Information Technology Career Field
Software
Subject Code: 145030
Outcome & Competency Descriptions

Course Description:
Students will apply knowledge and skills of commercial and open source operating systems in portable, stand alone, and networked devices. Students will install a variety of operating systems manually and using remote assistance. They will learn to configure, modify, and troubleshoot operating systems. Desktop virtualization, system security, and operating system history will be addressed.

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.
2.1.4. Identify security risks and describe associated safeguards and methodologies (e.g., auditing).
2.1.5. Describe major threats to computer systems (e.g., insider threats, viruses, worms, spyware, ransomware, spoofing, hacking, social engineering, phishing).
2.1.6. Describe the components of the physical environment (e.g., wiring closets, server rooms) and physical security systems.
2.1.7. Describe the need for security in networking (e.g., firewall, access controls, encryption, demilitarized zone).
2.1.8. Describe the need for security in application development.
2.1.9. Track and catalogue physical assets.
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 personal security in digital information and describe how personal information can be safeguarded.
2.1.12. Practice information security per job requirements.
2.1.13 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: 2.2. Networking Fundamentals
Apply networking fundamentals to infrastructure systems.

Competencies

2.2.1. Differentiate between Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), and Near Field Communication (NFC).
2.2.2. Select the basic point-to-point (PTP) and point-to-multipoint (PTMP) network topologies (e.g., star, ring, tree, network, mesh, irregular) and broadband and baseband transmission methods.
2.2.3. Select network storage techniques (e.g., fiber channel, Internet Small Computer System Interface [iSCSI], Fiber Channel over Ethernet [FCoE], Serial Attached SCSI [SAS], Network File Systems [NFS], Network Attached Storage/Server Message Blocks [NAS/SMB]).
2.2.4. Differentiate between the Internet, intranets, and extranets.
2.2.5. Identify and apply Transmission Control Protocol and Internet Protocol (TCP/IP), Internet Protocol Version 4 (IPv4), Internet Protocol Version 6 (IPv6) applications and services (e.g., rlogin, Simple Mail Transfer Protocol [SMTP], Telecommunications Network [Telnet], File Transfer Protocol [FTP], Domain Name System [DNS], Network File System [NFS], Voice over Internet Protocol [VoIP], Internet Control Message Protocol [ICMP]).
2.2.6. Differentiate between cable types (e.g., fiber optic, twisted pair, coaxial) and interfaces.
2.2.7. Identify the top-level domains (e.g., .gov, .com, .edu).
2.2.8. Describe the characteristics and uses of networks, network devices, and components (e.g., hubs, switches, routers, firewalls).

Outcome 2.4. Emerging Technologies

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

Competencies

2.4.1. Investigate the scope and the impact of mobile computing environments on society.
2.4.2. Describe the differences, advantages, and limitations of cloud computing (e.g., public cloud, private cloud, hybrid cloud) and on premises computing.
2.4.3 Utilize cloud computing applications (e.g., services, applications, virtual environments).
2.4.4 Describe emerging technologies (e.g., Bring your Own Device [BYOD], Services Virtualization, Augmented Reality [AR], SMART Devices, Additive Manufacturing [3D Printing]).

Outcome 2.5. Maintain operating systems

Maintain Operating Systems (OSs).

Competencies

2.5.1. Compare Operating Systems for computer hardware (e.g. personal computers, servers, mainframes, and mobile devices).
2.5.2. Describe virtual machines and why they are used
2.5.3. Identify the properties of open and proprietary systems.
2.5.4. Maintain file structures in an Operating Systems.
2.5.5. Use system utilities to maintain an Operating Systems.
2.5.6. Describe Operating System interfaces (e.g., command line, Graphic User Interface [GUI]).
2.5.7. Install and test updates and patches to Operating Systems.

Information Technology Career Field
Software
Subject Code: 145030
Outcome & Competency Descriptions

Outcome: 2.6. Installation and Configuration

Install and configure hardware and software.

Competencies

2.6.1. Comply with license agreements for software and hardware and describe the consequences of noncompliance.
2.6.2. Identify hardware requirements for software applications.
2.6.3. Verify software compatibility and troubleshoot any software incompatibility.
2.6.4. Install and test new software and software upgrades on stand-alone, mobile, and networked systems.
2.6.5. Preserve, convert, or migrate existing data files to a new format.
2.6.6. Determine compatibility of software and hardware and resolve any conflicts.
2.6.7. Install and test hardware peripherals.
2.6.8. Document installation, configuration, and compatibility of hardware and software.

Outcome: 2.10. Equipment

Select, operate, and maintain equipment.

Competencies

2.10.1. Identify hardware platforms, configurations, and support models.
2.10.2. Identify processor, memory, storage, power and environmental requirements.
2.10.3. Identify architecture requirements.
2.10.4. Identify software application requirements.
2.10.5. Prepare and operate equipment per project design specifications.
2.10.6. Monitor equipment operation and troubleshoot issues and problems.
2.10.7. Backup, restore, test, archive, and manage data.
2.10.8. Prepare equipment for storage or decommissioning.
2.10.9. Perform routine maintenance per manufacturer specifications.

Outcome: 2.11. Troubleshooting

Select and apply troubleshooting methodologies for problem solving.

Competencies

2.11.1. Identify the problem.
2.11.2. Select troubleshooting methodology (e.g., top down, bottom up, follow the path, spot the differences).
2.11.3. Investigate symptoms based on the selected methodology.
2.11.4. Gather and analyze data about the problem.
2.11.5. Design a solution.
2.11.6. Test a solution.
2.11.7. Implement a solution.
2.11.8. Document the problem and the verified solution.

Outcome: 2.12. Performance Tests and Acceptance Plans

Develop performance tests and acceptance plans.

Competencies

2.12.1. Create a written procedure agreed by the stakeholders and project team for determining the acceptability of the project deliverables.
2.12.2. Develop a test system that accurately mimics external interfaces.
2.12.3. Develop test cases that are realistic, compare with expected performance, and include targeted platforms and device types.
2.12.4. Develop, perform, and document usability and testing integration.
2.12.5. Make corrections indicated by test results.
2.12.6. Seek stakeholder acceptance upon successful completion of the test plan.

Outcome: 2.13. Rollout and Handoff

Plan rollout and facilitate handoff to customer.

Competencies

2.13.1. Include overall project goals and timelines in the rollout plan.
2.13.2. Communicate rollout plans to key stakeholders in a timely manner.
2.12.3. Conduct final review and approvals according to company standards.
2.13.4. Identify support staff, training needs, and contingency plans in the rollout plan.
2.13.5. Test delivered application to assure that it is fully functional for the customer or user and meets all requirements.
2.13.6. Deliver support and training materials.

Information Technology Career Field
Software
Subject Code: 145030
Outcome & Competency Descriptions

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: 3.1.1 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 authentication techniques (e.g. single factor, multifactor, passwords, biometrics, certificates, Radio Frequency Identification [RFID] cards).
3.1.3. Compare 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 (e.g., tape, disk, cloud).
3.2.2. Implement backup and verification procedures (e.g., tape, disk, cloud).
3.2.3. Describe and assign permissions (e.g., read-only, read-write).
3.2.4. Provide user authentication (e.g., assign and reset user accounts and passwords).
3.2.5. Install, test, implement, and update virus and malware detection and protection software.
3.2.6 Identify sources of virus and malware infection and remove viruses and malware.
3.2.7. Provide documentation, training, and support to users on established security procedures.
3.2.8. Identify the need for disaster recovery policies and procedures.

Outcome: 3.4. Multilayer Defense Structure

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

Competencies

3.4.1. Describe available systems for intrusion prevention, detection, and mitigation.
3.4.2. Review system log files to identify security risks.
3.4.3. Compare network analysis software (e.g., network analyzer) and hardware tools to identify security risks and vulnerabilities.
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. Identify security enhancements 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: 4.3. 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., single mode, multimode, CAT5, CAT5E, CAT6+).
4.3.4. Describe types of media connectors (e.g., Bayonet Neill-Concelman [BNC], Registered Jack [RJ]-45, LC, ST) and grounding 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.
4.3.7. Describe typical problems associated with cable installation.
4.3.8. Assemble and test Ethernet cable (e.g., straight-through, crossover, loopback).

Outcome: 4.13. Disaster Recovery

Recommend disaster recovery and business continuity plans.

Competencies

4.13.1. Differentiate between disaster recovery and business continuity.
4.13.2. Identify common backup devices.
4.13.3. Identify the criteria for selecting a backup system.
4.13.4. Establish a process for archiving files.
4.13.5. Develop a disaster recovery plan.