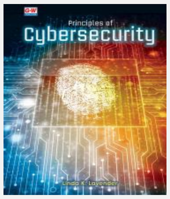
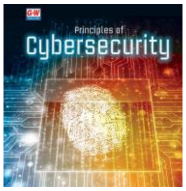
G-W PUBLISHER
Goodheart-Willcox Publisher
18604 West Creek Drive • Tinley Park, IL 60477-6243
Web www.g-w.com
Orders 800.323.0440
Phone 708.687.5000
Fax 708.687.5068

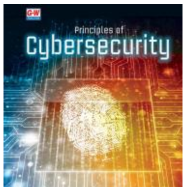
Goodheart-Willcox
Correlation of Principles of Cybersecurity ©2020
To Georgia Department of Education
Information Technology Career Cluster
Introduction to Cybersecurity
Course Number: 11.48100 (Grade 9-12)



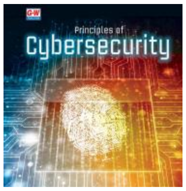
Course Task/Competency Lists		Correlating Textbook Pages
IT-ICS-1	**Demonstrate employability skills required by business and industry.**	
1.1	Communicate effectively through writing, speaking, listening, reading, and interpersonal abilities.	24, 569-591
1.2	Demonstrate creativity by asking challenging questions and applying innovative procedures and methods.	24, 572-573
1.3	Exhibit critical thinking and problem-solving skills to locate, analyze and apply information in career planning and employment situations.	568-569, 572-573
1.4	Model work readiness traits required for success in the workplace including integrity, honesty, accountability, punctuality, time management, and respect for diversity.	24
1.5	Apply the appropriate skill sets to be productive in a changing, technological, diverse workplace to be able to work independently and apply teamwork skills.	24, 567-569, 572-573
1.6	Present a professional image through appearance, behavior, and language.	567
IT-ICS-2	**Review and update personal online career portfolio.**	
2.1	Review and update résumé to reflect new knowledge and skills mastery and additional work experience.	574-576, 575 (Figure 18-8 Resume)
2.2	Compose an additional cover letter seeking employment for a position representative of new skills, knowledge, and work experience.	574-576, 575 (Figure 18-8 Resume)
2.3	Replace outdated transcripts to reflect current courses successfully completed.	574, 576
2.4	Review and revise existing artifacts to bring them up to date with new skills mastered, as necessary.	574, 576
2.5	Identify and upload additional industry-appropriate artifacts reflective of mastered skills throughout this course. Write and include a reflective entry for each artifact discussing steps taken, problems encountered and how they were overcome, and other pertinent information about the learning.	574, 576
IT-ICS-3	**Demonstrate an understanding of cybersecurity concepts and research.**	
3.1	Explain the importance of data security and data classification (confidential, sensitive, etc.).	388-411



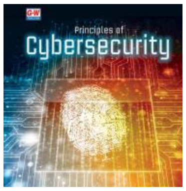
Course Task/Competency Lists		Correlating Textbook Pages
3.2	Explain the concepts of confidentiality, integrity, availability, authentication, and non- repudiation. [NICE 63]	35, 73-76, 567
3.3	Research current events on breaches; focus on particular Information Assurance (IA) areas that were compromised. [NICE 165]	388-411
3.4	Explain the importance of physical security.	149-152
IT-ICS-4	**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.**	
4.1	Define and identify the different types of LANs.	37
4.2	Identify and describe the purpose for a perimeter network.	294
4.3	Identify the different network topologies to include client/server and peer-to-peer distributed networks.	289-300
4.4	Define and describe Ethernet standards.	37-38
4.5	Identify wireless devices, wireless settings and configurations, wireless standards, and encryption protocols.	335-345
IT-ICS-5	**Identify the fundamental principles of the Open Systems Interconnection Model, Internet Protocol IPv4 and IPv6, and common networking services to include Name Resolution Techniques.**	
5.1	Explain the Open Systems Interconnection (OSI) model by defining each of the layers and their functions.	423
5.2	Explain the differences and operation of layer 2 and layer 3 switches.	423
5.3	Differentiate between the OSI model and the TCP model.	423
5.4	Demonstrate how to categorize IPv5 addresses using the Class A, B, and C classifications.	255-261
5.5	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.	289-292
5.6	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.	254



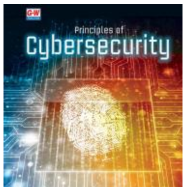
Course Task/Competency Lists		Correlating Textbook Pages
5.7	Demonstrate the basics of IPv6 and how to configure IPv6 in the command line and define dual stack and tunneling technologies.	257-261
5.8	Implement Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to client computers demonstrating an understanding of the four-step process known as DORA (discover, offer, request, acknowledgment).	255-261
5.9	Implement Terminal Services so that client computers can connect remotely to a server and take control of it in the Graphical User Interface (GUI).	255-261
5.10	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).	35-39
5.11	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.	289-292
IT-ICS-6	**Demonstrate how to work with the basic and advanced command prompts.**	
6.1	Manipulate and explain the command prompt as an administrator.	110-111
6.2	Demonstrate basic TCP/IP commands such as ipconfig and ping to analyze and test a network.	110-111
6.3	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.	277-278
6.4	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.	110-111
IT-ICS-7	**Demonstrate how to work with the basic and advanced command prompts.**	
7.1	Differentiate between the Internet, Intranets, and Extranets.	295
7.2	Demonstrate how to set up a virtual private network (VPN).	296-297
7.3	Explain firewalls and how to initiate port scans on them to see whether they are locked down and what it means if they are.	206-211
7.4	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).	208, 294



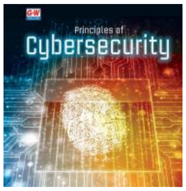
Course Task/Competency Lists		Correlating Textbook Pages
IT-ICS-8	**Demonstrate how to work with fundamental components of cybersecurity.**	
8.1	Explain the security function and purpose of network devices and technologies (e.g., Intrusion Detection System (IDS) tools and applications and IDS hardware and software, including open-source tools, and their capabilities. [NICE 3, 59 and 146].	307-308
8.2	Distinguish and differentiate between network design elements and compounds.	289-300
8.3	Securely install cabling.	23-24
8.4	Configure firewalls.	206-211
8.5	Configure secure network connections (in Windows or Linux).	251-268
8.6	Justify the use of basic Windows or Linux commands to configure communications (e.g., ipconfig/ifconfig).	110-119, 134-138
8.7	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]	251-268
IT-ICS-9	**Demonstrate how to employ host system and application security.**	
9.1	Compare and contrast common operating systems, e.g., Windows, Linux, OS X.	110-119, 134-138
9.2	Compare and contrast common file systems.	376-377
	a. Demonstrate how to protect them by locking them down with a File Integrity Monitor, such as Carbon Black.	376-377
9.3	Explain the importance of application security.	35-38
9.4	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]	227, 341, 388-411
9.5	Install, configure, and maintain (patch) anti-virus software.	23-24



Course Task/Competency Lists		Correlating Textbook Pages
9.6	Perform command line exercises specific to operating systems.	110-141
9.7	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	251-268
9.8	Justify the need and implement Active X and Java Security.	251-268
9.9	Discuss protection from buffer overflow attacks.	392
9.10	Recognize, mitigate, and prevent input validation attacks and scripting attacks.	388-411
9.11	Justify the need for and implement secure cookies.	47
IT-ICS-10	**Demonstrate how to implement proper security administration**	
10.1	Implement appropriate procedures to establish host security.	201-212
10.2	Secure operating systems (OS), user profiles, and computer permissions.	73-103, 178-183
	a. Explain the differences between system purposes, such as production system, QA system, development system and others.	73-103, 178-183
10.3	Secure firewalls and Web browsers.	206-211
10.4	Establish a secure baseline for host OS.	183, 185
10.5	Analyze security using Microsoft Baseline Security Analyzer (MBSA).	183, 185
10.6	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]	520-521
10.7	Methodically examine and conduct a security audit to review system performance and settings in Windows and Linux.	196-197
10.8	Demonstrate the ability to select and set both file and folder permissions in Windows and Linux.	80
10.9	Set up shared documents and folders.	93-97



Course Task/Competency Lists		Correlating Textbook Pages
10.10	View and edit Windows services (disable services).	179-180
10.11	Secure DNS/BIND, web, email, messaging, FTP servers.	34-38, 79-80
IT-ICS-11	**Demonstrate how to monitor proper access controls and identity management..**	
11.1	Demonstrate knowledge of host/network access controls (e.g., access control list) to include the function and purpose of authentication services. [NICE 49]	93-101
11.2	Explain the fundamental concepts and best practices related to authentication, authorization, and access control.	73-74, 93-101
11.3	Implement appropriate security controls when performing account management.	35-38
11.4	Review authentication using Passfaces.com.	73-74
11.5	Manage user accounts, including basic to advanced protocol procedures	91
IT-ICS-12	**Research and explore basic principles of cryptology.**	
12.1	Summarize general cryptography concepts (symmetric encryption, asymmetric encryption). [NICE 27]	353-381
12.2	Demonstrate basic cipher systems (e.g., Caesar cipher, Vigenere cipher).	353
12.3	Demonstrate file hashing.	84
12.4	Demonstrate knowledge of current applications of steganography to include concealed identification, authentication, and communications.	359, 361, 557
IT-ICS-13	**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..**	
13.1	Explain the goals, mission, and objectives of Future Business Leaders of America (FBLA) and/or Technology Student Association (TSA) and/or SkillsUSA.	576-577
13.2	Explore the impact and opportunities a student organization (FBLA, TSA, SkillsUSA) can develop to bring business and education together in a positive working relationship through innovative leadership and career development programs.	576-577



Course Task/Competency Lists		Correlating Textbook Pages
13.3	Explore the local, state, and national opportunities available to students through participation in related student organizations (FBLA, TSA, SkillsUSA) including but not limited to conferences, competitions, community service, philanthropy, and other student organization activities.	576-577
13.4	Explain how participation in career and technology education student organizations can promote lifelong responsibility for community service and professional development.	576-577
13.5	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.	576-577