

# Career & Technical Education | Information Technology

## Personal Computers

Subject Code: 145160

### Outcome & Competency Descriptions

#### Course Description:

Students will learn to install, repair, and troubleshoot computer hardware systems. They will perform preventative maintenance practices and learn techniques for maintaining computer hardware security. Communication skills and professionalism in troubleshooting situations will be emphasized.

#### Strand 1. Business Operations/21<sup>st</sup> 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

- 1.1.1. Identify the knowledge, skills, and abilities necessary to succeed in careers.
- 1.1.2. Identify the scope of career opportunities and the requirements for education, training, certification, licensure, and experience.
- 1.1.3. Develop a career plan that reflects career interests, pathways, and secondary and postsecondary options.
- 1.1.4. Describe the role and function of professional organizations, industry associations, and organized labor and use networking techniques to develop and maintain professional relationships.
- 1.1.8. Identify the correlation between emotions, behavior, and appearance and manage those to establish and maintain professionalism.
- 1.1.9. Give and receive constructive feedback to improve work habits.
- 1.1.11. Recognize different cultural beliefs and practices in the workplace and demonstrate respect for them.
- 1.1.12. Identify healthy lifestyles that reduce the risk of chronic disease, unsafe habits and abusive behavior.

**Outcome: 1.2      Leadership and Communications**

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

**Competencies**

1.2.12. Use technical writing skills to complete forms and create reports.

**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.

**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**

- 1.4.1. Use office equipment to communicate (e.g., phone, radio equipment, fax machine, scanner, public address systems).
- 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.

**Outcome: 1.8      Operations Management**

Plan, organize and monitor an organization or department to maximize contribution to organizational goals and objectives.

**Competencies**

1.8.8. Identify routine activities for maintaining business facilities and equipment.

## **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**

- 2.1.4. 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).

### **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), Near Field Communication (NFC) and other network infrastructure.
- 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, cloud, Fiber Channel over Ethernet [FCoE], Serial Attached SCSI [SAS], Network File Systems [NFS], Network Attached Storage/Server Message Blocks [NAS/SMB], Redundant Array of Inexpensive Disks [RAID]).
- 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. Understand and interpret various elements of a fully qualified domain.
- 2.2.8. Describe the characteristics and uses of networks, network devices, and components (e.g., hubs, switches, routers, firewalls).

## **Outcome: 2.5.      Operating Systems**

Install and maintain operating systems (OSs).

### **Competencies**

- 2.5.1. Compare Operating Systems for computer hardware (e.g., personal computers, servers, mainframes, operational technology (OT), and mobile devices).
- 2.5.2. Describe uses and functions of virtual machines.
- 2.5.3. Identify the properties of open and proprietary systems.
- 2.5.4. Maintain file structures in operating systems.
- 2.5.5. Use system utilities to maintain an operating system.
- 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.

## **Outcome: 2.6.      Install 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. Determine compatibility (software to software, software to hardware, hardware to hardware).
- 2.6.6. Install and test hardware peripherals.
- 2.6.7. Document installation, configuration, and compatibility of hardware and software.

## **Outcome: 2.10.      Equipment**

Select, prepare, 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**

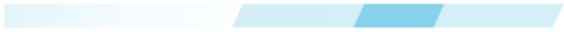
- 2.12.1. Create a written procedure agreed by the stakeholders and project team for determining the acceptability of the project deliverables.
- 2.12.2. Develop a test system that accurately mimics external interfaces.
- 2.12.3. Develop test cases that are realistic, compare with expected performance, 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.
- 2.13.3. 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.



### **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.
- 3.2.2. Perform backup, restore, and verification procedures.
- 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 (e.g., business continuity plans, scenario testing).

### **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. Analyze system log files to identify security events.
- 3.4.3. Compare and contrast 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. 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: 4.1. Network Infrastructure** Build a multinode network.

#### **Competencies**

- 4.1.3. Compare the characteristics of connection-oriented and connectionless protocols and select protocols based on given criteria.

### **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.
- 4.3.7. Describe typical problems associated with cable installation.
- 4.3.8. Assemble and test Ethernet cable (e.g., straight-through, crossover, loopback).

