Florida Department of Education
Curriculum Framework

Program Title: **Cybersecurity Operations**
Career Cluster: **Information Technology**

AS	
CIP Number	1511100300
Program Type	College Credit
Standard Length	60 credit hours
CTSO	Phi Beta Lambda, BPA
SOC Codes (all applicable)	15-1121 – Computer Systems Analysts 15-1122 – Information Security Analysts 15-1152 – Computer Network Support Specialists 15-1142 – Network and Computer Systems Administrators
CTE Program Resources	http://www.fldoe.org/academics/career-adult-edu/career-tech-edu/program-resources.stml

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 careers such as, cybersecurity operations analyst, security engineer, cybersecurity operations technician, data communication analyst, intrusion and detection analyst, security architect, or secure software developer in the Information Technology career cluster; which 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 the Information Technology career cluster.

The content includes but is not limited to the fundamentals of network security, installing, configuring, monitoring, and detecting network violations in the LAN/WAN environment.

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

Program Structure

This program is a planned sequence of instruction consisting of 60 credit hours.

Standards

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

01.0 Demonstrate a fundamental understanding of computer networking.
02.0 Demonstrate understanding of networked environments, hardware, and software.
03.0 Demonstrate fundamental proficiency in network security essentials.
04.0 Demonstrate an understanding of the directory services infrastructure and installation.
05.0 Demonstrate an understanding of network access control systems and methodology.
06.0 Demonstrate understanding of routing concepts.
07.0 Demonstrate understanding of routing protocols.
08.0 Demonstrate router configuration skills.
09.0 Perform coding activities
10.0 Perform programming and scripting activities.
11.0 Demonstrate proficiency with Internet structure, organization, and navigation.
12.0 Perform web design/development activities.
13.0 Demonstrate proficiency in analyzing network intrusions
14.0 Demonstrate proficiency in incident handling and response.
15.0 Demonstrate an understanding of how to mitigate network vulnerabilities.
16.0 Legal and ethical issues relative to the information technology environment.
17.0 Communications skills.

Florida Department of Education
Student Performance Standards

Program Title: **Cybersecurity Operations (60)**
CIP Number: **1511100300**
Program Length: **60 credit hours**
SOC Code(s): **15-1121, 15-1122, 15-1152, 15-1142**

Refer to Rule 6A-14.030 (4), F.A.C., for the minimum amount of general education coursework required in the Associate of Science (AS) degree. At the completion of this program, the student will be able to:	
01.0	Demonstrate a fundamental understanding of computer networking. The student will be able to:
01.01	Explain the use of binary numbers and perform binary arithmetic.
01.02	Describe current network environments.
01.03	Describe network communications and architecture.
01.04	Identify network components, media, connectors, applications and protocols.
01.05	Compare and contrast the OSI and TCP/IP reference models and their layers.
01.06	Identify and describe current relevant IEEE network standards.
01.07	Create an IP addressing scheme using Variable Length Subnet Masks (VLSM) and Classless Inter-Domain Routing (CIDR).
01.08	Identify and discuss issues related to networked environments, such as security, access control, fair use, privacy and redundancy.
01.09	Identify and discuss issues related to naming conventions for user IDs, email, passwords, and network hosts and devices.
01.10	Identify standard network topologies and describe the advantages and disadvantages of each topology.
01.11	Describe the major functions of LAN protocols.
01.12	Explain the functions of wireless components, standards, hardware, software, and infrastructure design.
01.13	Configure and manage the TCP/IP protocol stack.
01.14	Describe how TCP and UDP Port addresses, IP addresses, and MAC addresses function, and how they are used to deliver data across the network.
01.15	Identify emerging technologies and discuss related technical issues.
01.16	Design a local area network (LAN), including the specification of architecture, hardware and software.

	01.17 Identify the advantages and use of virtual local area networks (VLANs).
	01.18 Identify and explain wide area network (WAN) concepts.
	01.19 Plan, configure and test a small network and establish baselines.
	01.20 Describe the major functions of network server software components.
	01.21 Install applications on a server and configure clients for network access.
02.0	Demonstrate understanding of networked environments, hardware, and software. The student will be able to:
	02.01 Give several advantages and disadvantages of networked and non-networked environments.
	02.02 Describe current network environments and network topologies.
	02.03 Identify and discuss issues such as security, privacy and redundancy related to networked environments.
	02.04 Identify and discuss standardization issues related to naming conventions.
	02.05 List and define layers in the OSI and TCP/IP network protocol models.
	02.06 Identify and describe current relevant IEEE standards.
	02.07 Discuss the nature of IP and MAC addressing.
	02.08 Describe the major functions and requirements of web based server and client hardware and software components.
	02.09 Identify various of specialized servers.
	02.10 Recognize and describe current cable technologies.
	02.11 Describe current wireless technologies.
	02.12 Describe the major functions of network connectivity hardware, such as hubs, repeaters, bridges, routers, switches, and gateways.
	02.13 Describe the hardware needed to connect a LAN to the Internet.
	02.14 Describe the function of network storage devices and other peripherals.
	02.15 Compare and contrast major functions and features of current network operating systems (including directory services).
	02.16 Differentiate between telecommunications and data communications.
	02.17 Compare and contrast digital communications lines and cable characteristics (e.g. ISDN, DSL, T-1, T-3).

03.0	Demonstrate fundamental proficiency in network security essentials. The student will be able to:
	03.01 Describe common security threats to, and vulnerabilities of, computer systems and the corresponding best practices for mitigation.
	03.02 Define and describe malicious software and techniques to protect systems from its effects.
	03.03 Describe Denial of Service attacks and means to defend against them.
	03.04 Identify the risks and techniques of data loss and its prevention.
	03.05 Describe the principles and techniques of securing data storage and transmission.
	03.06 Identify current encryption and authentication standards.
	03.07 Implement security policies, including compliance and operational security.
	03.08 Enable access control, identity management and security logging.
	03.09 Manage client and network system security software and related updates.
	03.10 Describe the functions and characteristics of firewalls.
	03.11 Perform a ping sweep to identify network hosts.
	03.12 Perform a port scan to probe network hosts for open TCP and UDP ports.
	03.13 Describe the purpose and operation of network protocol analyzers.
	03.14 Utilize a network protocol analyzer to capture and analyze network traffic for security issues.
04.0	Demonstrate an understanding of the directory services infrastructure and installation. The student will be able to:
	04.01 Describe the architecture of Active Directory.
	04.02 Discuss how Active Directory works.
	04.03 Describe the Active Directory design, plan, and implementation processes.
	04.04 Create a forest and domain structure.
	04.05 Configure the Domain Name Service (DNS) in an Active Directory environment.
	04.06 Raise the functional level of a forest and a domain.
	04.07 Create, manage, and delegate administrative control for organizational units.

05.0	Demonstrate an understanding of network access control systems and methodology. The student will be able to:
	05.01 Specify by access control mechanisms what users can do, which resources they can access, and what operations they can perform on a system.
	05.02 Compare and contrast access control techniques.
	05.03 Administer computer, group, and user accounts.
	05.04 Manage policies, rights, permissions, and passwords for users and/or groups of users.
	05.05 Demonstrate an understanding of various access control models.
	05.06 Manage password, PIN selection, maintenance, and control.
	05.07 Demonstrate an understanding of methods of identification and authentication.
	05.08 Implement centralized/remote authentication access controls.
	05.09 Implement and manage decentralized access controls such as domain and trust relationships.
	05.10 Analyze methods of server attacks.
	05.11 Demonstrate an understanding of the different types of intrusions and the different methods of intrusion detection.
	05.12 Monitor the network using various forms of intrusion detection resources to detect attacks.
	05.13 Investigate audit trails for signs of network intrusions.
	05.14 Perform penetration testing to find weaknesses in the access control systems.
06.0	Demonstrate understanding of routing concepts. The student will be able to:
	06.01 Describe the purpose, architecture, and operations of a router.
	06.02 Identify the hardware and software components of routers.
	06.03 Explain the purpose and nature of routing tables.
	06.04 Describe administrative distance and routing metrics such as hop counts and cost.
	06.05 Describe how a router determines a path and switches packets.
	06.06 Differentiate between static and dynamic routing.
	06.07 Explain the differences between class-full and classless routing.

	06.08 Describe the use and operation of VLSM and CIDR.
	06.09 Describe how a network converges.
07.0	Demonstrate an understanding of routing protocols. The student will be able to:
	07.01 Describe the characteristics of distance vector routing protocols.
	07.02 Describe the characteristics of link state routing protocols.
	07.03 Describe the differences between distance vector and link state routing protocols and determine the best routing protocol to use in a given situation.
	07.04 Describe the features and operation of current internal and external routing protocols.
08.0	Demonstrate router configuration skills. The student will be able to:
	08.01 Configure and verify router interfaces.
	08.02 Perform basic router configuration using the Command Line Interface (CLI) to inspect the operations of the router.
	08.03 Design and implement a classless IP addressing scheme for a network.
	08.04 Configure a router for RIP version 2 operation.
	08.05 Use advanced configuration commands with routers.
	08.06 Configure and modify metric on a router to improve network performance.
	08.07 Configure summarization and default route settings on a router to optimize network performance
	08.08 Verify and troubleshoot router operations in complex network environment.
09.0	Perform coding activities. The student will be able to:
	09.01 Identify modules.
	09.02 Design modules.
	09.03 Code modules.
	09.04 Document modules.
	09.05 Test modules.
	09.06 Debugging code.

	09.07 Revise code.
	09.08 Assemble modules.
10.0	Perform programming and scripting activities. The student will be able to:
	10.01 Identify several of the most prominent current programming languages.
	10.02 Characterize the stages of the system development life cycle.
	10.03 Differentiate between two common strategies for problem solving.
	10.04 Describe the program design and development process.
	10.05 Differentiate between structured programming and object-oriented programming.
	10.06 Use procedural and object-oriented constructs of programming, scripting, and/or macro languages to create and test programs.
	10.07 Apply principles of good design and documentation when developing programs.
	10.08 Design, review, and test specifications and algorithms.
	10.09 Write program according to specifications and revise based on testing and debugging.
11.0	Demonstrate proficiency with Internet structure, organization, and navigation. The student will be able to:
	11.01 Describe the origin of the Internet.
	11.02 Outline the history of the Internet.
	11.03 Describe Internet organization, such as the InterNIC, domains and requests for comments (RFCs).
	11.04 Describe the structure of the Internet.
	11.05 Differentiate between the Internet and the WWW.
	11.06 Differentiate among an Intranet site, an extranet site, and an Internet site.
	11.07 Describe and identify several major ethical and legal issues related to Internet use and how they affect intellectual property rights.
	11.08 Describe the World Wide Web (WWW) and identify how it affects personal security and privacy and our society.
	11.09 Describe and differentiate between file types and protocols.
	11.10 Demonstrate the use of typical remote access mechanisms.

	11.11 Describe various sections of a URL.
12.0	Perform web design/development activities. The student will be able to:
	12.01 Describe and use the process of storyboarding a website.
	12.02 Describe format, structure and design principles for websites.
	12.03 Identify existing resources and constraints.
	12.04 Create site navigation plan including directory structure.
	12.05 Procure/create and incorporate standard and animated graphics into a webpage.
	12.06 Design page templates to implement on final site.
	12.07 Create a webpage using authoring tools.
	12.08 Code page(s) using current web programming languages.
	12.09 Check page for cross-browser capability and other access issues.
	12.10 Upload pages and run site analysis.
	12.11 Incorporate sound files onto a webpage.
	12.12 Incorporate a streaming video file onto a webpage.
	12.13 Incorporate a video file for download into a webpage.
	12.14 Perform simple graphic modifications using a graphics utility.
	12.15 Incorporate an e-mail link on a webpage.
	12.16 Incorporate internal and external links on a webpage.
	12.17 Incorporate file transfer capabilities on a webpage.
	12.18 Incorporate handicapped-accessibility options into the website.
	12.19 Create a web form and produce e-mail results.
13.0	Demonstrate proficiency in analyzing network intrusions. The student will be able to:
	13.01 Describe the role of a Cybersecurity Operations Analyst in the enterprise.

	13.02 Describe various software applications needed to support cybersecurity analyses.
	13.03 Describe the operation of the network infrastructure
	13.04 Demonstrate how to analyze network intrusion data to identify compromised hosts and vulnerabilities.
	13.05 Identify various network security alerts.
	13.06 Correctly analyze intrusion data to determine potential exploits.
	13.07 Describe the types of log files used in security monitoring.
	13.08 Demonstrate the use of websites to generate malware analysis.
14.0	Demonstrate proficiency in incident handling and response. The student will be able to:
	14.01 Classify the various types of network attacks.
	14.02 Manage evidentiary data in an electronic environment.
	14.03 Describe the essential elements of forensic analysis.
	14.04 Describe incident response models used to manage network security incidents.
15.0	Demonstrate an understanding of how to mitigate network vulnerabilities. The student will be able to:
	15.01 Describe various methods to prevent malicious access to computer networks, hosts, and data.
	15.02 Describe the impacts of cryptography on network security monitoring.
	15.03 Describe how to investigate endpoint vulnerabilities.
16.0	Legal and ethical issues relative to the information technology environment. The student will be able to:
	16.01 Discuss the types of works that are protected by intellectual property laws.
	16.02 Discuss the basic elements of a contract.
	16.03 Discuss email litigation, including anti-spam laws.
	16.04 Discuss email use and ownership.
	16.05 Describe customer and employee privacy issues and safeguards.
	16.06 Develop examples of acceptable use policies.

	16.07 Compare organizational codes of ethics.
	16.08 Research industry standards and codes of conduct for information technology professionals.
	16.09 Write a personal code of ethics.
17.0	Communications skills. The student will be able to:
	17.01 Write logical and clear statements, or phrases, to accurately fill out forms/invoices commonly used in business and industry.
	17.02 Read and explain graphs, charts, diagrams, and tables commonly used in this industry/occupation area.
	17.03 Deliver and follow oral and written instructions.
	17.04 Answer and ask questions coherently and concisely.
	17.05 Read critically by recognizing assumptions and implications and by evaluating ideas.
	17.06 Demonstrate appropriate communication skills.
	17.07 Prepare and deliver a technical presentation.
	17.08 Observe and interpret verbal and nonverbal behavior.

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 intercurricular career and technical student organization(s) 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.

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.

Certificate Programs

A College Credit Certificate consists of a program of instruction of less than sixty (60) credits of college-level courses, which is part of an AS or AAS degree program and prepares students for entry into employment (Rule 6A-14.030, F.A.C.).

Additional Resources

For additional information regarding articulation agreements, Bright Futures Scholarships, Fine Arts/Practical Arts Credit and Equivalent Mathematics and Equally Rigorous Science Courses please refer to:
http://www.fldoe.org/academics/career-adult-edu/career-tech-edu/program-resources.stml