

Career & Technical Education | Information Technology

Cybersecurity Defense & Reinforcement

Subject Code: 164010

Outcome & Competency Descriptions

Course Description:

Students will learn the process of systematic defense for Information Technology systems. They will apply knowledge and skills required to secure network resources including infrastructure, operating systems, data, and applications. Students will apply the knowledge of disaster recovery and business continuity.

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: 1.2. 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.
- 1.2.8. Identify the strengths, weaknesses, and characteristics of leadership styles that influence internal and external workplace relationships.
- 1.2.10. Use interpersonal skills to provide group leadership, promote collaboration, and work in a team.

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

- 1.3.1. Analyze how regulatory compliance affects business operations and organizational performance.
- 1.3.2. Follow protocols and practices necessary to maintain a clean, safe, and healthy work environment.
- 1.3.3. Use ethical character traits consistent with workplace standards (e.g., honesty, personal integrity, compassion, justice).
- 1.3.4. Identify how federal and state consumer protection laws affect products and services.
- 1.3.5. Access and implement safety compliance measures (e.g., quality assurance information, safety data sheets [SDSs], product safety data sheets [PSDSs], United States Environmental Protection Agency [EPA], United States Occupational Safety and Health Administration [OSHA]) that contribute to the continuous improvement of the organization.
- 1.3.8. Verify compliance with computer and intellectual property laws and regulations.

Outcome: 1.4. Knowledge Management and Information Technology

Demonstrate current and emerging strategies and technologies used to collect, analyze, record, and share information in business operations.

Competencies

- 1.4.3. Verify compliance with security rules, regulations and codes (e.g., property, privacy, access, accuracy issues, client and patient record confidentiality) pertaining to technology specific to the industry pathway.
- 1.4.4. Use system hardware to support software applications.
- 1.4.5. Use information technology tools to maintain, secure and monitor business records.
- 1.4.6. Use an electronic database to access and create business and technical information.
- 1.4.7. Use personal information management and productivity applications to optimize assigned tasks (e.g., lists, calendars, address books).

Outcome: 1.7. Entrepreneurship / Entrepreneurs

Analyze the environment in which a business operates, and the economic factors and opportunities associated with self-employment.

Competencies

- 1.7.13. Protect intellectual property and knowledge (e.g., copyright, patent, trademark, trade secrets, processes).

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

- 2.1.2. Describe authentication, authorization, and auditing.
- 2.1.4. Identify security risks and describe associated safeguards and methodologies (e.g., auditing).
- 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.

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: 3.2. General Security Compliance
Implement and maintain general security compliance.

Competencies

- 3.2.7. Provide documentation, training, and support to users on established security procedures.

Outcome: 3.3. Network Security
Implement and maintain network security.

Competencies

- 3.3.1. Identify the need for disaster recovery policies and procedures (e.g., business continuity plans, scenario testing).
- 3.3.5. Assess risk levels based on vulnerability of the organization, likelihood of risk, and impact on the organization.
- 3.3.7. Train users in network security procedures.

Outcome: 3.4. Multilayer Defense Structure
Explain information technology mechanisms as they apply to a multilayer defense structure.

Competencies

- 3.4.2. Analyze system log files to identify security events.
- 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.
- 3.5.2. Compare methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication Dial In User Service [RADIUS]).
- 3.5.3. Research security standards provided by Institute of Electrical and Electronics Engineers (IEEE).
- 3.5.4. Describe practices and policies for preventing and detecting installation of rogue networks.
- 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: 4.10. Cloud Computing

Implement a hypervisor.

Competencies

- 4.10.2. Provision cloud services (e.g., Software as a Service [SaaS], Platform as a Service [PaaS], Infrastructure as a Service [IaaS], Security as a Service [SECaaS], and Everything as a Service [XaaS]).

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.

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, manage 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.
- 9.1.3. Maintain data security using data classification, handling, and disposal as prescribed by policy and law.
- 9.1.4. Mitigate threats by remaining abreast of industry information.

- 9.1.5. Identify types of controls (e.g., Deterrent, Preventive, Detective, Compensating, Technical, and Administrative).
- 9.1.6. Manage physical and digital assets.

Outcome: 9.2. Access Control and Asset Security

Apply identification (ID), authorization, and physical asset security.

Competencies

- 9.2.1. Perform authorization control (e.g., least privilege, separation of duties, mandatory access, discretionary access, rule-based access control, role-based access control, time of day restrictions, location distractions).
- 9.2.2. Implement authentication techniques (e.g., Tokens, Common access card, Smart card, Multifactor authentication, Single sign-on, Biometrics, Personal identification verification card, Username, Federation, Transitive trust/authentication).
- 9.2.3. Use authentication factors (e.g., something you are, something you have, something you know).
- 9.2.4. Mitigate security implications of third-party connectivity and access.
- 9.2.5. Implement Data Loss Prevention (DLP).
- 9.2.6. Implement perimeter security (e.g., Fencing, Proximity readers, Access list, Proper lighting, Mantraps, Video Surveillance, Signs, Guards, Barricades, Biometrics, Protected distribution (cabling), Alarms, Motion detection).
- 9.2.7. Inventory organizational assets (e.g. applications, devices, software).
- 9.2.8. Explain zero trust principles and how they effect security.
- 9.2.9. Implement password management techniques.

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).
- 9.3.2. Mitigate application attacks (e.g., SANS, OWASP, MITRE).
- 9.3.3. Implement secure coding concepts (e.g., Error and exception handling, Input validation, Cross-site scripting prevention, Cross-site Request Forgery, (XSRF) prevention, OWASP).

- 9.3.4. Implement secure application configuration (e.g., Application hardening, Application patch management).
- 9.3.5. Discover and mitigate common database vulnerabilities and attacks.
- 9.3.6. Differentiate between Server-side vs. client-side validation.
- 9.3.7. Inventory applications on-hand.
- 9.3.8. Secure communication paths and data flow processes to harden the system.

Outcome: 9.4. Set up a secure network

Set up and maintain network security.

Competencies

- 9.4.1. Setup and maintain secure roles and system management techniques (e.g., password, group, and user privilege policies and monitoring).
- 9.4.2. Secure use of network Protocols (e.g., IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS, HTTPS, SCP, ICMP).
- 9.4.3. Apply principles of IPv4 and IPv6 securely.
- 9.4.4. Apply wireless security configurations (e.g., Disable SSID broadcast, TKIP, CCMP, Antenna placement, Power level controls).
- 9.4.5. Manage PKI and certificates (Transport encryption, Non-repudiation, Hashing, Key escrow, Steganography, Digital signatures).
- 9.4.6. Use algorithms/protocols with transport encryption (e.g., SSL, TLS, IPSec, SSH, HTTPS).
- 9.4.7. Install and configure network devices (firewalls, switches, load balancers, proxies, web security gateways, VPN concentrators).
- 9.4.8. Install and configure network security devices. (Protocol analyzers, UTM security appliances, URL filter, Content inspection, Malware inspection, Web Application Firewall (WAF)).
- 9.4.9. Implement port security.
- 9.4.10. Define Unified Threat Management and how to monitor a network.
- 9.4.11. Mitigate network threats (e.g., Flood guards, Loop protection, Implicit deny, Network separation, Log analysis, peripheral and removable media, DOS and DDOS).
- 9.4.12. Apply the principles of secure Network Design (e.g., DMZ, Subnetting, NAT/PAT, Remote access, Telephony, Virtualization, proxy servers, segmentation).

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).
- 9.5.3. Configure defenses for Password attacks (e.g., Brute Force, Dictionary attacks, Hybrid, Birthday attacks, Rainbow tables).

- 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).
- 9.5.5. Perform penetration testing.

Outcome: 9.6. Cybersecurity Law
Adhere to Cybersecurity laws.

Competencies

- 9.6.1. Adhere to licensing and intellectual property laws (e.g., copyright, trademark, digital-rights management).
- 9.6.2. Adhere to regulatory and industry standards (e.g., PCIDSS, PADASS, NICE Framework).

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).

Outcome: 9.8. Countermeasures
Use countermeasures to monitor systems and reduce risk.

Competencies

- 9.8.1. Design and implement network segmentation.
- 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).
- 9.8.4. Create, edit and use roles and system management tools.
- 9.8.5. Implement endpoint security.
- 9.8.6. Implement Access Control Lists (ACL).
- 9.8.7. Deploy a server hardening plan.
- 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).

Outcome: 9.9. Disaster Recovery and Business Continuity

Apply fundamentals of disaster recovery and business continuity.

Competencies

- 9.9.1. Describe the concepts of Risk Management (e.g., Business continuity concepts, Business impact analysis, Identification of critical systems and components, Removing single points of failure).
- 9.9.2. Describe the concepts of Risk assessment (e.g., Disaster recovery plan, IT contingency planning - Succession planning, Redundancy).
- 9.9.3. Describe and plan Fault tolerance (e.g., Hardware, RAID, Clustering, Load balancing, Disaster recovery concepts, Backup plans/policies, Backup execution/frequency).

Outcome: 9.10. Risk Management

Apply concepts of risk management.

Competencies

- 9.10.1. Enforce concepts related to threat vectors and probability/threat likelihood).
- 9.10.2. Identify concepts of risk calculation (Likelihood, Fair Risk Model, Impact, SLE, ARO, MTTR, MTTF, MTBF).
- 9.10.3. Implement Governance, risk management and Compliance Management processes (risk mitigation, govern compliance).