to consider when prioritizing an incident.
63.04	Describe the activities that make up the Containment, Eradication, and Recovery Phase of the Incident Response Life Cycle, including selecting a containment strategy, collecting and preserving evidence for forensic analysis, identifying the attacker, re-securing the system and system restoration.
63.05	Describe the activities that make up the Post Incident Activity Phase of the Incident Response Life Cycle, including identification of lessons learned and evidence retention.

Course Number: CTS0019 Occupational Completion Point: B Information Security Manager – 150 Hours	
64.0	Demonstrate proficiency in cybersecurity risk mitigation planning. The student will be able to:
64.01	Describe the major activities and security controls that are implemented as part of a sound risk management program.
64.02	Discuss the rationale for executive sponsorship and delineated management responsibilities in successfully implementing a risk management program.
65.0	Demonstrate proficiency in establishing a risk management framework. The student will be able to:
65.01	Describe the importance of creating a system definition for use in assessing vulnerabilities and risks.
65.02	Describe the major elements of a system definition.
65.03	Differentiate among critical assets, cyber assets, and critical cyber assets.
65.04	Explain why cyber assets are classified as public, restricted, confidential, or private and why this plays a role in creating a risk management framework.
65.05	Compare and contrast the classes of cyber assets (i.e., public, restricted, confidential, private) and give examples of each.
65.06	Create a system definition that identifies all cyber assets, their class, and their risk category (e.g., critical).
65.07	Describe an Electronic Security Perimeter (ESP) and discuss its role in formulating a risk management framework.
65.08	Describe the process and goals of a vulnerability assessment of ESP access points.
65.09	Define risk level and explain the variabilities of its components.
65.10	Describe ways in which system vulnerability may be ranked according to impact (e.g., safety, outage, privacy, monetary).
65.11	Describe some of the security controls (e.g., access control, training, audit, configuration, maintenance) that come into play when determining the appropriate risk mitigation strategy.

	65.12 Compare and contrast a top-down and a bottoms-up analysis approach for identifying and mitigating risks.
	65.13 Describe the range of testing/evaluation and associated tools used to monitor mitigation control effectiveness.
	65.14 Create a risk management framework.
66.0	Demonstrate proficiency in creating a corporate security policy. The student will be able to:
	66.01 Describe the best practices and security controls that typify a sound corporate security policy.
	66.02 Discuss the elements of a corporate security policy, including policy management, personnel and training, critical asset management, ESP, physical security, incident reporting and response, disaster recovery and business continuity plans.
	66.03 Describe the need for specific implementation and enforcement processes as part of a corporate security policy.
	66.04 Explain the controls required for addressing personnel risks in a corporate security policy (e.g., training, hiring due diligence, enforcement of “least privilege,” access revocation).
67.0	Demonstrate proficiency in addressing process risks. The student will be able to:
	67.01 Describe the best practices and security controls typically implemented for assessing and mitigating operational risks, including:
	• Conduct periodic posture risk assessments.
	• Enforce access control, monitoring, and logging.
	• Perform disposal/redeployment of assets.
	• Enforce change control and configuration management.
	• Conduct vulnerability assessments.
	• Control, Monitor, and log all access to assets.
	• Configuration and maintenance.
	• Ensure incident-handling processes.
	• Provide for contingency planning.
	67.02 Create an organized mitigation table that identifies operational or process risks, the potential impact of the risk, and specific actions required to mitigate the risk.
68.0	Demonstrate proficiency in addressing physical security risks. The student will be able to:
	68.01 Describe the best practices and security controls that ensure good physical security of critical infrastructure and assets.
	68.02 Discuss the resulting potential for compromise once physical security is breached.
	68.03 Create an organized mitigation table that identifies physical security risks, the potential impact of the risk, and specific actions required to mitigate the risk.
69.0	Demonstrate proficiency in cybersecurity contingency planning. The student will be able to:
	69.01 Define resiliency and its relationship to contingency planning.

	69.02	Describe the purpose and scope of an Information Systems Contingency Plan (ISCP).
	69.03	Identify the five main components of a contingency plan (i.e., Supporting Information, Activation and Notification, Recovery, Reconstitution, and Appendices).
	69.04	Describe the contingency planning process and the rationale for each step in the process.
	69.05	Explain the three step process for conducting a business impact analysis (i.e., determine recovery criticality, identify resource requirements, identify recovery priorities).
	69.06	Compare and contrast Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO).
	69.07	Discuss the criteria typically used to activate the contingency plan.
	69.08	Discuss the role of backup and recovery considerations in contingency planning.
	69.09	Create a contingency plan that includes roles and responsibilities, a business impact analysis with contingency strategies/solutions, outage assessment, resource recovery priorities, backup and recovery strategies, and testing/training considerations.
70.0	Demonstrate proficiency in cybersecurity disaster recovery planning. The student will be able to:	
	70.01	Describe the purpose and scope of a cybersecurity disaster recovery plan.
	70.02	Describe various recovery strategies according to their appropriateness.
	70.03	Explain the key considerations when formalizing a disaster recovery plan.
	70.04	Discuss the role of data collection relative to disaster recovery.
	70.05	Identify the types, purposes, and role of documentation during disaster recovery.
	70.06	Discuss the role of testing in a disaster recovery plan.
71.0	Demonstrate proficiency in cybersecurity business continuity planning. The student will be able to:	
	71.01	Describe the purpose and scope of a cybersecurity business continuity plan.
	71.02	Explain the concept of fault tolerance and discuss its role in business continuity planning.
	71.03	Identify and use various utilities employed for the purpose of business continuity.
	71.04	Describe the role of backups for ensuring business continuity.
72.0	Demonstrate proficiency in the essential elements of forensic analysis. The student will be able to:	
	72.01	Describe the four phases of forensic analysis and discuss the activities performed in each phase.
	72.02	Describe the forensic and evidentiary considerations when determining containment.
	72.03	Describe the types and sources of data collected for forensic analysis.
	72.04	Explain the various forms of data and associated collection/retrieval tools for the application transport, IP, and link layers.
	72.05	Explain the processes by which data is collected for analysis.

72.06	Describe the role of system event logs in data collection.
72.07	Describe the role of the process log in data collection.
72.08	Describe the processes associated with preserving evidence collected for forensic purposes.
72.09	Describe how the chain of custody can be maintained for evidence collected during a forensic analysis effort.
Course Number: CTS0021 Occupational Completion Point: B Data Security Specialist – 150 Hours	
73.0	Demonstrate an understanding of database design, structure, and operation. The student will be able to:
73.01	Describe a relational database and its key elements.
73.02	Describe the Entity Relationship Model (ERM) and relate how it is a factor in database security.
73.03	Describe the process of normalization and explain its role in database security.
73.04	Differentiate between one-to-many, many-to-many and one-to-one relationships.
73.05	Define referential integrity and describe its implications on database security.
73.06	Discuss the role of authentication in database security.
74.0	Demonstrate a fundamental understanding of Structured Query Language (SQL). The student will be able to:
74.01	List the capabilities of SQL SELECT statements.
74.02	Execute basic SQL statements, including SELECT, INSERT, and UPDATE.
74.03	Apply the concatenation operator to link columns to other columns, arithmetic expressions, or constant values to create a character expression.
74.04	Use column aliases to rename columns in the query result.
74.05	Use SQL to display the structure of a table.
74.06	Apply SQL syntax to restrict the rows returned from a query.
74.07	Demonstrate application of the WHERE clause syntax.
74.08	Apply the proper comparison operator to return a desired result.
74.09	Create, drop, rename and truncate tables using SQL.
74.10	Create and remove an index using a SQL statement.
74.11	Create or modify users and roles using SQL statements.
74.12	Use the GRANT and REVOKE SQL statements to control access.

	74.13 Differentiate between Data Definition Language (DDL) and Data Manipulation Language (DML) SQL statements and discuss their respective implications to database security.
75.0	Demonstrate an understanding of database security policies. The student will be able to:
	75.01 Explain the role of the Database Management System (DBMS) in maintaining database security.
	75.02 Describe three aspects of system level security related to databases (i.e., user privilege schema, user authentication, operating system level privileges).
	75.03 Describe the mechanisms that control access to and use of the database at the object level.
	75.04 Explain how role-based privilege assignment can be used as a data security model.
	75.05 Compare and contrast the implications of connecting to a database with administrator versus user privileges.
76.0	Demonstrate an understanding of database access control, functions, methods, and verification. The student will be able to:
	76.01 Compare and contrast rights and privileges as they relate to database security.
	76.02 Describe the manner in which database user rights and privileges are controlled (e.g., granted, revoked).
	76.03 Describe application access rights and discuss their role in a database security schema.
	76.04 Compare and contrast table, column, and row level security, including VIEW implications.
	76.05 Describe fine-grained access control and its use in database security.
	76.06 Describe the operation of a database firewall and explain its role in a database security schema.
	76.07 Describe how database security policies may be used to trigger security auditing events.
	76.08 Describe the various types of auditing (e.g., statement, privilege, object, fine-grained) and associated records.
77.0	Demonstrate an understanding of database vulnerabilities, attack vectors, and associated countermeasures. The student will be able to:
	77.01 Describe the SQL Injection attack vector and explain its potential consequences (e.g., privilege escalation, data compromise, data destruction).
	77.02 Describe database inference as a vulnerability and explain how sensitive information can be compromised inadvertently.
	77.03 Discuss ways in which to prevent or limit database inference at design time and query time.
	77.04 Compare and contrast the various countermeasures and strategies to prevent an SQL injection from being successful.
	77.05 Compare and contrast the ways in which encryption might be applied to a database (i.e., database, fields, records, columns) and discuss the tradeoffs of each.
78.0	Demonstrate an understanding of pre- and post-intrusion actions to facilitate database recovery. The student will be able to:
	78.01 Describe the criteria that might be employed to trigger an intrusion or breach alarm.
	78.02 Identify the sources for confirming and tracking intrusion.
	78.03 Describe the tools and methodologies used to determine the scope of data compromise.

	78.04 Assess an intrusion, determine the scope of compromise, and restore compromised data.
	78.05 Describe the appropriate actions related to database recovery during incidence response.
Course Number: CTS0060 Occupational Completion Point: B Software Security Specialist – 150 Hours	
79.0	Demonstrate an understanding of software design, structure, and operation. The student will be able to:
	79.01 Describe a typical software application and its key elements.
	79.02 Compare and contrast software quality and software security in terms of development time, testing, and implementation.
	79.03 Explain how security can be a software design parameter and discuss the inherent trade-offs during the development life cycle.
	79.04 Describe the common failings in software security (e.g., input handling, inadequate testing, incomplete/incorrect algorithms, memory misuse, holes for privilege escalation).
80.0	Demonstrate a fundamental understanding of common software attack vectors. The student will be able to:
	80.01 Describe how buffer overflow attacks can be prevented through input validation and proper interpretation.
	80.02 Describe a command injection attack, how it can occur, and the potential consequences.
	80.03 Describe an SQL injection attack, how it can occur, and the potential consequences.
	80.04 Describe a code injection attack, including PHP remote code injection, how it can occur, and the potential consequences.
	80.05 Describe cross-site scripting attack, how it can occur, and the potential consequences.
81.0	Demonstrate an understanding input syntax validation. The student will be able to:
	81.01 Explain the need for validating input syntax to ensure proper input handling.
	81.02 Describe canonicalization and its role in handling alternate encoding schemas.
	81.03 Discuss the risks associated with improper handling of signed or unsigned numeric input (e.g., very large data length versus negative number).
82.0	Demonstrate an understanding of best practices for processing input data to ensure safe and secure program code. The student will be able to:
	82.01 Explain why any input processing algorithm must correctly handle all problem variants.
	82.02 Explain why debug or test code should be removed from all production bound software.
	82.03 Describe the need for ensuring that machine instructions correctly implement the intended actions of the high-level language code.
	82.04 Describe the concept of a strongly typed programming language and explain its role in correct data interpretation.
	82.05 Describe memory leak as it pertains to dynamically allocated memory, its causes, and potential consequences (e.g., DOS attack).

	82.06 Describe the race condition associated with shared memory access, its causes, and potential consequences (e.g., DOS attack causing deadlock).
83.0	Demonstrate an understanding of the role of environment variables in the operation of software applications. The student will be able to:
	83.01 Describe how the PATH, IFS, and LD_LIBRARY_PATH environment variables can be exploited.
	83.02 Explain how dynamic libraries can be subverted through the use of environment variables and describe the potential consequences (e.g., elevated privileges).
	83.03 Describe the principle of "least privilege" relative to the operation of software applications, particularly as it relates to file/directory ownership management.
84.0	Demonstrate an understanding of program design strategies for inhibiting elevated privilege attacks. The student will be able to:
	84.01 Describe a Root/Admin program and explain the development and operational benefits of partitioning the program into smaller modules.
	84.02 Identify the sources for confirming and tracking intrusion.
	84.03 Describe the tools and methodologies used to determine the scope of data compromise.
	84.04 Assess an intrusion, determine the scope of compromise, and restore compromised data.
	84.05 Describe the appropriate actions related to database recovery during incidence response.
Course Number: CTS0085 Occupational Completion Point: B Web Security Specialist – 150 Hours	
85.0	Demonstrate an understanding of the primary security services used in Internet and intranet environments. The student will be able to:
	85.01 Describe Secure Sockets Layer (SSL) security service.
	85.02 Compare and contrast SSL with Transport Layer Security (TLS) as a security service.
	85.03 Describe Internet Protocol Security (IPsec) and discuss its benefits and three functional areas (i.e., authentication, confidentiality, key management).
	85.04 Describe Secure/Multipurpose Internet Mail Extension (S/MIME) and discuss its role in achieving secure Internet-based communications.
86.0	Demonstrate a fundamental understanding of the SSL protocol stack and its elements. The student will be able to:
	86.01 Compare and contrast SSL Connection and SSL Session.
	86.02 Describe SSL Record Protocol services and discuss their role in managing SSL exchanges (i.e., message integrity, confidentiality).
	86.03 Describe the operation of the SSL Record Protocol, including the key steps that ensure security (e.g., adding message authentication code, encryption).
	86.04 Explain the role of the SSL Change Cipher Spec Protocol in ensuring secure transactions.

	86.05	Explain the role of the SSL Alert Protocol.
	86.06	Describe the SSL Handshake Protocol and explain the role of each phase of communication (i.e., establish security capability, server authentication/key exchange, client authentication/key exchange, complete secure connection).
87.0	Demonstrate an understanding of IPsec, including its uses, elements, and mechanisms. The student will be able to:	
	87.01	Compare and contrast IPsec with SSL and TSL.
	87.02	Compare and contrast security services provided under IPv4 and IPv6.
	87.03	Differentiate between the three facilities available under IPsec (i.e., Authentication Header, Encapsulating Security Payload, key exchange).
	87.04	Describe the concept of Security Association (SA) and explain the roles of its three parameters (i.e., Security Parameters Index, IP Destination Address, Security Protocol Identifier).
	87.05	Describe the purpose, structure, and criteria of the Authentication Header (AH).
	87.06	Describe the purpose, structure, and elements of the Encapsulating Security Protocol (ESP).
	87.07	Describe the structure and operation of the key management facility of IPsec.
88.0	Demonstrate an understanding of S/MIME, including its uses, functions, cryptographic algorithms, and key certificates. The student will be able to:	
	88.01	Describe the role of S/MIME in conducting email communications.
	88.02	Compare and contrast the four new security functions provided by S/MIME (i.e., enveloped data, signed data, clear-signed data, signed and enveloped data).
	88.03	Outline the process of using S/MIME during email processing.
	88.04	Describe the various cryptographic algorithms used by S/MIME and discuss their applicability (i.e., DSS, RSA, SHA-1, MD5, ElGamal, AES, 3DES, HMAC).
	88.05	Describe memory leak as it pertains to dynamically allocated memory, its causes, and potential consequences (e.g., DOS attack).
	88.06	Describe the need for using x.509 v3 public key certificates with S/MIME.
89.0	Demonstrate an understanding of Kerberos and its role in third-party authentication in a distributed network. The student will be able to:	
	89.01	Compare and contrast the roles and operation of a Kerberos Authentication Server (AS) and a Ticket Granting Server (TGS).
	89.02	Describe a Kerberos realm and the mechanism for inter-realm authentication.
90.0	Demonstrate an understanding of identity management and ways in which secure identify information is exchanged across different domains. The student will be able to:	
	90.01	Describe the key components of identity management architecture.
	90.02	Describe the concept of identity federation and explain its benefits.
	90.03	Describe the standards used in federated identity management (i.e., XML, SOAP, WS-Security, SAML).

Course Number: CTS0089 **Occupational Completion Point: B** **Information Security Administrator – 150 Hours**	
91.0	Complete a safety skills inventory. The student will be able to:
91.01	Practice safety procedures while enrolled in this course.
91.02	Demonstrate an understanding of safety and general policies and procedures.
92.0	Demonstrate acceptable project values. The student will be able to:
92.01	Maintain a positive relationship with peers.
92.02	Demonstrate adaptive self-management skills.
92.03	Adhere to industry accepted, legal, and ethical standards of cyber conduct.
92.04	Rotate through a wide variety of increasingly responsible experiences.
92.05	Apply superior skills in communications, mathematics, and science appropriate to technological content and learning activities.
93.0	Demonstrate the ability to detect and resolve system vulnerabilities. The student will be able to:
93.01	Prepare a vulnerability matrix to identify and record weak points, the type of vulnerability, significance of the vulnerability, the priority, and the solution.
93.02	Determine possible solutions for each vulnerability.
93.03	Research each detected vulnerability.
93.04	Document solutions as they are devised.
93.05	Prepare an alternative for any solution that is not successful.
93.06	Continue the process until a workable solution is found for each vulnerability.
94.0	Plan, organize, and carry out a penetration-testing plan. The student will be able to:
94.01	Determine the scope and attack vectors for the test.
94.02	Organize the team according to individual strengths.
94.03	Assign specific tasks within a team.
94.04	Prioritize the attack vectors and sequence the test.
94.05	Identify required resources.
94.06	Carry out the testing plan to successful completion.
94.07	Create the test report detailing the goals, tests, findings, and results.

95.0	Demonstrate proficiency in conducting forensic analysis. The student will be able to:
95.01	Create security incident handling and response policies.
95.02	Recover deleted, encrypted, or damaged file information as evidence for prosecution in computer crimes.
95.03	Deploy proprietary and/or open source tools to identify intruder footprints.
95.04	Coordinate incident response activities.
95.05	Prepare proper documentation of chain of custody, including accounting for evidence source, destination, and possession.
95.06	Preserve forensic integrity of evidence.
95.07	Model highest moral and ethical standards in conducting digital forensic investigations.
96.0	Successfully work as a member of a team. The student will be able to:
96.01	Accept responsibility for specific tasks in a given situation.
96.02	Document progress, and provide feedback on work accomplished in a timely manner.
96.03	Complete assigned tasks in a timely and professional manner.
96.04	Reassign responsibilities when the need arises.
96.05	Complete daily tasks as assigned on one's own initiative.
97.0	Manage time according to a plan. The student will be able to:
97.01	Set realistic time frames and schedules.
97.02	Record time worked in the daily journal.
97.03	Meet goals and objectives set by the team.
97.04	Identify individual priorities.
97.05	Complete a weekly evaluation of accomplishments, and reevaluate goals, objectives and priorities as needed.
98.0	Keep acceptable records of progress problems and solutions. The student will be able to:
98.01	Develop a record keeping system in the form of a logbook or journal to record daily progress.
98.02	Use a project journal to identify problem statement.
98.03	Develop a portfolio of work accomplished to include design drawings, research, drawings and plans, storyboards, models, mock-ups and prototypes.
99.0	Manage resources. The student will be able to:
99.01	Identify required resources for each stage of the project plan.
99.02	Determine the methods needed to acquire needed resources.

	99.03 Demonstrate good judgment in the use of resources.
	99.04 Recycle and reuse resources where appropriate.
	99.05 Demonstrate an understanding of proper legal and ethical treatment of copyrighted material.
100.0	Use tools, materials, and processes in an appropriate and safe manner. The student will be able to:
	100.01 Identify the proper tool for a given job.
	100.02 Use tools and machines in a safe manner.
	100.03 Adhere to laboratory or job site safety rules and procedures.
	100.04 Identify the application of processes appropriate to the task at hand.
	100.05 Identify materials appropriate to their application.
101.0	Research content related to the project and document the results. The student will be able to:
	101.01 Identify the basic research needed to develop the project plan.
	101.02 Identify available resources for completing background research required in the project plan.
	101.03 Demonstrate the ability to locate resource materials in a library, database, internet and other research resources.
	101.04 Demonstrate the ability to organize information retrieval.
	101.05 Demonstrate the ability to prepare a topic outline.
	101.06 Write a draft of the design and testing report.
	101.07 Edit and proof the respective report.
	101.08 Prepare an electronically composed report in proper form.
102.0	Use presentation skills, and appropriate media to describe the progress, results and outcomes of the experience. The student will be able to:
	102.01 Prepare a multi-media presentation on the completed project.
	102.02 Make an oral presentation, using multi-media materials.
	102.03 Review the presentation, and make changes in the delivery method(s) to improve presentation skills.
103.0	Demonstrate competency in the area of expertise related to the Applied Cybersecurity education program previously completed that this project is based upon. The student will be able to:
	103.01 Demonstrate a mastery of the content of the selected subject area.
	103.02 Demonstrate the ability to use related technological tools, materials and processes related to the specific program area.
	103.03 Demonstrate the ability to apply the knowledge, experience and skill developed in the previous program completion to the successful completion of this demonstration.

103.04 Demonstrate the acquisition of additional knowledge, skill and experience in one area of the selected field of study beyond the performance standards of the initial program standards.

Additional Information

Laboratory Activities

Laboratory investigations that include scientific inquiry, research, measurement, problem solving, emerging technologies, tools and equipment, as well as, experimental, quality, and safety procedures are an integral part of this career and technical program/course. Laboratory investigations benefit all students by developing an understanding of the complexity and ambiguity of empirical work, as well as the skills required to manage, operate, calibrate and troubleshoot equipment/tools used to make observations. Students understand measurement error; and have the skills to aggregate, interpret, and present the resulting data. Equipment and supplies should be provided to enhance hands-on experiences for students.

Career and Technical Student Organization (CTSO)

Phi Beta Lambda (PBL) and Business Professionals of America (BPA) are the co-curricular student organizations providing leadership training and reinforcing specific career and technical skills. Career and Technical Student Organizations provide activities for students as an integral part of the instruction offered.

Cooperative Training – OJT

On-the-job training is appropriate but not required for this program. Whenever offered, the rules, guidelines, and requirements specified in the OJT framework apply.

Basic Skills

In Career Certificate Programs offered for 450 hours or more, in accordance with Rule 6A-10.040, F.A.C., the minimum basic skills grade levels required for postsecondary adult career and technical students to complete this program are: Computation (Mathematics) and Communications (Reading and Language Arts). These grade level numbers correspond to a grade equivalent score obtained on a state designated basic skills examination.

Adult students with disabilities, as defined in Section 1004.02, Florida Statutes, may be exempted from meeting the Basic Skills requirements (Rule 6A-10.040). Students served in exceptional student education (except gifted) as defined in s. 1003.01, F.S., may also be exempted from meeting the Basic Skills requirement. Each school district and Florida College must adopt a policy addressing procedures for exempting eligible students with disabilities from the Basic Skills requirement as permitted in Section 1004.91, F.S.

Accommodations

Federal and state legislation requires the provision of accommodations for students with disabilities to meet individual needs and ensure equal access. Postsecondary students with disabilities must self-identify, present documentation, request accommodations if needed, and develop a plan with their counselor and/or instructors. Accommodations received in postsecondary education may differ from those received in secondary education. Accommodations change the way the student is instructed. Students with disabilities may need accommodations in such areas as

instructional methods and materials, assignments and assessments, time demands and schedules, learning environment, assistive technology and special communication systems. Documentation of the accommodations requested and provided should be maintained in a confidential file.

Note: postsecondary curriculum and regulated secondary programs cannot be modified.