Northwest Arkansas Community College

Business and Computer Information Systems Division

Discipline Code

NTWK

Course Number

2153

Course Title

Microcomputer Software Support

Catalog Description

Students will learn to install, configure, and maintain current Microsoft Windows operating systems and document common software issues while applying troubleshooting skills. IOS, Android, Mac OS, Linux, and Windows Phone, are covered from a user's perspective. Client-side virtualization concepts will be covered as will computer security. Students will develop the skills to provide appropriate customer support. Students completing this course will have begun the preparation necessary for success in the following industry-recognized certifications: CompTIA A+ 220-1002 (Core 2). (Note: Preparation for the A+ certifications should include NTWK 2053 and NTWK 2153) (Outside lab time will be required.)

Prerequisites

CISQ 1103 or equivalent knowledge

Credit Hours

3 credit hours

Contact hours

45 lecture/lab contact hours

Load hours

3 load hours

Semesters Offered

Fall, On Demand

ACTS Equivalent

N/A

Grade Mode

A-F

Learning Outcomes

Upon completion of this course, student will:

- Compare and contrast the features and requirements of various Microsoft Operating Systems.
- Install and configure operating systems using the most appropriate method.
- Given a scenario, use appropriate command line tools.
- Given a scenario, use appropriate operating system features and tools.
- Given a scenario, use Control Panel utilities
- Setup and configure Windows networking on a client/desktop.
- Perform preventive maintenance procedures using appropriate operating system tools.
- Explain the differences among basic operating system security settings.
- Explain the basics of client-side virtualization.
- Compare and contrast common OS security threats.
- Implement security best practices to secure a workstation.
- Given a scenario, use the appropriate data destruction/disposal method.
- Explain the basic features of mobile operating systems.
- Establish basic network connectivity and configure email.
- Compare and contrast methods for securing mobile devices.
- Execute and configure mobile device synchronization.
- Explain software troubleshooting theory.
- Troubleshoot common video and display issues.
- Troubleshoot operating system problems with appropriate tools.
- Troubleshoot common security issues with appropriate tools and best practices.
- Troubleshoot, and repair common laptop issues while adhering to the appropriate procedures.

General Education Outcomes Supported

- Students can use computers proficiently.

Standard Practices

Topics list

- Virtualization (hypervisors, client-side virtualization, cloud computing, cloud services)
- Windows Operating System installation
- Disk architecture
- Hardware and software compatibility
- Operating system upgrades
- Disk management (partitions, logical drives, filesystems)
- Windows boot sequence
- Windows versions
- Windows configuration
- Windows Registry
- Windows utilities (task manager, file explorer, device manager, disk manager, control panels, system utilities, and administrative tools)
- Windows user accounts and credential manager
- Windows network settings and configuration
- Windows system controls
- Windows language and time settings.
- Windows system administration

- Windows command line interface and basic commands (file system, disk, task, and system commands)
- Powershell
- Basic scripting
- Scripting languages
- Third party software installation, updating and removal.
- Troubleshooting
- Encryption
- Windows networking (Sharing resources, mapping drives, network connections, remote access)
- Operating systems preventative maintenance
- Mobile operating systems (iOS, Android, Windows)
- Mobile device features
- Securing mobile devices
- Linux and macOS operating systems
- Linux and macOS filesystems
- Linux command line interface and basic commands
- Linux and macOS administration
- Security overview (costs of intrusion, goals of network security, creating a secure network strategy, defense in depth, layering, usability, minimizing exposure)
- Security threats (malware, network attacks, social engineering)
- Security policy
- Security procedures (physical security, data protection, data destruction)
- Best practices for securing a Windows workstation (passwords, local security policy, managing users and groups, firewalls, web security, updates, backups)
- Disaster recovery
- Change management
- IT documentation
- Soft skills (Communication skills, professional behavior, customer service)
- Legal and ethical considerations in IT

Learning activities

- A virtual environment for activities, assignments and projects utilizing a current Windows version and a popular UNIX operating system.
- This course requires some in class, hands-on work and also additional hands-on work in a virtual or on-campus computer lab.

Assessments

- Homework
- Lab Assignments
- Hands-on activities
- Projects
- Quizzes
- Exams
- Skills Exams

Grading guidelines

- A = 90-100
- B = 80-89
- C = 70-79
- D = 60-69
- F = 59 & below

Revision Date

May 20, 2020