Career & Technical Education | Information Technology Cybersecurity

Subject Code: 146005

Outcome & Competency Descriptions

Course Description:
Students will learn the components of cybersecurity and the role each plays in preventing, detecting and mitigating vulnerabilities and attacks. Components include the security of the network infrastructure, security of the systems, and the prevention, detection, and mitigation of common vulnerabilities and attacks. Throughout this course, students will examine and implement security safeguards for desktop, network, and application security.

Strand 1. Business Operations/21st Century Skills

Learners apply principles of economics, business management, marketing, and employability in an entrepreneur, manager, and employee role to the leadership, planning, developing, and analyzing of business enterprises related to the career field.

Outcome: 1.1. Employability Skills

Develop career awareness and employability skills (e.g., face-to-face, online) needed for gaining and maintaining employment in diverse business settings.

Competencies

1.1.7. Apply problem-solving and critical-thinking skills to work-related issues when making decisions and formulating solutions.

Outcome: 1.2. Leadership and Communications

Process, maintain, evaluate, and disseminate information in a business. Develop leadership and team building to promote collaboration.

Competencies

1.2.4. Use negotiation and conflict-resolution skills to reach solutions.

1.2.5. Communicate information (e.g., directions, ideas, vision, workplace expectations) for an intended audience and purpose.

1.2.7. Use problem-solving and consensus-building techniques to draw conclusions and determine next steps.

Outcome: 1.3. **Business Ethics and Law**

Analyze how professional, ethical, and legal behavior contributes to continuous improvement in organizational performance and regulatory compliance.

Competencies

1.3.2. Follow protocols and practices necessary to maintain a clean, safe, and healthy work environment.

1.3.7. Identify the labor laws that affect employment and the consequences of noncompliance for both employee and employer (e.g., harassment, labor, employment, employment interview, testing, minor labor laws, Americans with Disabilities Act, Fair Labor Standards Acts, Equal Employment Opportunity Commission [EEOC]).

Outcome: 1.5. **Global Environment**

Evaluate how beliefs, values, attitudes and behaviors influence organizational strategies and goals.

Competencies

1.5.1. Describe how cultural understanding, cultural intelligence skills and continual awareness are interdependent.

1.5.2. Describe how cultural intelligence skills influence the overall success and survival of an organization.

1.5.3. Use cultural intelligence to interact with individuals from diverse cultural settings.

1.5.4. Recognize barriers in cross-cultural relationships and implement behavioral adjustments.

1.5.7. Use intercultural communication skills to exchange ideas and create meaning.

1.5.8. Identify how multicultural teaming and globalization can foster development of new and improved products and services and recognition of new opportunities.

Outcome: 1.10. Sales and Marketing

Manage pricing, place, promotion, packaging, positioning and public relations to improve quality customer service.

Competencies

1.10.1 Identify how the roles of sales, advertising, and public relations contribute to a company's brand.
1.10.2 Determine the customer's needs and identify solutions.
1.10.3 Communicate features, benefits, and warranties of a product or service to the customer.
1.10.4 Identify the company policies and procedures for initiating product and service improvements.
1.10.5 Monitor customer expectations and determine product/services satisfaction by using measurement tools.
1.10.6 Discuss the importance of correct pricing to support a product or service's positioning in the marketing mix.
1.10.7 Describe the importance and diversity of distribution channels (i.e., direct, indirect) to sell a product.
1.10.8 Use promotional techniques to maximize sales revenues (e.g., advertising, sales promotions, publicity, public relations).
1.10.9 Describe how product mix (e.g., product line, product items) maximize sales revenues, market, share, and profit margin.
1.10.10 Demonstrate sales techniques.

Outcome: 1.12. Cyber Hygiene

Apply digital information security principles to keep information secure.

Competencies

1.12.1. Identify the purpose and practices of Cyber Hygiene.
1.12.2. Differentiate between appropriate and inappropriate information.
1.12.3. Interpret security policies through job specific training and training updates.
1.12.4. Apply secure password behavior.
1.12.5. Apply physical and virtual situational awareness (e.g., clean desk policies, shoulder surfing, social engineering, tailgating).

Strand 2. IT Fundamentals

Learners apply fundamental principles of IT, including the history of IT and its impact on society, common industry terms, systems theory, information storage and retrieval, database management, and computer hardware, software, and peripheral device configuration and installation. This base of knowledge and skills may be applied across the career field.

Outcome: 2.1. Security, Risks, and Safeguards

Describe the need for security and explain security risks and security safeguards.

Competencies

2.1.1. Explain the need for confidentiality, integrity, and availability (CIA) of information.
2.1.2. Describe authentication, authorization, and auditing.
2.1.3. Describe multilevel security.
2.1.5. Describe major threats to computer systems (e.g., internal threats, viruses, malware, ransomware, spoofing, hacking, social engineering, phishing, Denial of Service, web application attacks, network-based attacks).
2.1.10. Describe computer forensics, its importance in information security and cybersecurity, and its relevance to law enforcement.
2.1.11. Identify the need for information security and implement best practices for maintaining cyber hygiene (e.g. personal identifiable information, private financial documents, corporate records).
2.1.12. Describe privacy security compliance on systems (e.g., Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry [PCI], Sarbanes Oxley Act [SOX], Americans with Disabilities Act [ADA], General Data Protection Regulation [GDPR], European Union Data Protection Regulation [EUDPR]).

Outcome 2.4. Emerging Technologies

Identify trending technologies, their fundamental architecture, and their value in the marketplace.

Competencies

2.4.1. Identify emerging technologies that are applicable to the marketplace.

2.4.2. Describe the fundamental architectures of emerging technologies and how they are integrating into the existing systems of information technology.
2.4.3. Research the value of emerging technologies on the marketplace.
2.4.4. Describe emerging technologies (e.g., Bring your Own Device [BYOD], Services Virtualization, Mixed Reality [MR], SMART Devices, Additive Manufacturing [3D Printing], Internet of Things, Large Language Models, Machine Learning, and Artificial Intelligence).

Outcome: 2.14. Artificial Intelligence

Understand and apply prescribed methods of using Artificial Intelligence.

Competencies

2.14.1. Describe how machine learning and neural networks operate differently than standard decision trees.
2.14.2. Analyze how artificial intelligence technology impacts society and the ethical implications of its usage.
2.14.3. Write and revise a prompt to generate the desired response from an AI.
2.14.4. Evaluate the result of an AI query on a variety of parameters (e.g. validity, relevance, authenticity, potential bias and hallucinations).
2.14.5. Identify and analyze opportunities to apply AI across business, industry and society.
2.14.6. Critically analyze scenarios involving AI usage.

Strand 3. Information Security

Learners apply principles of information security to implement and maintain security compliance and network security. Learners select components and mechanisms required for a multilayer defense structure and evaluate and minimize security risks to wired and wireless networks and devices.

Outcome: 3.1. Components of Information Security

Describe the components associated with information security systems.

Competencies

3.1.1. Differentiate between authentication and authorization.

3.1.2. Compare and contrast authentication techniques (e.g., single factor, multifactor, passwords, biometrics, certificates, Radio Frequency Identification [RFID] cards).

3.1.3. Compare and contrast methods of achieving information assurance and integrity and confidentiality (e.g., digital signatures, digital certifications, hashing algorithms, encryption).

3.1.4. Describe Virtual Private Networks (VPNs) using tunneling protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Secure Socket Tunneling Protocol [SSTP], Point-to-Point Tunneling Protocol [PPTP]) and encrypting techniques).

3.1.5. Discuss the role of certificate authorities (CAs) and Public Key Infrastructure (PKI).

Outcome: 3.2. General Security Compliance

Implement and maintain general security compliance.

Competencies

3.2.1. Identify and implement data and application security.

3.2.8. Identify the need for disaster recovery policies and procedures (e.g., business continuity plans, scenario testing).

Outcome: 3.3. Network Security

Implement and maintain network security.

Competencies

3.3.4. Describe Access Control Lists (ACLs) and explain why they are used.

3.3.5. Assess risk levels based on vulnerability of the organization, likelihood of risk, and impact on the organization.

3.3.6. Describe the relationships among change, vulnerability, configuration, and patch management to protect systems and applications.

Outcome: 3.4. Multilayer Defense Structure

Explain information technology mechanisms as they apply to a multilayer defense structure.

Competencies

3.4.4. Identify the components of human security (e.g., social engineering) and techniques to mitigate human security threats (e.g., policies, procedures, training).

Outcome: 3.5. **Wireless Security**

Implement secure wireless networks.

Competencies

3.5.1. Describe wireless security risks (e.g., unauthorized access) and how to mitigate them.

3.5.5. Describe security practices and policies for personal devices.

3.5.6. Implement and test the security of a wireless network.

Strand 4. Infrastructure Systems

Learners apply principles of networking and infrastructure related to the installation, administration, and maintenance of computer networks and components. Knowledge and skills may be applied to network connectivity, cabling, protocols, architecture, classification, topologies, operating systems, Open Systems Interconnection (OSI) standards, data encoding, Quality of Service (QoS), Internet Protocol (IP) addressing, and wide area network (WAN) design.

Outcome: 4.1. **Network Infrastructure**
Build a multinode network.

Competencies

4.1.1. Determine the basic point-to-point (PTP) and point-to-multipoint (PTMP) network topologies (e.g., star, ring, tree, mesh, hybrid) and identify broadband and baseband (e.g., Ethernet) transmission methods and standards.

4.1.4. Identify standard and emerging network technologies (e.g., broadband, satellite, optic, cellular, Local-Area Network (LAN) and WiFi).

Outcome: 4.2. **Open Systems Interconnection**
Describe the Open Systems Interconnection (OSI) standard (International Organization for Standardization [ISO] Standard 7498).

Competencies

4.2.3. Compare the seven layers of the Open Systems Interconnection stack to the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) stack.

4.2.5. Describe actions to be performed at each of the Open Systems Interconnection physical layers.

Outcome: 4.3. **Network Media**
Select, assemble, terminate, and test media.

Competencies

4.3.1. Identify the criteria used in selecting media (e.g., physical properties, transmission technologies, transmission span, bandwidth, topology, security, noise immunity, installation considerations, cost).

4.3.2. Differentiate between media types (e.g., coaxial, twisted pair, fiber optic) and interfaces.

4.3.3. Compare media categories (e.g., fiber (single mode vs. multimode), CAT5, CAT5E, CAT6+).

4.3.4. Describe types of media connectors (e.g., Bayonet Neill-Concelman [BNC], RJ-11, RJ-45, LC, ST, SC, Duplex Multimode LC) and grounding and bonding techniques.
4.3.5. Identify media standards (e.g., American National Standards Institute [ANSI], Electronic Industries Alliance/Telecommunications Industry Association [EIA/TIA]-568, EIA/TIA-568A and 568B).
4.3.6 Identify the advantages and disadvantages of cabling systems.

Outcome: 4.4. Wireless Communications
Explain wireless communications.

Competencies
4.4.1. Compare wireless standards in common use (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.11, Cellular, Bluetooth, Worldwide Interoperability for Microwave Access [WiMAX], Radio Frequency Identification [RFID], Near Field Communication [NFC]).

Outcome: 4.5. Wireless Network Solutions
Design and implement wireless network solutions.

Competencies
4.5.3. Describe the Service Set Identifier (SSID) as used in wireless communications.
4.5.4. Select and install access points, wireless Network Interface Cards (NICs), antennas, and other hardware and software components to provide a wireless networking solution as determined by a site and customer survey.
4.5.5. Troubleshoot Wireless Local Area Networks (WLANs) using system logs, vendor-provided utilities, and diagnostic tools.
4.5.6. Secure the wireless network.
4.5.7. Configure a wireless mesh network with non-overlapping channels.

Outcome: 4.7. Transmission Control Protocol/Internet Protocol (TCP/IP)
Describe IP addressing schemes and create subnet masks.

Competencies
4.7.1. Explain Fully Qualified Domain Names (FQDNs) and how they are used.
4.7.2. Explain the IP addressing scheme and how it is used.
4.7.3. Identify Class A, B, and C reserved (i.e., private) address ranges and why they are used.
4.7.4. Identify the class of network to which a given address belongs.

Outcome: 4.12. Disaster Recovery
Recommend disaster recovery and business continuity plans.

Competencies
4.12.1. Differentiate between disaster recovery and business continuity.
4.12.2. Identify common local and cloud-based backup options.

4.12.3. Identify the criteria for selecting a backup system.
4.12.4. Establish a process for archiving files.
4.12.5. Develop and simulate a disaster recovery plan.

Outcome: 4.13. Internet of Things

Install, configure, and operate IoT devices.

Competencies

4.13.1. Compare IoT wireless standards (e.g. Z-Wave, Zigbee).
4.13.2. Compare smart home ecosystems (e.g. Apple Homekit, Google Home, Amazon Alexa, Matter).
4.13.3. Configure, secure and connect IoT devices to the network.
4.13.4. Create IoT automations.
4.13.5. Explain fog computing in the IoT environment.

Strand 9. Cybersecurity

Learners apply principles of Cybersecurity to secure and defend information technology systems, selection and implementation of methods and tools to secure physical and digital assets, mange threats, deploy countermeasures, and establish strategies to protect business information using risk and incident management.

Outcome: 9.1. Cybersecurity

Examine and employ principles of Cybersecurity.

Competencies

9.1.1. Identify the goals, objectives and purposes of cybersecurity.

9.1.2. Describe the threats, vulnerabilities, threat actors and their capabilities to mitigate risk in cyber security.

9.1.5. Identify types of controls (e.g., Deterrent, Preventive, Detective, Compensating, Technical, and Administrative).

Outcome: 9.3. Application Development Security

Develop and maintain application security.

Competencies

9.3.1. Identify application vulnerabilities (e.g., Cross-site scripting, SQL injection, LDAP injection, XML injection, Directory traversal/command injection, Buffer overflow, Integer overflow, Zero-day, Cookies and attachments, Locally Shared Objects (LSOs), Flash cookies, Malicious add-ons, Session hijacking, Header manipulation, Arbitrary code execution/remote code execution).

9.3.6. Differentiate between Server-side vs. client-side validation.

Outcome: 9.5. Threat Management

Mitigate common threats.

Competencies

9.5.1. Describe, locate, and mitigate security threats (e.g., Adware, Viruses, Spyware, Trojan, Rootkits, Botnets, Ransomware).

9.5.2. Describe and discover vulnerabilities to and mitigate network attacks. (e.g., Man-in-the-middle, DDoS, DoS, Replay, Smurf attack, Spoofing, and other attacks).

9.5.4. Describe, appraise for, and mitigate Social Engineering attacks (e.g., Shoulder surfing, Dumpster diving, Tailgating, Impersonation, Hoaxes, Phishing, Spear Phishing, Whaling, Vishing, Principles, URL hijacking, Watering Hole, Spam, Spim, and Spit).

Outcome: 9.7. Digital Forensics

Capture and analyze information using digital tools.

Competencies

9.7.1. Recognize digital reconnaissance techniques (e.g., packet capture, OS fingerprinting, topology discovery, DNS harvesting).

9.7.4. Collect digital evidence according to established policies and protocols (e.g., system image, packet captures).

9.7.5. Maintain chain of custody on evidence.

Outcome: 9.8. Countermeasures

Use countermeasures to monitor systems and reduce risk.

Competencies

9.8.2. Differentiate between detection controls and prevention controls (e.g., IDS vs. IPS, Camera vs. guard).

9.8.3. Use discovery tools and utilities to identify threats (e.g., Protocol analyzer, Vulnerability scanner, Honeypots, Honeynets, Port scanner).

9.8.8. Implement a Network Access Control (NAC) plan.

9.8.9. Interpret alarms and alert trends.

9.8.10. Apply Incident response procedures (e.g., Preparation, Incident identification, Escalation and notification, Mitigation steps, Lessons learned, Reporting, Recovery procedures, First responder, Incident isolation, Quarantine, Device removal, Data breach).

9.8.11. Differentiate between types of Penetration testing (e.g., Black box, White box, Gray box).