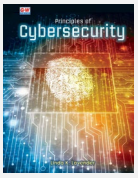
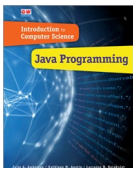
Goodheart-Willcox Publisher
18604 West Creek Drive • Tinley Park, IL 60477-6243
Web www.g-w.com
Orders 800.323.0440
Phone 708.687.5000
Fax 708.687.5068

Goodheart-Willcox
Correlation Introduction to Principles of Cybersecurity, (2020)
Texas Essential Knowledge And Skills For Career Development
And Career And Technical Education
Course Name and Number: 127.792 Foundations of Cybersecurity (Grade 9-12)

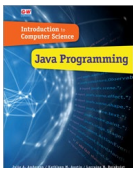


Standards	Correlating Text Pages
(c) Introduction	
(1) Career and technical education instruction provides content aligned with challenging academic standards, industry and relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and emerging professions.	
(2) The Science, Technology, Engineering, and Mathematics (STEM) Career Cluster focuses on planning, managing, and providing scientific research and professional and technical services such as laboratory and testing services and research and development services.	
(3) Cybersecurity is a critical discipline concerned with safeguarding computers, networks, programs, and data from unauthorized access. As a field, it has gained prominence with the expansion of a globally connected society. As computing has become more sophisticated, so too have the abilities of adversaries looking to penetrate networks and access systems and sensitive information. Cybersecurity professionals prevent, detect, and respond to minimize disruptions to governments, organizations, and individuals.	
(4) In the Foundations of Cybersecurity course, students will develop the knowledge and skills needed to explore fundamental concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will review and explore security policies designed to mitigate risks. The skills obtained in this course prepare students for additional study in cybersecurity. A variety of courses are available to students interested in this field. Foundations of Cybersecurity may serve as an introductory course in this field of study.	
(5) Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.	
(6) Statements that contain the word "including" reference content that must be mastered, while those containing the phrase "such as" are intended as possible illustrative examples.	
(d) Knowledge and Skills	
(1) Employability skills. The student demonstrates necessary skills for career development and successful completion of course outcomes. The student is expected to:	
(A) identify and demonstrate employable work behaviors such as regular attendance, punctuality, maintenance of a professional work environment, and effective written and verbal communication;	24, 567-571
(B) identify and demonstrate positive personal qualities such as authenticity, resilience, initiative, and a willingness to learn new knowledge and skills;	24, 567-571

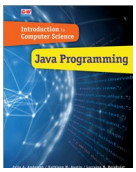


Standards	Correlating Text Pages
(C) solve problems and think critically;	24, 572-573
(D) demonstrate leadership skills and function effectively as a team member; and	24, 568-569
(E) demonstrate an understanding of ethical and legal responsibilities and ramifications in relation to the field of cybersecurity.	24, 58-64, 567
(2) Professional awareness. The student identifies various employment opportunities and requirements in the cybersecurity field. The student is expected to:	
(A) identify job and internship opportunities and accompanying job duties and tasks;	574-577
(B) research careers in cybersecurity and information security and develop professional profiles that match education and job skills required for obtaining a job in both the public and private sectors;	574-577
(C) identify and discuss certifications for cybersecurity-related careers; and	25-27, 437-444
(D) explain the different types of services and roles found within a cybersecurity functional area such as a security operations center (SOC).	574-577

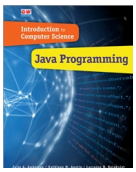
Goodheart-Willcox Publisher
18604 West Creek Drive • Tinley Park, IL 60477-6243
Web www.g-w.com
Orders 800.323.0440
Phone 708.687.5000
Fax 708.687.5068



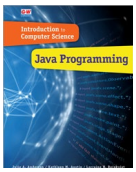
Standards	Correlating Text Pages
(3) Ethics and laws. The student understands ethical and current legal standards, rights and restrictions governing technology, technology systems, digital media, and the use of social media. The student is expected to:	
(A) demonstrate and advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers;	24, 58-64, 567
(B) investigate and analyze local, state, national, and international cybersecurity laws such as the USA PATRIOT Act of 2001, General Data Protection Regulation, Digital Millennium Copyright Act, Computer Fraud and Abuse Act, and Health Insurance Portability and Accountability Act of 1996 (HIPAA);	58-64
(C) investigate and analyze noteworthy incidents or events regarding cybersecurity;	4-9
(D) communicate an understanding of ethical and legal behavior when presented with various scenarios related to cybersecurity activities;	58-64, 567
(E) define and identify tactics used in an incident such as social engineering, malware, denial of service, spoofing, and data vandalism; and	4-9
(F) identify and use appropriate methods for citing sources.	50-52
(4) Ethics and laws. The student differentiates between ethical and malicious hacking. The student is expected to:	
(A) identify motivations and perspectives for hacking;	4-5, 7, 11-15



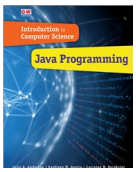
Standards	Correlating Text Pages
(B) distinguish between types of threat actors such as hacktivists, criminals, state-sponsored actors, and foreign governments;	11-15
(C) identify and describe the impact of cyberattacks on the global community, society, and individuals;	4-7
(D) differentiate between industry terminology for types of hackers such as black hats, white hats, and gray hats; and	5
(E) determine and describe possible outcomes and legal ramifications of ethical versus malicious hacking practices.	4-5, 24, 58-64
(5) Ethics and laws. The student identifies and defines cyberterrorism and counterterrorism. The student is expected to:	
(A) define cyberterrorism, state-sponsored cyberterrorism, and hacktivism;	4-7, 11-15
(B) compare and contrast physical terrorism and cyberterrorism, including domestic and foreign actors;	4-7, 11-15
(C) define and explain intelligence gathering;	4-7, 11-15
(D) explain the role of cyber defense in protecting national interests and corporations;	10-11, 34-35



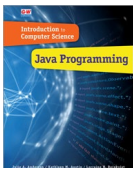
Standards	Correlating Text Pages
(E) explain the role of cyber defense in society and the global economy; and	10-11, 34-35
(6) Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding significant issues related to digital technology, digital hygiene, and cyberbullying. The student is expected to:	
(A) identify and understand the nature and value of privacy;	35
(B) analyze the positive and negative implications of a digital footprint and the maintenance and monitoring of an online presence;	50-56
(C) discuss the role and impact of technology on privacy;	50-56
(D) identify the signs, emotional effects, and legal consequences of cyberbullying and cyberstalking; and	4-5, 12
(E) identify and discuss effective ways to deter and report cyberbullying.	15-16
(7) Digital citizenship. The student understands the implications of sharing information and access with others. The student is expected to:	
(A) define personally identifiable information (PII);	168



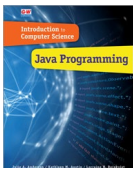
Standards	Correlating Text Pages
(B) evaluate the risks and benefits of sharing PII;	168, 170
(C) describe the impact of granting applications unnecessary permissions such as mobile devices accessing camera and contacts;	168, 170
(D) describe the risks of granting third parties access to personal and proprietary data on social media and systems; and	168, 170
(E) describe the risks involved with accepting Terms of Service (ToS) or End User License Agreements (EULA) without a basic understanding of the terms or agreements.	456
(8) Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:	
(A) define cybersecurity and information security;	5, 34
(B) identify basic risk management and risk assessment principles related to cybersecurity threats and vulnerabilities, including the Zero Trust model;	486-489
(C) explain the fundamental concepts of confidentiality, integrity, and availability (CIA triad);	34-35
(D) describe the trade-offs between convenience and security;	34-38



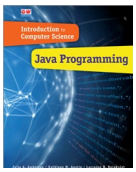
Standards	Correlating Text Pages
(E) identify and analyze cybersecurity breaches and incident responses;	4-11
(F) identify and analyze security challenges in domains such as physical, network, cloud, and web;	35-38
(G) define and discuss challenges faced by cybersecurity professionals such as internal and external threats;	41-56, 48 (Case Study), 50 (Ethical issue), Third-Party Cookie
(H) identify indicators of compromise such as common risks, warning signs, and alerts of compromised systems;	485, 491-498, 493 (FYI), 494 (Case Study), Responding to Risk
(I) explore and discuss the vulnerabilities of network-connected devices such as Internet of Things (IoT);	37, 221, 272-281, 275 (Ethical Issue), Ping Sweep
(J) use appropriate cybersecurity terminology;	4 – 15, 8 (FYI), 12 (FYI), 14 (FYI), 15 (Ethical Issues)
(K) explain the concept of penetration testing, including tools and techniques; and	15, 419-435, 420 (Case Study), Penetration Test Executive Standard, 435 (Case Study)
(L) explore and identify common industry frameworks such as MITRE ATT&CK™, MITRE Engage ™, and Cyber Kill Chain, and the Diamond Model.	37



Standards	Correlating Text Pages
(9) Cybersecurity skills. The student understands and explains various types of malicious software (malware). The student is expected to:	
(A) define malware, including spyware, ransomware, viruses, and rootkits;	41 – 45
(B) identify the transmission and function of malware such as trojan horses, worms, and viruses;	41 – 45
(C) discuss the impact of malware and the model of "as a service";	41 – 45
(D) explain the role of reverse engineering for the detection of malware and viruses; and	41-45
(E) describe free and commercial antivirus and anti-malware software also known as Endpoint Detection and Response software.	41-45
10. Cybersecurity skills. The student understands and demonstrates knowledge of techniques and strategies to prevent a system from being compromised. The student is expected to:	
(A) define system hardening;	178-183
(B) use basic system administration privileges;	178-183



Standards	Correlating Text Pages
(C) explain the importance of patching operating systems;	45, 201-203
(D) explain the importance of software updates;	392-394
(E) describe standard practices to configure system services;	201-203
(F) explain the importance of backup files;	520-528, 521 (Type of Backups)
(G) research and explain standard practices for securing computers, networks, and operating systems, including the concept of least privilege; and	73-91 , 303-311, 326-333
(H) identify vulnerabilities caused by a lack of cybersecurity awareness and training such as weaknesses posed by individuals within an organization.	4-15
11. Cybersecurity skills. The student understands basic network operations. The student is expected to:	
(A) identify basic network devices, including routers and switches;	303-311
(B) define network addressing;	254-255



Standards	Correlating Text Pages
(C) analyze incoming and outgoing rules for traffic passing through a firewall;	206-208
(D) identify well known ports by number and service provided, including port 22 (Secure Shell Protocol/ssh), port 80 (Hypertext Transfer Protocol/http), and port 443 (Hypertext Transfer Protocol Secure/https);	279, 396-397
(E) identify commonly exploited ports and services, including ports 20 and 21 (File Transfer Protocol/ftp), port 23 (telnet protocol), and port 3389 (Remote Desktop Protocol/rdp); and	279, 281
(F) identify common tools for monitoring ports and network traffic.	289-301, 301 (Ethical Issues)
12. Cybersecurity skills. The student identifies standard practices of system administration. The student is expected to:	
(A) define what constitutes a secure password;	378-381
(B) create a secure password policy, including length, complexity, account lockout, and rotation;	378-381
(C) identify methods of password cracking such as brute force and dictionary attacks; and	379-381