

IT FUNDAMENTALS
ACTIVITY/COURSE CODE: 5025

COURSE DESCRIPTION:

The IT Fundamentals course is designed to prepare the student to take the CompTIA Strata Fundamentals of Information Technology Certificate of Achievement exam FC0-U41. Students receive instruction in safety, communication skills, leadership skills, human relations and employability skills, the knowledge to identify and explain PC components, set up a basic PC workstation, conduct basic software installation, identify compatibility issues and recognize/prevent basic security risks. Also included is instruction in the areas of Green IT and preventative maintenance of computers

The most current listing of standards for this course/program can be found on the Certiport Web site at <http://www.certiport.com> or the CompTIA home page <http://www.comptia.org>.

OBJECTIVE:

Given the necessary equipment, materials, and instruction, the student, on completion of the prescribed course of study, will be able to successfully accomplish the following standards.

COURSE CREDITS: 1 Carnegie unit

PREREQUISITE(S): Based on individual schools and school districts

RECOMMENDED GRADE LEVELS: 9-10

A. SAFETY AND ETHICS

1. Identify major causes of work-related accidents in offices.
2. Describe the threats to a computer network, methods of avoiding attacks, and options in dealing with virus attacks.
3. Identify potential abuse and unethical uses of computers and networks.
4. Explain the consequences of illegal, social, and unethical uses of information technologies, e.g., piracy; illegal downloading; licensing infringement; and inappropriate uses of software, hardware, and mobile devices.
5. Differentiate between freeware, shareware, and public domain software copyrights.
6. Discuss computer crimes, terms of use, and legal issues such as copyright laws, fair use laws, and ethics pertaining to scanned and downloaded clip art images, photographs, documents, video, recorded sounds and music, trademarks, and other elements for use in Web publications.
7. Identify netiquette including the use of email, social networking, blogs, texting, and chatting.
8. Describe ethical and legal practices in business professions such as safeguarding the confidentiality of business-related information.
9. Discuss the importance of cyber safety and the impact of cyber bullying.

B. EMPLOYABILITY SKILLS

1. Identify positive work practices, e.g., appropriate dress code for the workplace, personal grooming, punctuality, time management, and organization.
2. Demonstrate positive interpersonal skills, e.g., communication, respect, and teamwork.

C. STUDENT ORGANIZATIONS

1. Explain how related student organizations are integral parts of career and technology education courses.
2. Explain the goals and objectives of related student organizations.
3. List opportunities available to students through participation in related student organization conferences/competitions, community service, philanthropy, and other activities.
4. Explain how participation in career and technology education student organizations can promote lifelong responsibility for community service and professional development.

D. DOMAINS

1.0 Technology and Computer Hardware Basics

1.1 Identify basic IT vocabulary that supports seven key hardware components.

1. Processor speed/cores:
 - a) Single, Dual, Quad core
 - b) Intel based/Cell based/AMD based
 - c) GHz versus MHz
 - d) Processor cache size
 - e) Bus speed (as it relates to motherboards, memory, etc.)
2. RAM:
 - a) Single data rate, dual data rate, triple data rate
 - b) DIMMS versus SODIMMS
3. Hard drives:
 - a) RPMs
 - b) Cache size
 - c) Flash based versus traditional hard drives
 - d) SATA, SCSI, IDE
 - e) Internal versus external
 - f) Local versus network shares
4. Networking:
 - a) Wireless networking terms
 - b) 802.11a/b/g/n
 - c) Bluetooth

- d) RF (radio frequency)
- e) Interference
- f) WAP (wireless access point)
- g) SSID
- h) Wireless router
- 5. Ethernet technologies:
 - a) CAT5 connections and cables
 - b) Home plug (Ethernet over Power)
 - c) Broadband router
 - d) DSL and cable modems
 - e) Standard vs. crossover cables
 - f) Auto-negotiating (speed and duplex)
- 6. Internet protocols:
 - a) HTTP versus HTTPS
 - b) FTP
 - c) SSL
 - d) POP3
 - e) SMTP
 - f) IMAP
 - g) DNS
 - h) DHCP
 - i) TCP/IP (IPv4 address, IPv6 address)
- 7. Internet browser:
 - a) Plug-ins
 - b) Customization (text sizes, text styles, etc.)
 - c) Anti-phishing features
 - d) ActiveX and Java
 - e) Cookies
 - f) Internet cache

1.2 Demonstrate the proper use of the following four hardware components.

- 1. Monitor:
 - a) Adjusting monitor settings (brightness, contrast, etc.)
- 2. Desktop
- 3. Server
- 4. Portable:
 - a) Laptop
 - b) PDA
 - c) Smartphone
 - d) Netbook

1.3 Explain the functions of internal and external storage devices and the characteristics of each item.

1. CD/CD-RW drive
2. DVD/DVD-RW drive
3. Blu-Ray disk drive
4. USB storage (solid state versus magnetic disk)
5. Multi-card reader and writer
6. Hard drive
7. Mobile media device (e.g., MP3 player or PDA)

1.4 Explain the characteristics and functions of six peripheral devices.

1. Digital camera
2. Web camera
3. Speaker
4. Tuner
5. Microphone
6. Printer/scanner

1.5 Explain the characteristics and functions of five core input devices.

1. Keyboard
2. Mouse
3. Tablet (touch screen)
4. Numeric keypad
5. Gamepad

1.6 Identify the risks associated with upgrading the following technologies and equipment.

1. Operating systems (open source and commercial)
 - a) Compatibility issues
 - b) Upgrade issues
 - c) Data loss
2. PC Speed/storage capability and compatibility issues
 - a) Upgrade issues
 - b) Bus differences
 - c) Hardware failure
3. Applications
 - a) Minimum requirements
 - b) Compatibility issues
4. Bandwidth and contention
 - a) VoIP
 - b) Streaming
 - c) Web delivered services

5. Automatic application and operating system updates
 - a) Risks of automatic updates
 - b) Risks of not using automatic updates
 - c) Risks of not using manufacturers' Web sites

1.7 Demonstrate the ability to set up a basic PC workstation.

1. Identify differences between connector types.
 - a) DVI, VGA, HDMI
 - b) USB, PS/2
 - c) FireWire
 - d) Bluetooth and wireless
 - e) Serial
 - f) Network connectors
 - g) PCMCIA
 - h) ExpressCard
 - i) 3.5mm audio jack
 - j) Power connectors
2. Identify differences between monitor types.
3. Identify differences between computer types (desktop, tower, laptop, custom cases).
4. Identify differences between keyboard types (keyboard layout, regionalization).
5. Identify differences between mouse types (touchpad, optical, trackball).
6. Identify differences between types of printers (USB, wireless, networked).
7. Identify voltage and power requirements.
8. Turn on and use the PC and peripherals.

2.0 COMPATIBILITY ISSUES AND COMMON ERRORS

2.1 Identify basic compatibility issues between the following.

1. Processor performance
2. RAM
3. USB (1.1, 2.0, 3.0)
4. FireWire
5. PS/2
6. Ethernet
7. Wireless networks

2.2 Describe common operational problems caused by hardware.

1. Critical error message or crash
2. System lockup (freeze)
3. Application not starting or loading
4. Inability to log on to network

5. Driver/hardware compatibility
6. Input device not functioning

2.3 Demonstrate the ability to minimize risks.

1. Data loss
2. Loss of service
3. Damage to equipment

3.0 SOFTWARE INSTALLATION AND FUNCTIONS

3.1 Conduct basic software installation, removal, and/or upgrading.

1. Follow basic installation/upgrade procedures related to the following.
 - a) PC meeting minimum requirements.
 - b) Administrative rights.
 - c) Firewall access (unblocking ports for proper functionality).
2. Configure the operating system to support the following actions.
 - a) Basic settings adjustment (e.g. volume, date, time, time zone)
 - b) User accounts
 - c) Power settings (power save, sleep mode, etc.)
 - d) Screen resolutions
3. Ensure documentation is validated by obtaining the following.
 - a) Licensing (commercial, freeware, shareware)
 - b) Software registration
4. Follow digital rights management procedures.
5. Follow software removal (clean un-installation) procedures.
6. Follow re-installation (clean installation) procedures.

3.2 Identify issues related to folder and file management.

1. Create, delete, rename and move folders.
 - a) Assign folder structure during installation.
2. Create, delete, rename, move and print files
3. Explain importance of following back-up guidelines and procedures.

3.3 Explain the function and purpose of software tools.

1. Performance and error correction tools
2. Activity or event logging
3. Back-up tools
4. Disk clean-up tools
5. File compression tools

4.0 SECURITY

4.1 Recognize basic security risks and procedures to prevent them

1. Identify risks associated with the following.
 - a) Social engineering
 - b) Viruses
 - c) Worms
 - d) Trojan horses
 - e) Unauthorized access
 - 1) Hackers
 - 2) Phishing
 - 3) Spyware
 - 4) Adware
 - 5) Malware
 - 6) Identity fraud
2. Determine risks associated with file and folder sharing.
3. Determine risks associated with Web browsers.
4. Discuss operating systems' vulnerability.
 - a) Service packs
 - b) Security updates
5. Discuss risks associated with theft.
6. Discuss risks associated with open or free networks.
7. Identify prevention methods associated with security risks.
 - a) User awareness/education
 - b) Anti-virus software
 - c) Ensuring use of proper security certificate (SSL)
 - d) Wireless encryption (WPA/WEP)
 - e) Anti-spyware
 - f) File encryption
 - g) Firewalls
 - h) Anti-spam software
 - i) Password best practice
 - 1) Complexity (password construction)
 - 2) Password confidentiality
 - 3) Change frequency
 - 4) Re-use
 - 5) Utilization
8. Identify access control methods used to limit security risks of users.
 - a) Passwords and user ID
 - b) Screensavers
 - c) Physical security of hardware
 - d) Locks
 - e) Parental controls
 - f) Smart card

- g) Fingerprint reader
- h) One time password
- 9. Identify security threats related to multiple information sources.
 - a) Media used for backup (theft or loss)
 - b) Screen visibility (shoulder surfing)
 - c) Cookies (can be stolen, stores passwords, browser tracking)
 - d) Pop-ups (automatic installations, click on links to malware)
 - e) Accidental misconfiguration

4.2 Identify security breaches and determine ways to resolve them.

- 1. Recognize the proper diagnostic procedures when infected with a virus.
- 2. Run anti-virus scan.
- 3. Quarantine virus when possible.
- 4. Escalate to IT professional when needed.
- 5. Recognize the proper procedures to maintain a secure environment
- 6. Regular antivirus and malware scans
- 7. Application / operating system updates

5.0 Green IT and Preventative Maintenance

5.1 Identify environmentally sound techniques to preserve power and dispose of materials

- 1. Environmentally hazardous substance disposal
 - a) Battery disposal
 - b) CRT disposal-replace with LCDs
 - c) Recycling of computers for reuse or parts
 - d) Toner disposal
 - e) Cleaning supply disposal
 - f) Materials that meet RoHS guidelines
- 2. Power management (Power saving features)
 - a) Shutdown/power off procedures/policies at end of day
 - b) Automatic power off after 15 minutes of non-use
 - c) Shutdown scripts

5.2 Identify green techniques, equipment and procedures

- 1. Cloud computing
 - a) Define Virtualization (Have more than one server running on a single piece of hardware)
 - b) Reduced power and cooling consumption
- 2. Duplex printing and use lower cost per page network printers
- 3. Terminal Servers
- 4. Energy Star rating
- 5. Using low power NAS (network attached storage) instead of file servers

6. Employee telecommuting
 - a) Reduced emissions
 - b) Reduced office space heating, lighting, etc
7. Solid State drives
8. Defining VoIP and how it relates to Green IT
9. Green building infrastructure
 - a) Elimination of cool air leaks in server rooms
 - b) Proper spacing for cooling IT equipment
 - c) Energy efficient cooling fans-BIOS adjustable

5.3 Identify preventative maintenance products, techniques, and how to use them.

1. Liquid cleaning compounds
2. Types of materials to clean contacts and connections
3. Compressed air
4. Cleaning monitors
5. Cleaning removable media devices
6. Ventilation, dust, and moisture control on the PC hardware interior
7. Surge suppressors
8. Use of ESD equipment
9. Wire placement and safety