Florida Department of Education
Curriculum Framework

The standards and/or benchmarks for this program were updated for the 2026-27 academic year.

Program Title: **Network Systems Administration**
Program Type: **Career Preparatory**
Career Cluster: **Information Technology**

Career Certificate Program		
Program Number	B079300	
CIP Number	0511090105	
Grade Level	30, 31	
Program Length	1050 hours	
Teacher Certification	Refer to the **Program Structure** section.	
CTSO	PBL, BPA	
SOC Codes (all applicable)	For program SOC codes, please see the Program and Course Tables section of the CTE Program Resources page linked below.	
CTE Program Resources	http://www.fldoe.org/academics/career-adult-edu/career-tech-edu/program-resources.stml	
Basic Skills Level	Computation (Mathematics): 9	Communications (Reading and Language Arts): 9

Purpose

This program offers a sequence of courses that provides coherent and rigorous content aligned with challenging academic standards and relevant technical knowledge and skills needed to prepare for further education and careers such as a Computer Support Assistant, Network Support Technician, Systems Administrator, Systems Engineer, Wireless Network Administrator, and Data Communications Analyst in the Information Technology career cluster; provides technical skill proficiency, and includes competency-based applied learning that contributes to the academic knowledge, higher-order reasoning and problem-solving skills, work attitudes, general employability skills, technical skills, and occupation-specific skills, and knowledge of all aspects of the Information Technology career cluster.

The content includes but is not limited to instruction in computer literacy; software application support; basic hardware configuration and troubleshooting; networking technologies, troubleshooting, security, and administration; and customer service and human relations skills.

Additional Information relevant to this Career and Technical Education (CTE) program is provided at the end of this document.

Program Structure

This program is a planned sequence of instruction consisting of seven occupational completion points.

This program is comprised of courses which have been assigned course numbers in the SCNS (Statewide Course Numbering System) in accordance with Section 1007.24 (1), F.S. Career and Technical credit shall be awarded to the student on a transcript in accordance with Section 1001.44(3)(b), F.S.

To teach the courses listed below, instructors must hold at least one of the teacher certifications indicated for that course.

The following table illustrates the postsecondary program structure:

			Teacher Certification	
A	OTA0040	Information Technology Assistant	OTA0040 Teacher Certifications	150 hours
B	EEV0504	Computer Support Assistant	BUS ED 1 @2 COMPU SCI 6 COMP SVC 7G CYBER TECH 7G INFO TECH 7G	150 hours
C	CTS0026	Network Support Technician		150 hours
D	CTS0027	Systems Administrator		150 hours
E	CTS0028	Systems Engineer		150 hours
F	CTS0029	Wireless Network Administrator		150 hours
G	EEV0317	Data Communications Analyst		150 hours

Florida's Career Readiness Skills for CTE Programs

Employability Skills

01.0	Apply academic skills to workplace scenarios.
	01.01 Use reading skills.
	01.02 Use writing skills.
	01.03 Use mathematical strategies and procedures.
	01.04 Use scientific principles and procedures.
02.0	Design a solution to an industry problem.
	02.01 Use critical thinking.
	02.02 Use creativity.
	02.03 Make sound decisions.
	02.04 Solve problems.
	02.05 Reason.
	02.06 Plan and organize.
03.0	Manage resources within an industry project
	03.01 Manage time.
	03.02 Manage money or resources.
	03.03 Manage materials.
	03.04 Manage personnel.
04.0	Oversee the subcomponents, operations and output of a technical or organizational system.
	04.01 Manage systems.
	04.02 Monitor systems.
	04.03 Improve systems.
05.0	Use information for decision making.
	05.01 Locate information.
	05.02 Organize information.
	05.03 Use information.

	05.04 Analyze information.
	05.05 Communicate information.
06.0	Apply relevant technology to workplace scenarios to aid productivity.
	06.01 Use technology.
07.0	Interpret and express interpersonal communication.
	07.01 Communicate verbally.
	07.02 Listen actively.
	07.03 Comprehend written material.
	07.04 Convey information in writing.
	07.05 Communicate nonverbally.
	07.06 Interpret nonverbal communication.
08.0	Interact with others to accomplish workplace goals.
	08.01 Collaborate with others in a team.
	08.02 Respond to customer needs.
	08.03 Exercise leadership.
	08.04 Negotiate to resolve conflict.
	08.05 Respect others.
09.0	Manage personal behavior to maximize productivity and professional growth.
	09.01 Demonstrate responsibility and self-discipline.
	09.02 Adapt and show flexibility.
	09.03 Work independently.
	09.04 Demonstrate a willingness to learn.
	09.05 Demonstrate integrity.
	09.06 Demonstrate professionalism.
	09.07 Take initiative.
	09.08 Display positive attitude.
	09.09 Take responsibility for professional growth.

Job Attainment	
10.0	Find, assess and apply to job opportunities.
10.01	Identify online job posts relevant to his or her career aspirations.
10.02	Compare and contrast the job posts' required qualifications, job duties, compensation, benefits and employers.
10.03	Define what information, documentation and writing prompts are required for the positions.
11.0	Communicate personal competence, character and fit for a job opportunity.
11.01	Develop a resume.
11.02	Write a cover letter.
11.03	Curate a professional portfolio that includes work products.
11.04	Prepare for and experience a mock job interview.
12.0	Cultivate and leverage relationships to professionally advance.
12.01	Request a signed reference letter, letter of recommendation and/or an online skill/professionalism endorsement.
12.02	Develop a plan to cultivate a professional digital footprint.
12.03	Develop a networking plan for a specific industry of interest.

Standards

Information Technology Assistant (OTA0040) is the first course in this and other programs within the Information Technology Career Cluster. Standards 01.0 – 15.0 are associated with this course.

After successfully completing this program, the student will be able to perform the following:

01.0 Demonstrate knowledge, skill, and application of information technology to accomplish job objectives and enhance workplace performance.
02.0 Demonstrate an understanding of networks.
03.0 Use word processing applications to enhance the effectiveness of various types of documents and communication.
04.0 Use presentation applications to enhance communication skills.
05.0 Use spreadsheet applications to enhance communication skills.
06.0 Use database applications to store and organize data.
07.0 Use electronic mail to enhance communication skills.
08.0 Investigate individual assessment and job/career exploration and individual career planning that reflect the transition from school to work, lifelong learning, and personal and professional goals.
09.0 Incorporate appropriate leadership and supervision techniques, customer service strategies, and standards of personal ethics to accomplish job objectives and enhance workplace performance.
10.0 Demonstrate competence using computer networks, Internet and online databases to facilitate collaborative or individual learning and communication.
11.0 Develop awareness of computer languages, web-based and software applications, and emerging technologies.
12.0 Demonstrate comprehension and communication skills.
13.0 Use social media to enhance online communication and develop an awareness of a digital footprint.
14.0 Develop an awareness of the fundamentals of cybersecurity.
15.0 Investigate emerging technologies and their impact on the world.
16.0 Incorporate appropriate leadership, customer-service strategies and professional ethics to enhance workplace performance.
17.0 Install, configure, and upgrade desktop and mobile computer systems following industry-standard procedures.
18.0 Diagnose and troubleshoot hardware, software, and connectivity problems.
19.0 Apply safety, maintenance, and environmental sustainability practices.
20.0 Demonstrate understanding of processors, memory and storage technologies.
21.0 Demonstrate knowledge of printing and imaging systems.
22.0 Demonstrate basic networking concepts and connectivity skills.
23.0 Provide effective end-user assistance.
24.0 Demonstrate proficiency using modern graphical user interfaces and productivity tools.
25.0 Incorporate leadership, supervision, customer-service strategies, and ethical standards to enhance workplace performance.
26.0 Participate in work-based learning experiences.
27.0 Perform end-user support through multiple communication channels.
28.0 Install and configure operating systems and network services.
29.0 Demonstrate proficiency using network standards and protocols.
30.0 Configure and troubleshoot hardware devices and drivers.

31.0 Monitor and optimize system performance and reliability.
32.0 Manage and troubleshoot storage and user data.
33.0 Configure and troubleshoot network connections.
34.0 Implement and troubleshoot system and network security.
35.0 Demonstrate effective communication in technical environments.
36.0 Apply critical thinking and problem-solving skills.
37.0 Use information technology tools to enhance productivity and collaboration.
38.0 Describe organizational roles and team dynamics in IT environments.
39.0 Demonstrate professional ethics and legal responsibilities in IT support.
40.0 Incorporate leadership, customer-service strategies, and ethical standards to enhance workplace performance.
41.0 Participate in work-based learning experiences.
42.0 Administer accounts and resources on computers running server operating systems.
43.0 Modify and manage directory objects.
44.0 Perform administrative functions using groups.
45.0 Manage access to resources and permissions.
46.0 Implement printing and device management in a network environment.
47.0 Delegate administrative control and manage organizational units.
48.0 Implement Group Policy and centralized configuration management.
49.0 Manage computer and server security.
50.0 Administer servers remotely.
51.0 Monitor and analyze server performance.
52.0 Collect performance data and identify system bottlenecks.
53.0 Maintain device drivers and hardware compatibility.
54.0 Configure and manage disks and volumes.
55.0 Secure data through encryption and quotas.
56.0 Plan for and perform disaster recovery and business continuity.
57.0 Manage software updates and patch management.
58.0 Configure IP addressing and troubleshoot address issues.
59.0 Configure an Internet protocol (IP) address for client computers.
60.0 Implement name resolution and DNS services.
61.0 Configure routing, remote access, and VPN connectivity.
62.0 Install and configure client operating systems.
63.0 Configure and support remote and mobile users.
64.0 Monitor resources and system performance.
65.0 Demonstrate the importance of health, safety, and environmental management systems.
66.0 Demonstrate leadership and teamwork skills.
67.0 Explain employability and entrepreneurship skills.
68.0 Apply communication skills (reading, writing, speaking, listening, viewing) in a courteous, concise, and correct manner on personal and professional levels.
69.0 Participate in work-based learning experiences.

70.0 Plan a network infrastructure.
71.0 Plan and optimize a TCP/IP physical and logical network.
72.0 Plan and troubleshoot routing.
73.0 Plan a DHCP strategy.
74.0 Plan a DNS strategy.
75.0 Optimize and troubleshoot DNS.
76.0 Plan and troubleshoot IPsec and network security.
77.0 Plan network access.
78.0 Troubleshoot network access.
79.0 Analyze global director infrastructure.
80.0 Implement directory and domain structure.
81.0 Implement organizational unit (O.U.) structures.
82.0 Implement user, group, and computer accounts.
83.0 Implement Group Policy and access management.
84.0 Deploy and manage software and updates through policy.
85.0 Implement sites and replication strategies.
86.0 Implement domain-controller placement and resilience.
87.0 Design and apply a security framework.
88.0 Recognize and predict common threats by using a threat model.
89.0 Apply risk management principles.
90.0 Design security for physical resources.
91.0 Design security for computers and endpoints.
92.0 Design security for accounts and identities.
93.0 Design security for authentication and access control.
94.0 Design security for data and storage.
95.0 Design security for data transmission.
96.0 Design security for network perimeters and edge devices.
97.0 Design an audit policy and an incident response procedure.
98.0 Linux Foundation.
99.0 Linux Fundamentals.
100.0 Linux installation and configuration.
101.0 Linux Systems Operation.
102.0 Linux users, groups, and permissions.
103.0 Linux Basic Security and System Monitoring.
104.0 Participate in simulated work-based learning experiences.
105.0 Demonstrate proficiency in applying radio frequency (RF) technologies.
106.0 Develop an awareness of wireless LAN technologies.
107.0 Perform implementation and management activities.
108.0 Develop an awareness of wireless security systems.
109.0 Demonstrate knowledge of wireless industry standards.

110.0 Participate in simulated work-based learning experiences.
111.0 Demonstrate knowledge of general security concepts.
112.0 Develop an awareness of communication security concepts.
113.0 Develop an awareness of network infrastructure security.
114.0 Develop an awareness of cryptography and its relation to security.
115.0 Incorporate organizational and operational security in an appropriate and effective manner.

Florida Department of Education
Student Performance Standards

Program Title: Network Systems Administration
Career Certificate Program Number: B079300

Course Number: OTA0040 **Occupational Completion Point: A** **Information Technology Assistant – 150 Hours**	
Information Technology Assistant (OTA0040) is part of several programs across the various CTE career clusters. To ensure consistency, the standards and benchmarks for this course (01.0 – 15.0) have been placed in a separate document. To access this document, visit: Information Technology Assistant (OTA0040)	
Course Number: EEV0504 **Occupational Completion Point: B** **Computer Support Assistant – 150 Hours**	
16.0	Incorporate appropriate leadership, customer-service strategies and professional ethics to enhance workplace performance. The student will be able to:
16.01	Develop courteous, solution-focused communication methods when assisting customers.
16.02	Demonstrate teamwork, adaptability, and positive attitude in classroom or help-desk simulations.
16.03	Apply ethical and confidentiality standards when handling user data or credentials.
16.04	Document service requests and resolutions accurately using digital ticketing or workflow systems.
17.0	Install, configure, and upgrade desktop and mobile computer systems following industry-standard procedures. The student will be able to:
17.01	Identify major hardware components (motherboard, CPU, memory, storage, power, I/O devices) and describe their functions.
17.02	Recognize modern interface standards (USB-C, HDMI, DisplayPort, Bluetooth, Wi-Fi, Ethernet).
17.03	Assemble, disassemble, and reassemble systems safely using antistatic and ESD precautions.
17.04	Install and configure operating systems (Windows 10/11, Linux, macOS) and required drivers.
17.05	Perform system updates, backups, and recovery procedures.
17.06	Install productivity, collaboration, and endpoint-management applications.
17.07	Configure basic virtualization software for testing or lab use.
17.08	Customize user settings, accessibility features, and regional preferences.
17.09	Explain the importance of firmware/BIOS updates and secure-boot settings.

18.0	Diagnose and troubleshoot hardware, software, and connectivity problems. The student will be able to:
	18.01 Apply structured troubleshooting methodologies to isolate faults.
	18.02 Use built-in diagnostics, system logs, and Task Manager to analyze performance issues.
	18.03 Troubleshoot startup failures, application crashes, and driver conflicts.
	18.04 Resolve common peripheral, display, and input/output problems.
	18.05 Identify symptoms of failing components and recommend replacement or repair.
	18.06 Diagnose basic network-connectivity issues using ping, ipconfig/ifconfig, and Wi-Fi utilities.
	18.07 Apply malware-removal and remediation techniques using approved tools.
	18.08 Document troubleshooting steps and verify operational success with the user.
19.0	Apply safety, maintenance, and environmental sustainability practices.
	19.01 Follow safe tool usage, lifting, and electrical-safety guidelines.
	19.02 Perform routine cleaning, firmware updates, and hardware checks to maintain reliability.
	19.03 Dispose of electronic waste responsibly (batteries, toner, displays) per EPA and school-district standards.
	19.04 Apply ergonomic principles for workstation design and device placement.
	19.05 Secure devices and data using cable locks, privacy screens, and password protection.
20.0	Demonstrate understanding of processors, memory, and storage technologies. The student will be able to:
	20.01 Differentiate types and speeds of RAM, cache, and storage media (SSD, NVMe, cloud).
	20.02 Install and configure internal and external storage devices.
	20.03 Explain the relationship between CPU cores, threads, and virtualization features.
	20.04 Configure and verify disk partitions and file systems.
	20.05 Describe basic redundancy concepts such as RAID and cloud backup.
21.0	Demonstrate knowledge of printing and imaging systems. The student will be able to:
	21.01 Identify common printer types (laser, inkjet, thermal, multifunction) and their use cases.
	21.02 Install and configure printers locally and on a network.
	21.03 Troubleshoot print queues, driver mismatches, and connectivity issues.
	21.04 Implement environmentally responsible printing practices and consumable recycling.
22.0	Demonstrate basic networking concepts and connectivity skills.

	22.01 Define networking and describe its purpose in a business environment.
	22.02 Identify the functions of key components (switches, routers, access points, cables).
	22.03 Explain network topologies, IP addressing, and common protocols (TCP/IP, DNS, DHCP).
	22.04 Connect and configure a workstation for wired and wireless access.
	22.05 Verify network connectivity and performance using diagnostic tools.
	22.06 Describe the importance of network security measures such as firewalls and encryption.
	22.07 Perform basic data-backup and restore operations using local or cloud storage.
	22.08 Explain the purpose of disaster-recovery planning and business-continuity concepts.
23.0	Provide effective end-user assistance. The student will be able to:
	23.01 Use professional communication and active-listening techniques when supporting users.
	23.02 Gather and record accurate problem details in a service ticket.
	23.03 Provide step-by-step guidance or remote assistance for basic issues.
	23.04 Escalate unresolved problems following established procedures.
24.0	Demonstrate proficiency using modern graphical user interfaces and productivity tools. The student will be able to:
	24.01 Navigate GUI environments and customize layouts for accessibility and efficiency.
	24.02 Use menus, ribbons, and keyboard shortcuts effectively.
	24.03 Organize and maintain file structures in local and cloud directories.
	24.04 Run multiple applications, manage windows, and multitask securely.
	24.05 Access help systems, documentation, and online knowledge bases for problem-solving.
Course Number: CTS0026 **Occupational Completion Point: C** **Network Support Technician – 150 Hours**	
25.0	Incorporate leadership, supervision, customer-service strategies, and ethical standards to enhance workplace performance. The student will be able to:
	25.01 Communicate professionally and diplomatically with customers and peers to resolve technical issues.
	25.02 Demonstrate integrity, confidentiality, and professional ethics when handling client information.
26.0	Participate in work-based learning experiences. The student will be able to:
	26.01 Participate in simulated or real network support projects using trouble-ticket systems and change-management workflows.

	26.02 Demonstrate the use of technology tools to support end-users, including remote-support and collaboration platforms.
27.0	Provide end-user support through multiple communication channels. The student will be able to:
	27.01 Perform first-response troubleshooting for hardware, software, and network issues via phone, email, chat, or remote desktop.
	27.02 Document incidents accurately and follow escalation procedures.
	27.03 Demonstrate effective listening and customer-service skills when assisting users.
28.0	Install and configure operating systems and network services. The student will be able to:
	28.01 Install, configure, and update client operating systems (Windows 10/11, Linux Mint/Ubuntu).
	28.02 Join workstations to a domain or directory service (Active Directory, Azure AD, or LDAP).
	28.03 Configure Internet connectivity and basic LAN parameters (IP, DNS, gateway).
	28.04 Deploy operating-system images using WDS, MDT, or cloning software.
	28.05 Install and configure network applications such as file sharing, printers, and web services.
	28.06 Monitor and troubleshoot shared resources and permissions.
	28.07 Implement remote-management tools and assist with updates and patches.
29.0	Demonstrate proficiency using network standards and protocols. The student will be able to:
	29.01 Describe the purpose of network standards (IEEE, IETF) and protocols (TCP/IP, DNS, DHCP, HTTP, FTP, SSH).
	29.02 Explain the OSI and TCP/IP models and map common protocols to each layer.
	29.03 Use network utilities (ping, tracert, ipconfig, nslookup, netstat) to verify connectivity.
30.0	Configure and troubleshoot hardware devices and drivers. The student will be able to:
	30.01 Install and configure hardware components (NICs, storage, peripherals).
	30.02 Update, roll back, or uninstall device drivers.
	30.03 Troubleshoot hardware resource conflicts and compatibility issues.
	30.04 Use diagnostic utilities to verify device functionality and firmware versions.
31.0	Monitor and optimize system performance and reliability. The student will be able to:
	31.01 Monitor CPU, memory, disk, and network usage using built-in tools (Task Manager, Resource Monitor, Performance Monitor).
	31.02 Manage startup processes and optimize system resources.
	31.03 Implement scheduled maintenance tasks (cleanups, updates, defragmentation).
	31.04 Perform system and user data backups and restores.

32.0	Manage and troubleshoot storage and user data. The student will be able to:
	32.01 Configure user profiles and local folder redirection.
	32.02 Partition and format drives; monitor and repair volumes using disk utilities.
	32.03 Configure disk quotas and data compression.
	32.04 Recover from disk errors and restore lost data using recovery tools.
33.0	Configure and troubleshoot network connections. The student will be able to:
	33.01 Install and configure network adapters and drivers.
	33.02 Configure IP addressing (IPv4 and IPv6), subnet masks, and gateways.
	33.03 Test and troubleshoot LAN and WLAN connections using appropriate tools.
	33.04 Configure VPN clients and remote access solutions.
	33.05 Identify and resolve common network protocol issues (DNS, DHCP, HTTP, SMB).
34.0	Implement and troubleshoot system and network security. The student will be able to:
	34.01 Apply operating-system security settings, local policies, and account management.
	34.02 Configure and troubleshoot file and folder permissions and encryption (EFS, BitLocker).
	34.03 Enable auditing and review security logs.
	34.04 Implement antivirus, firewall, and endpoint protection solutions.
	34.05 Apply principles of least privilege and password/MFA policies.
35.0	Demonstrate effective communication in technical environments. The student will be able to:
	35.01 Communicate technical information clearly to non-technical users in oral and written form.
	35.02 Document troubleshooting steps and solutions using industry-standard templates.
	35.03 Deliver informal presentations or training to colleagues on IT topics.
	35.04 Use professional tone and grammar in all correspondence (tickets, chat, email).
36.0	Apply critical thinking and problem-solving skills. The student will be able to:
	36.01 Use structured troubleshooting models (CompTIA A+ 6-step process) to diagnose issues.
	36.02 Collaborate with team members to resolve complex technical problems.
	36.03 Conduct research using technical documentation and vendor resources.
	36.04 Track and analyze patterns in recurring issues to develop preventive solutions.

37.0	Use information technology tools to enhance productivity and collaboration. The student will be able to:
	37.01 Utilize IT asset-management and ticketing systems to record and track incidents.
	37.02 Use office productivity applications (Google Workspace, Microsoft 365) for documentation and reporting.
	37.03 Leverage remote-support and collaboration tools (Teams, Zoom, Slack) to assist users and teams.
	37.04 Apply version-control and file-management best practices for shared projects.
38.0	Describe organizational roles and team dynamics in IT environments. The student will be able to:
	38.01 Explain the structure and function of IT departments within an organization.
	38.02 Describe cross-functional collaboration between help desk, network, and security teams.
	38.03 Discuss quality assurance and continuous improvement processes in IT support.
	38.04 Identify how global and cloud technologies impact modern IT operations.
39.0	Demonstrate professional ethics and legal responsibilities in IT support. The student will be able to:
	39.01 Apply ethical decision-making when handling confidential data and user information.
	39.02 Recognize and comply with organizational policies and relevant laws (HIPAA, FERPA, GDPR).
	39.03 Describe the long-term consequences of unethical or illegal behavior in technology fields.
	39.04 Demonstrate responsible use of digital resources and adherence to acceptable-use policies.
Course Number: CTS0027 **Occupational Completion Point: D** **Systems Administrator – 150 Hours**	
40.0	Incorporate leadership, supervision, customer-service strategies, and ethical standards to enhance workplace performance. The student will be able to:
	40.01 Communicate professionally and diplomatically with customers and end users to resolve technical issues efficiently.
	40.02 Demonstrate ethical decision-making and confidential data-handling in IT environments.
41.0	Participate in work-based learning experiences. The student will be able to:
	41.01 Participate in simulated system-administration projects using ticketing and change-management tools.
	41.02 Discuss the role of technology in enterprise operations and IT service delivery.
	41.03 Demonstrate basic supervisory and project-coordination skills in a team environment.
42.0	Administer accounts and resources on computers running server operating systems. The student will be able to:
	42.01 Identify core roles and features of modern server operating systems (Windows Server 2022+, Linux Server distributions).

	42.02 Install and configure administrative tools (Active Directory Users and Computers, Server Manager, Remote Server Administration Tools).
	42.03 Create and manage user, group, and computer accounts.
	42.04 Organize resources within organizational units (OUs) for delegated administration.
43.0	Modify and manage directory objects. The student will be able to:
	43.01 Modify user and computer properties, enable and unlock accounts, and reset credentials.
	43.02 Locate directory objects using queries and PowerShell filters.
	43.03 Move and restore objects between organizational units and domains.
44.0	Perform administrative functions using groups. The student will be able to:
	44.01 Create and manage security and distribution groups.
	44.02 Assign permissions and roles through group membership.
	44.03 Apply best practices for group nesting and role-based access control (RBAC).
45.0	Manage access to resources and permissions. The student will be able to:
	45.01 Configure NTFS and share permissions for files and folders.
	45.02 Evaluate effective permissions and resolve conflicts.
	45.03 Implement access-based enumeration and offline files for remote users.
46.0	Implement printing and device management in a network environment. The student will be able to:
	46.01 Deploy printers using Group Policy or Universal Print services.
	46.02 Manage driver packages and printing permissions.
	46.03 Monitor and troubleshoot print queues and print servers.
47.0	Delegate administrative control and manage organizational units. The student will be able to:
	47.01 Plan OU hierarchies based on administrative and security requirements.
	47.02 Delegate control safely and audit delegated rights.
	47.03 Modify permissions for Active Directory objects following principle of least privilege.
48.0	Implement Group Policy and centralized configuration management. The student will be able to:
	48.01 Create and link Group Policy Objects (GPOs) to OUs and domains.
	48.02 Configure logon/logoff scripts and folder redirection.
	48.03 Implement security templates and administrative policies.

49.0	Manage computer and server security. The student will be able to:
	49.01 Apply security baselines and use Microsoft Security Compliance Toolkit or Linux CIS Benchmarks.
	49.02 Configure audit policies and analyze security logs.
	49.03 Implement firewall rules, antivirus, and endpoint protection solutions.
	49.04 Test and document security controls to ensure compliance.
50.0	Administer servers remotely. The student will be able to:
	50.01 Configure remote administration using RDP, PowerShell Remoting, or SSH.
	50.02 Secure remote sessions through encryption and multi-factor authentication.
	50.03 Manage remote services and scheduled tasks.
51.0	Monitor and analyze server performance. The student will be able to:
	51.01 Establish performance baselines and utilize Performance Monitor and Resource Monitor.
	51.02 Create and analyze performance logs and alerts.
	51.03 Use Task Manager and Event Viewer to detect anomalies.
52.0	Collect performance data and identify system bottlenecks. The student will be able to:
	52.01 Monitor CPU, memory, disk I/O, and network subsystems.
	52.02 Interpret counters and thresholds to identify bottlenecks.
	52.03 Recommend optimization or scaling solutions based on data.
53.0	Maintain device drivers and hardware compatibility. The student will be able to:
	53.01 Install and update drivers through Windows Update or vendor repositories.
	53.02 Roll back or restore previous drivers if compatibility issues occur.
54.0	Configure and manage disks and volumes. The student will be able to:
	54.01 Initialize, partition, and format storage devices.
	54.02 Create and extend volumes, mount points, and storage pools.
	54.03 Convert between basic and dynamic disks.
	54.04 Implement Storage Spaces and RAID redundancy.
55.0	Secure data through encryption and quotas. The student will be able to:
	55.01 Apply file compression and disk encryption (BitLocker, LUKS).

	55.02 Configure file encryption (EFS) and access control policies.
	55.03 Set and manage disk quotas to control storage usage.
56.0	Plan for and perform disaster recovery and business continuity. The student will be able to:
	56.01 Develop backup strategies using Windows Server Backup or third-party solutions.
	56.02 Schedule and verify incremental and full backups.
	56.03 Implement volume shadow copies and file version restoration.
	56.04 Perform bare-metal recovery and system state restores.
57.0	Manage software updates and patch management. The student will be able to:
	57.01 Deploy updates using Windows Server Update Services (WSUS), Intune, or Linux repositories.
	57.02 Automate patch approval and reporting.
	57.03 Validate update compliance and rollback failed deployments.
58.0	Configure IP addressing and troubleshoot address issues. The student will be able to:
	58.01 Convert IP Addresses from decimal to binary.
	58.02 Calculate a subnet mask.
	58.03 Create subnets using VLSM and CIDR.
	58.04 Isolate addressing issues associated with the IP routing process.
59.0	Configure an Internet protocol (IP) address for client computers. The student will be able to:
	59.01 Plan IPv4/IPv6 addressing schemes using VLSM and CIDR.
	59.02 Configure static and dynamic addresses.
	59.03 Identify and resolve routing and addressing conflicts.
60.0	Implement name resolution and DNS services. The student will be able to:
	60.01 Install and configure DNS servers and zones.
	60.02 Configure forwarders, conditional forwarding, and dynamic updates.
	60.03 Troubleshoot DNS records and caching issues using nslookup and PowerShell.
61.0	Configure routing, remote access, and VPN connectivity. The student will be able to:
	61.01 Implement Routing and Remote Access Services (RRAS) or Linux routing.
	61.02 Configure VPN connections (IPsec, SSL, or L2TP).

	61.03 Centralize authentication through RADIUS or Network Policy Server (NPS).
62.0	Install and configure client operating systems. The student will be able to:
	62.01 Deploy and upgrade client OS images using MDT or WDS.
	62.02 Automate installations with unattended files or deployment scripts.
	62.03 Configure domain joins and post-installation settings.
63.0	Configure and support remote and mobile users. The student will be able to:
	63.01 Configure Remote Desktop, VPN, and cloud workspace access.
	63.02 Implement authentication and encryption protocols for remote connections.
	63.03 Support mobile devices using Intune or Mobile Device Management (MDM).
64.0	Monitor resources and system performance. The student will be able to:
	64.01 Collect system information using Task Manager, Performance Monitor, and Resource Monitor.
	64.02 Analyze event logs for system and application errors.
	64.03 Use automated maintenance and optimization tools.
65.0	Demonstrate the importance of health, safety, and environmental management systems. The student will be able to:
	65.01 Follow safe electrical and ergonomic work practices when handling equipment.
	65.02 Describe emergency procedures and incident reporting requirements.
	65.03 Create a disaster or emergency response plan for IT operations.
66.0	Demonstrate leadership and teamwork skills. The student will be able to:
	66.01 Apply leadership principles to coordinate system projects and mentorship.
	66.02 Collaborate effectively within technical and cross-department teams.
	66.03 Conduct and document meetings to achieve team goals.
67.0	Explain employability and entrepreneurship skills. The student will be able to:
	67.01 Demonstrate positive work behaviors and professional attitudes.
	67.02 Develop a career plan including industry certifications.
	67.03 Research employment and entrepreneurial opportunities in systems administration.
	67.04 Maintain a career portfolio and continuing-education record.

Course Number: CTS0028 **Occupational Completion Point: E** **Systems Engineer – 150 Hours**	
68.0	Apply communication skills (reading, writing, speaking, listening, viewing) in a courteous, concise, and correct manner on personal and professional levels. The student will be able to:
	68.01 Communicate complex technical information clearly to technical and non-technical audiences using written, oral, and visual formats.
	68.02 Document configuration procedures, incident reports, and project summaries using professional IT communication standards.
69.0	Participate in work-based learning experiences. The student will be able to:
	69.01 Participate in simulated enterprise environments using ticketing, monitoring, and documentation systems.
	69.02 Demonstrate the use of modern network-management and automation tools.
	69.03 Compare and evaluate software and cloud-based applications used in systems administration and support.
70.0	Plan a network infrastructure. The student will be able to:
	70.01 Design scalable and redundant network topologies.
	70.02 Plan and document test environments for configuration and staging.
	70.03 Utilize management and monitoring tools for lifecycle maintenance.
	70.04 Identify technologies and services implemented in modern LAN, WAN, and cloud networks.
71.0	Plan and optimize a TCP/IP physical and logical network. The student will be able to:
	71.01 Explain the TCP/IP model and IPv4/IPv6 addressing schemes.
	71.02 Design IP addressing, subnetting, and VLSM plans.
	71.03 Optimize network performance using QoS, VLAN segmentation, and redundancy protocols.
72.0	Plan and troubleshoot routing. The student will be able to:
	72.01 Explain routing concepts and protocols (static, RIP, OSPF, BGP).
	72.02 Develop and implement secure routing strategies.
	72.03 Use routing diagnostic tools (ping, traceroute, netstat, pathping).
	72.04 Troubleshoot dynamic and static routing issues.
73.0	Plan a DHCP strategy. The student will be able to:
	73.01 Explain DHCP operation in enterprise networks.
	73.02 Design IP scope and reservation strategies for LAN and VLAN segments.
	73.03 Secure DHCP deployment through logging and access control.

74.0	Plan a DNS strategy. The student will be able to:
	74.01 Design namespace and zoning schemes supporting Active Directory and cloud integration.
	74.02 Configure primary and secondary zones with redundant replication.
	74.03 Deploy DNS security extensions (DNSSEC) to ensure integrity.
	74.04 Plan internal and external DNS resolution strategies.
75.0	Optimize and troubleshoot DNS. The student will be able to:
	75.01 Optimize DNS server performance and query response times.
	75.02 Monitor zone replication and server-to-server communications.
	75.03 Configure client-side DNS settings for enterprise efficiency.
	75.04 Troubleshoot name-resolution and connectivity issues using diagnostic tools.
76.0	Plan and troubleshoot IPsec and network security. The student will be able to:
	76.01 Explain IPsec protocols (AH, ESP) and their use in VPNs.
	76.02 Configure secure IPsec policies and rules in enterprise networks.
	76.03 Integrate IPsec with modern VPN technologies and cloud tunnels.
	76.04 Troubleshoot IPsec tunnel connectivity and encryption issues.
77.0	Plan network access. The student will be able to:
	77.01 Select appropriate wired and wireless access methods for users and devices.
	77.02 Develop remote-access and Zero-Trust Network Access (ZTNA) strategies.
	77.03 Implement RADIUS, TACACS+, and certificate-based authentication.
	77.04 Design a secure network-access and authorization plan.
78.0	Troubleshoot network access. The student will be able to:
	78.01 Use diagnostic utilities and logs to resolve connectivity issues.
	78.02 Troubleshoot wired and wireless authentication failures.
	78.03 Diagnose LAN segmentation or VLAN misconfigurations.
	78.04 Resolve remote-access and VPN issues.
79.0	Analyze global director infrastructure. The student will be able to:
	79.01 Describe Active Directory and Lightweight Directory Access Protocol (LDAP) architectures.

	79.02 Use administrative tools to analyze directory components.
	79.03 Plan and document directory design and replication requirements.
80.0	Implement directory and domain structure. The student will be able to:
	80.01 Create forests, domains, and organizational trusts.
	80.02 Configure DNS integration within directory services.
	80.03 Manage functional levels and domain relationships.
	80.04 Secure trust relationships using filtering and conditional access.
81.0	Implement organizational unit (O.U.) structures. The student will be able to:
	81.01 Create and organize O.U.s based on administrative roles and locations.
	81.02 Delegate permissions and control within O.U. hierarchies.
	81.03 Plan O.U. design to align with enterprise policy and security requirements.
82.0	Implement user, group, and computer accounts. The student will be able to:
	82.01 Create and manage accounts using Active Directory and automation tools such as PowerShell.
	82.02 Implement naming conventions and UPN suffixes.
	82.03 Move objects within and across domains while preserving permissions.
	82.04 Plan and audit account policies and lifecycle management.
83.0	Implement Group Policy and access management. The student will be able to:
	83.01 Create and configure Group Policy Objects (GPOs).
	83.02 Apply GPOs to users, computers, and O.U.s appropriately.
	83.03 Troubleshoot and verify Group Policy application.
	83.04 Delegate administrative control of Group Policies.
	83.05 Plan policy hierarchies to support compliance and security.
84.0	Deploy and manage software and updates through policy. The student will be able to:
	84.01 Explain modern software deployment concepts using Group Policy and Endpoint Management.
	84.02 Deploy applications using GPOs, MSI packages, or cloud management tools (Intune, SCCM).
	84.03 Manage updates and patches across enterprise devices.
	84.04 Troubleshoot software deployment and update failures.

	84.05 Plan a software deployment and maintenance strategy.
85.0	Implement sites and replication strategies. The student will be able to:
	85.01 Explain Active Directory replication processes and components.
	85.02 Create and configure sites and subnets for replication control.
	85.03 Monitor and troubleshoot replication failures.
	85.04 Design a site strategy based on bandwidth and security requirements.
86.0	Implement domain-controller placement and resilience. The student will be able to:
	86.01 Plan domain-controller and global-catalog placement across sites.
	86.02 Determine replication frequency and monitoring strategies.
	86.03 Design fault-tolerant domain-controller layouts for high availability.
87.0	Design and apply a security framework. The student will be able to:
	87.01 Describe core elements of enterprise security policies and procedures.
	87.02 Develop a security design framework based on industry standards (NIST, CIS, ISO 27001).
	87.03 Form a security planning and implementation team.
88.0	Recognize and predict common threats by using a threat model. The student will be able to:
	88.01 Explain modern vulnerabilities and attack vectors (phishing, malware, insider threats).
	88.02 Apply threat modeling methodologies such as STRIDE or MITRE ATT&CK to anticipate risks.
89.0	Apply risk management principles. The student will be able to:
	89.01 Explain risk assessment and treatment methods.
	89.02 Develop a risk management plan including impact analysis and mitigation controls.
90.0	Design security for physical resources. The student will be able to:
	90.01 Assess threats to facilities and equipment.
	90.02 Design physical security controls (environmental, access, video monitoring, locks).
91.0	Design security for computers and endpoints. The student will be able to:
	91.01 Analyze and mitigate endpoint vulnerabilities (antivirus, EDR, HIDS).
	91.02 Design hardening standards for servers and workstations.
92.0	Design security for accounts and identities. The student will be able to:

	92.01 Assess account privilege risks and apply least-privilege principles.
	92.02 Design account protection using multi-factor authentication and conditional access.
93.0	Design security for authentication and access control. The student will be able to:
	93.01 Evaluate authentication threats and develop identity protection strategies.
	93.02 Design role-based and policy-based access control mechanisms.
94.0	Design security for data and storage. The student will be able to:
	94.01 Identify data classification levels and associated risks.
	94.02 Design data protection and encryption strategies for storage systems and cloud resources.
95.0	Design security for data transmission. The student will be able to:
	95.01 Analyze risks to data in transit and apply secure protocols (TLS, SSH, HTTPS).
	95.02 Design encryption and tunneling methods for data communication.
96.0	Design security for network perimeters and edge devices. The student will be able to:
	96.01 Identify threats to network perimeters and edge infrastructure.
	96.02 Design segmentation and defense-in-depth architectures using firewalls and IDS/IPS.
97.0	Design an audit policy and an incident response procedure. The student will be able to:
	97.01 Explain the importance of auditing, logging, and incident response.
	97.02 Develop an audit policy and retention plan.
	97.03 Create an incident-response and post-incident review procedure.
98.0	Linux Foundation. The student will be able to:
	98.01 Explain the evolution and philosophy of Linux and open-source software.
	98.02 Differentiate between common distributions and their enterprise roles.
	98.03 Describe the GNU General Public License (GPL) and Free/Open Source Software (FOSS) concepts.
	98.04 Identify Linux roles in server, network, and cloud environments.
99.0	Linux Fundamentals. The student will be able to:
	99.01 Access and use the command line shell.
	99.02 Utilize sudo and root privileges safely.
	99.03 Use text editors (vi, nano) and manual pages for reference.

	99.04 Manage environment variables and shell profiles.
	99.05 Perform redirection, piping, and process control.
	99.06 Manage files, links, and directory structures based on the Filesystem Hierarchy Standard.
	99.07 Compress, archive, and extract files using standard utilities.
100.0	Linux installation and configuration. The student will be able to:
	100.01 Plan and perform Linux installation including partitioning and LVM.
	100.02 Install server and desktop distributions in bare-metal or virtual environments.
	100.03 Configure boot loaders and startup parameters (GRUB2).
101.0	Linux Systems Operation. The student will be able to:
	101.01 Manage processes and services using systemd.
	101.02 Monitor resource usage and update software packages.
	101.03 Mount and unmount volumes and shared storage.
	101.04 Manage libraries and dependencies.
102.0	Linux users, groups, and permissions. The student will be able to:
	102.01 List, create, and manage local users and groups.
	102.02 Explain the use of the /etc/passwd and /etc/shadow files and their security implications.
	102.03 Assign users to groups and manage group memberships.
	102.04 Explain Linux file and folder ownership, permissions, and inheritance.
	102.05 Change ownership and group ownership using chown and chgrp.
	102.06 Interpret and modify file permissions using symbolic and octal (binary) notation.
	102.07 Demonstrate read, write, and execute permissions and how they affect system security.
	102.08 Apply and remove special permissions (setuid, setgid, sticky bit).
	102.09 Implement basic access-control lists (ACLs) to extend standard permissions.
103.0	Linux Basic Security and System Monitoring. The student will be able to:
	103.01 Configure IPv4 and IPv6 interfaces manually and with NetworkManager.
	103.02 Deploy and manage firewall rules using iptables or nftables.
	103.03 Monitor and analyze log files using tail, less, grep, journalctl, and logrotate.

103.04 Back up and restore critical system and security logs.
103.05 Write and schedule scripts with bash and cron to automate administrative tasks.
103.06 Harden systems by disabling unnecessary services and closing unused ports.
103.07 Implement fail2ban or equivalent intrusion-prevention software for brute-force protection.
103.08 Explain and apply the principle of least privilege on Linux systems.
Course Number: CTS0029 **Occupational Completion Point: F** **Wireless Network Administrator – 150 Hours**
104.0 Participate in simulated work-based learning experiences. The student will be able to:
104.01 Participate in simulated wireless network support tasks including installation, configuration, and troubleshooting of WLAN components.
104.02 Use network monitoring and documentation tools to log maintenance activities and technical findings.
104.03 Demonstrate effective communication, teamwork, and customer service within a wireless support environment.
105.0 Demonstrate proficiency in applying radio frequency (RF) technologies. The student will be able to:
105.01 Define and apply basic RF behavior concepts including frequency, amplitude, wavelength, and signal attenuation.
105.02 Explain antenna types (omnidirectional, directional, sector, patch) and their uses in various wireless environments.
105.03 Identify components affecting RF transmission such as gain, reflection, absorption, and interference.
105.04 Describe spread-spectrum techniques including DSSS, OFDM, and MIMO as used in modern Wi-Fi standards.
105.05 Explain channel bonding, bandwidth allocation, and modulation schemes (QAM, OFDMA).
105.06 Identify FCC regulations governing wireless transmissions including frequency bands, channel spacing, and power limits.
105.07 Recognize common interference sources (Bluetooth, microwave, IoT) and recommend mitigation strategies.
106.0 Develop an awareness of wireless LAN technologies. The student will be able to:
106.01 Explain IEEE 802.11 a/b/g/n/ac/ax/be standards and their relative speeds, frequencies, and capabilities.
106.02 Describe authentication and association processes between clients and access points.
106.03 Define SSID, BSSID, ESS, and describe client roaming between access points.
106.04 Explain power management features and their impact on battery life and performance.
106.05 Differentiate between infrastructure, ad hoc, mesh, and cloud-managed WLAN architectures.

107.0	Perform implementation and management activities. The student will be able to:
	107.01 Determine where wireless LAN technology is suitable based on coverage and performance requirements.
	107.02 Install, configure, and manage wireless access points, controllers, and cloud-based WLAN systems.
	107.03 Configure and manage wireless LAN client devices and adapters.
	107.04 Install and secure wireless LAN gateways and bridges for inter-network connectivity.
	107.05 Identify antenna attributes such as gain, beamwidth, and polarization for proper deployment.
	107.06 Plan antenna placement and alignment for optimal coverage and minimal interference.
	107.07 Calculate free-space path loss and apply basic link-budget concepts.
	107.08 Identify and manage WLAN accessories (PoE injectors, cabling, mounting hardware).
	107.09 Diagnose and correct common WLAN challenges such as multipath, reflection, and absorption.
	107.10 Explain how antenna diversity and MIMO technologies improve reliability and throughput.
	107.11 Conduct a wireless site survey to assess coverage, capacity, and interference.
	107.12 Identify required tools and equipment for predictive and active RF site surveys.
	107.13 Perform site surveys and document findings with signal maps and heatmaps.
	107.14 Analyze results and provide site-survey reports with recommendations.
108.0	Develop an awareness of wireless security systems. The student will be able to:
	108.01 Compare wireless security protocols (WEP, WPA2, WPA3) and their relative strengths and weaknesses.
	108.02 Identify common WLAN security threats including rogue APs, Evil Twin, deauthentication, and packet sniffing attacks.
	108.03 Implement security features such as 802.1X authentication, RADIUS integration, and encryption.
	108.04 Apply corporate wireless security policies including password, encryption, and network segmentation standards.
	108.05 Use wireless analyzers to detect unauthorized devices and validate network compliance.
109.0	Demonstrate knowledge of wireless industry standards. The student will be able to:
	109.01 Differentiate between 2.4 GHz, 5 GHz, and 6 GHz frequency bands, including channel widths and limitations.
	109.02 Identify key industry organizations including IEEE, Wi-Fi Alliance, FCC, and IETF, and their roles in WLAN standardization.
	109.03 Explain the differences between ISM and UNII bands and their permitted applications.
	109.04 Describe power-output regulations and antenna-alignment requirements for point-to-point and point-to-multipoint links.

Course Number: EEV0317 **Occupational Completion Point: G** **Data Communications Analyst – 150 Hours**
110.0 Participate in simulated work-based learning experiences. The student will be able to:
110.01 Participate in simulated network support activities using help-desk or ticketing systems.
110.02 Use collaboration and documentation platforms to record network incidents and service tasks.
110.03 Demonstrate professional and supervisory skills appropriate for a network support environment.
111.0 Demonstrate a knowledge of general security concepts. The student will be able to:
111.01 Describe access-control models (MAC, DAC, RBAC, Zero Trust).
111.02 Explain authentication and authorization processes (MFA, SSO, identity providers).
111.03 Identify common cyberattacks (phishing, DDoS, spoofing, social engineering, insider threats).
111.04 Harden endpoints by disabling unused services and enforcing secure configuration baselines.
111.05 Recognize and mitigate malware types (viruses, worms, Trojans, ransomware).
111.06 Configure system auditing, logging, and vulnerability scanning to support incident response.
112.0 Develop an awareness of communication security concepts. The student will be able to:
112.01 Configure secure remote-access solutions (VPN, RADIUS, L2TP, SAML, ZTNA).
112.02 Identify email-security risks (spam, spoofing, malicious attachments) and apply mitigation techniques.
112.03 Explain web and application-security concepts (HTTPS, TLS certificates, content filtering).
112.04 Demonstrate secure file-transfer methods (SFTP, FTPS, encrypted cloud storage).
112.05 Describe wireless-security protocols (WPA3, 802.1X) and common vulnerabilities.
113.0 Develop an awareness of network infrastructure security. The student will be able to:
113.01 Install and configure firewalls and access-control lists to protect network segments.
113.02 Identify physical and signal security considerations for copper and fiber media.
113.03 Secure removable media and external devices through encryption and policy controls.
113.04 Describe secure network topologies (DMZ, security zones, NAT, micro-segmentation).
113.05 Deploy and monitor intrusion-detection and prevention systems (IDS/IPS).
113.06 Maintain security baselines through updates, patch management, and configuration control.
113.07 Configure Virtual Private Networks (VPNs) for secure remote connectivity.

	113.08 Explain the role of NAT, firewall rules, and routing policies in network security.
114.0	Develop an awareness of cryptography and its relation to security. The student will be able to:
	114.01 Explain modern encryption algorithms (AES, RSA, ECC) and hash functions (SHA-3).
	114.02 Use digital certificates and PKI to authenticate users and devices.
	114.03 Describe cryptographic standards and protocols used in secure commerce (SSL/TLS, tokenization, digital signatures).
115.0	Incorporate organizational and operational security in an appropriate and effective manner. The student will be able to:
	115.01 Develop and apply a network-security policy and incident-response procedures.
	115.02 Implement physical security controls (badges, locks, cameras, secure racks).
	115.03 Establish and test backup and disaster-recovery plans.
	115.04 Explain business-continuity principles and their relationship to network resilience.
	115.05 Describe acceptable-use, password, and remote-access policies within an organization.
	115.06 Apply privilege management and role-based access to systems and data.
	115.07 Describe digital-forensics concepts related to incident response and evidence handling.
	115.08 Promote security-awareness training for employees and supervisors.
	115.09 Document security standards, procedures, and change-management records.

Additional Information

Laboratory Activities

Laboratory investigations that include scientific inquiry, research, measurement, problem solving, emerging technologies, tools and equipment, as well as, experimental, quality, and safety procedures are an integral part of this career and technical program/course. Laboratory investigations benefit all students by developing an understanding of the complexity and ambiguity of empirical work, as well as the skills required to manage, operate, calibrate and troubleshoot equipment/tools used to make observations. Students understand measurement error; and have the skills to aggregate, interpret, and present the resulting data. Equipment and supplies should be provided to enhance hands-on experiences for students.

Career and Technical Student Organization (CTSO)

CTSOs are co-curricular career and technical student organizations providing leadership training and reinforcing specific career and technical skills. Career and Technical Student Organizations provide activities for students as an integral part of the instruction offered. Other CTSOs not listed in this curriculum framework or recognized by the Florida Department of Education are permissible provided they support student mastery over the standards and benchmarks of this curriculum framework.

Cooperative Training – OJT

On-the-job training is appropriate but not required for this program. Whenever offered, the rules, guidelines, and requirements specified in the OJT framework apply.

Basic Skills

In a Career Certificate Program offered for 450 hours or more, in accordance with Rule 6A-10.040, F.A.C., the minimum basic skills grade levels required for postsecondary adult career and technical students to complete this program are: Computation (Mathematics) and Communications (Reading and Language Arts). These grade level numbers correspond to a grade equivalent score obtained on a state designated basic skills examination.

Adult students with disabilities, as defined in Section 1004.02, Florida Statutes, may be exempted from meeting the Basic Skills requirements (Rule 6A-10.040). Students served in exceptional student education (except gifted) as defined in s. 1003.01, F.S., may also be exempted from meeting the Basic Skills requirement. Each school district and Florida College System Institution must adopt a policy addressing procedures for exempting eligible students with disabilities from the Basic Skills requirement as permitted in Section 1004.91, F.S.

Accommodations

Federal and state legislation requires the provision of accommodations for students with disabilities to meet individual needs and ensure equal access. Postsecondary students with disabilities must self-identify, present documentation, request accommodations if needed, and develop a plan with their counselor and/or instructors. Accommodations received in postsecondary education may differ from those received in secondary education. Accommodations change the way the student is instructed. Students with disabilities may need accommodations in such areas as

instructional methods and materials, assignments and assessments, time demands and schedules, learning environment, assistive technology and special communication systems. Documentation of the accommodations requested and provided should be maintained in a confidential file.

Note: postsecondary curriculum and regulated secondary programs cannot be modified.