Information Technology Career Cluster
Introduction to Cybersecurity
Course Number: 11.48100

Course Description:
Introduction to Cybersecurity is designed to provide students the basic concepts and terminology of cybersecurity. The course examines how the concept of security integrates into the importance of user involvement, security training, ethics, trust, application of cybersecurity practices and devices, and best practices management. The fundamental skills cover internal and external threats to network security and design, how to enforce network level security policies, how to protect an organization’s information, and a broad range of other topics.

Various forms of technologies will be used to expose students to resources, software, and applications of cybersecurity. Professional communication skills will be used to expose students to resources, software, and applications of cybersecurity. Professional communication skills and practices, problem-solving, ethical and legal issues, and the impact of effective presentation skills are enhanced in this course to prepare students to be college and career ready. Employability skills are integrated into activities, tasks, and projects throughout the course standards to demonstrate the skills required by business and industry. Competencies in the co-curricular student organization, Future Business Leaders of America (FBLA), are integral components of the employability skills standard for this course.

Introduction to Cybersecurity is the second course in the Cybersecurity career pathway of the Information Technology Career Cluster and primarily focuses on the National Cybersecurity Workforce Framework category Protect and Defend and the Computer Network Defense work roles. Students enrolled in this course should have successfully completed Introduction to Digital Technology.

Course Standard 1

IT-ICS-1
Demonstrate employability skills required by business and industry.
The following elements should be integrated throughout the content of this course.

1.1 Communicate effectively through writing, speaking, listening, reading, and interpersonal abilities.
1.2 Demonstrate creativity with multiple approaches to ask challenging questions resulting in innovative procedures, methods, and products.
1.3 Exhibit critical thinking and problem solving skills to locate, analyze, and apply information in career planning and employment situations.
1.4 Model work readiness traits required for success in the workplace including integrity, honesty, accountability, punctuality, time management, and respect for diversity.
1.5 Apply the appropriate skill sets to be productive in a changing, technological, and diverse workplace to be able to work independently, interpret data, and apply teamwork skills.
1.6 Present a professional image through appearance, behavior, and language.

Course Standard 2

IT-ICS-2

Demonstrate an understanding of cybersecurity concepts and research.

2.1 Explain the importance of data security.
2.2 Explain the concepts of confidentiality, integrity, availability, authentication, and non-repudiation. [NICE 63]
2.3 Research current events on breaches; focus on particular Information Assurance (IA) areas that were compromised. [NICE 165]
2.4 Explain the importance of physical security.

Course Standard 3

IT-ICS-3

Identify the fundamental principles of networking (wired and wireless), local area networks (elements, perimeter networks, IP addressing, access methods and topologies), client-server and peer-to-peer networking models, and wide area networks.

3.1 Define and identify the different types of LANs.
3.2 Identify and describe the purpose for a perimeter network.
3.3 Identify the different network topologies to include client/server and peer-to-peer distributed networks.
3.4 Define and describe Ethernet standards.
3.5 Identify twisted-pair cable, cabling tools, cabling testers and describe what can interfere with twisted-pair cabling, and how to avoid it.
3.6 Identify wireless devices, wireless settings and configurations, wireless standards, and encryption protocols.
3.7 Explain the differences between static and dynamic routing.
3.8 Explain how to install and configure Routing and Remote Access Service (RRAS) to function as a network router and how to install the Routing Information Protocol.
3.9 Explain the basics about various other wide area networking technologies.
3.10 Explain different personal and small business Internet connectivity types.

Course Standard 4

IT-ICS-4

Identify the fundamental principles of the Open Systems Interconnection Model, Internet Protocol IPv4 and IPv6, and common networking services to include Name Resolution Techniques.

4.1 Explain the Open Systems Interconnection (OSI) model by defining each of the layers and their functions.
4.2 Explain the differences and operation of layer 2 and layer 3 switches.
4.3 Differentiate between the OSI model and the TCP model.
4.4 Demonstrate how to categorize IPv4 addresses using the Class A, B, and C classifications.
4.5 Identify the default gateway and Domain Name System (DNS) server and explain how to configure within a network adapter’s Transmission Control Protocol/Internet Protocol (TCP/IP) properties dialog box.
4.6 Demonstrate how to define advanced TCP/IP concepts, such as Network Address Translation (NAT) and sub-nets, and how to create a sub-netted network.
4.7 Demonstrate the basics of IPv6 and how to configure IPv6 in the command line and define dual stack and tunneling technologies.

4.8 Implement Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to client computers demonstrating an understanding of the four-step process known as DORA (discover, offer, request, acknowledgment).
4.9 Implement Terminal Services so that client computers can connect remotely to a server and take control of it in the Graphical User Interface (GUI).
4.10 Implement Network Policy Service (NPS) as a LAN router and define IPsec and the various types of protocols, including Security Associations (SA), Authentication Header (AH), and Encapsulating Security Payload (ESP).
4.11 Explain the function of Domain Name System (DNS) and Windows Internet Name Service (WINS) and explain how to install in Windows Server 2008, as well as how to create forward-lookup zones.

Course Standard 5

IT-ICS-5

Demonstrate how to work with the basic and advanced command prompts.

5.1 Manipulate and explain the command prompt as an administrator.
5.2 Demonstrate basic TCP/IP commands such as ipconfig and ping to analyze and test a network.
5.3 Demonstrate more advanced commands such as netstat, nbtstat, tracert, pathping, route, and netsh to fully examine a computer and configure it in the command line.
5.4 Manipulate the Net command in an effort to find out more information about a system, start and stop services, and work with the network configuration.

Course Standard 6

IT-ICS-6

Explore and research network infrastructures and network security.

6.1 Differentiate between the Internet, Intranets, and Extranets.
6.2 Demonstrate how to set up a virtual private network (VPN).
6.3 Explain firewalls and how to initiate port scans on them to see whether they are locked down.
6.4 Explain other perimeter devices and zones, such as proxy servers, internet content filters, Network Intrusion Detection Systems (NIDS), Network Intrusion Prevention Systems (NIPS), and Demilitarized Zones (DMZ).

Course Standard 7

IT-ICS-7

Demonstrate how to work with fundamental components of cybersecurity.

7.1 Explain the security function and purpose of network devices and technologies (e.g., Intrusion Detection System (IDS) tools and applications and IDS hardware and software, including open source tools, and their capabilities. [NICE 3, 59 and 146].
7.2 Distinguish and differentiate between network design elements and compounds.
7.3 Securely install cabling.
7.4 Configure firewalls.
7.5 Configure secure network connections (in Windows or Linux).
7.6 Justify the use of basic Windows or Linux commands to configure communications (e.g. ipconfig/ifconfig).
7.7 Design a basic secure network topology demonstrating knowledge of intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies. [NICE 66]

Course Standard 8

IT-ICS-8

Demonstrate how to employ host system and application security.

8.1 Compare and contrast common operating systems, e.g., Windows, Linux, OS X.
8.2 Compare and contrast common file systems.
8.3 Explain the importance of application security.
8.4 Demonstrate knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). [NICE 105]
8.5 Install and configure anti-virus software.
8.6 Perform command line exercises specific to operating systems.
8.7 Demonstrate knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities and how to differentiate between types of application attacks. [NICE 150]
8.8 Justify the need and implement Active X and Java Security.
8.9 Discuss protection from buffer overflow attacks.
8.10 Prevent input validation attacks and scripting attacks.
8.11 Justify the need for and implement secure cookies.

Course Standard 9

IT-ICS-9

Demonstrate how to implement proper security administration.

9.1 Implement appropriate procedures to establish host security.
9.2 Secure operating systems (OS), user profiles, and computer permissions.
9.3 Secure firewalls and Web browsers.
9.4 Establish a secure baseline for host OS.
9.5 Install and manage MS Windows.
9.6 Analyze security using Microsoft Baseline Security Analyzer (MBSA).
9.7 Demonstrate knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools such as Microsoft (MS) Backup/Restore. [NICE 29]
9.8 Methodically examine and conduct a security audit to review system performance and settings in Windows and Linux.
9.9 Demonstrate the ability to select and set both file and folder permissions in Windows and Linux.
9.10 Set up shared documents and folders.
9.11 View and edit Windows services (disable services).
9.12 Enable Extended File System (EFS).
9.13 View and change the backup archive bit in order to change the backup file status.
9.14 Secure DNS/BIND, web, email, messaging, FTP servers.
9.15 Secure directory services, Dynamic Host Configuration Protocol (DHCP), file, and print servers.

Course Standard 10

IT-ICS-10

Demonstrate how to implement proper access controls and identity management.

10.1 Demonstrate knowledge of host/network access controls (e.g., access control list) to include the function and purpose of authentication services. [NICE 49]
10.2 Explain the fundamental concepts and best practices related to authentication, authorization, and access control.
10.3 Implement appropriate security controls when performing account management.
10.4 Review authentication using Passfaces.com.
10.5 Manage user accounts, including basic to advanced protocol procedures.

Course Standard 11

IT-ICS-11

Research and explore basic principles of cryptology.

11.1 Summarize general cryptography concepts (symmetric encryption, asymmetric encryption). [NICE 27]
11.2 Demonstrate basic cipher systems (e.g., Caesar cipher, Vigenere cipher).
11.3 Demonstrate file hashing.
11.4 Demonstrate knowledge of current applications of steganography to include concealed identification, authentication, and communications.

Course Standard 12

IT-ICS-12

Explore how related student organizations are integral parts of career and technology education courses through leadership development, school and community service projects, entrepreneurship development, and competitive events.

12.1 Explain the goals, mission and objectives of Future Business Leaders of America.
12.2 Explore the impact and opportunities a student organization (FBLA) can develop to bring business and education together in a positive working relationship through innovative leadership and career development programs.
12.3 Explore the local, state, and national opportunities available to students through participation in related student organization (FBLA) including but not limited to conferences, competitions, community service, philanthropy, and other FBLA activities.
12.4 Explain how participation in career and technology education student organizations can promote lifelong responsibility for community service and professional development.
12.5 Explore the competitive events related to the content of this course and the required competencies, skills, and knowledge for each related event for individual, team, and chapter competitions.