INFORMATION TECHNOLOGY CAREER CLUSTER DESIGN

Network Systems Pathway

CIP CODE 11.0901

APPROVED PATHWAY:

1. Includes a minimum of three secondary-level credits.
2. Includes a work-based element.
3. Consist of a sequence:
   - Introductory-level course.
   - Technical-level course.
   - Application-level course.
4. Supporting documentation includes:
   - Articulation Agreement(s).
   - Certification.
   - Program Improvement Plan.
   - Program of Study.
5. Technical-level and Application-level courses receive.5 state weighted funding in an approved CTE pathway.

INTRODUCTORY LEVEL

Title	Code	Credit
Computing Systems	10002/60002	1
Computer Applications	10004/60004	1

TECHNICAL LEVEL

Title	Code	Credit
* Foundations of Information Technology	10001	1

APPLICATION LEVEL

Title	Code	Credit
CyberSecurity I	10020	1
# CyberSecurity II	10900	1
#Network Systems I	10112	1
#Network Systems II	10147	1
Work-based Learning in Network Systems	10148	1

* Required course for pathway approval.

# Has prerequisite course(s): Courses comprising a sequence are numbered consecutively. See Competency Profile for details.

Course	Foundations of Information Technology	Course #	10001	Credit	1.0
Pathways & CIP	Information Support & Services (11.0301); Network Systems (11.0901)				
Course Description:	Technical Level: a course intended to provide students with exposure to various information technology occupations and the information technology pathways available: Network Systems, Information Support and Services, and Programming and Software Development. Students will demonstrate core competencies in safety, electronics and basic digital theory, overview of the internet and operating systems, basic IT terminology and concepts, organization of data and materials, and basic programming. At the conclusion of the course, students should be prepared to make an informed decision about which Information Technology program(s) of study they would like to pursue in conjunction with their IPS.				

Directions: *The following competencies are required for full approval of this course. Check the appropriate number to indicate the level of competency reached for learner evaluation.*

Rating Scale:

4. Exemplary Achievement: Student possesses outstanding knowledge, skills, or professional attitude.

3. Proficient Achievement: Student demonstrates good knowledge, skills, or professional attitude. Requires limited supervision.

2. Limited Achievement: Student demonstrates fragmented knowledge, skills, or professional attitude. Requires close supervision.

1. Inadequate Achievement: Student lacks knowledge, skills, or professional attitude.

0. No Instruction / Training: Student has not received instruction or training in this area.

Student: ______________________________

Graduation Date: ______________________________

I certify that the student has received training in the areas indicated.

Instructor Signature: ______________________________

Benchmark 1.0: Knowledge of Equipment & lab safety standards.

	Competencies					
1.1	Accurately read, interpret, and demonstrate adherence to safety rules, including Internet safety, Occupational Safety and Health Administration (OSHA) guidelines, and state and national code requirements. Be able to distinguish between rules and explain why certain rules apply.	4	3	2	1	0
1.2	Identify and explain the intended use of safety equipment available in the classroom. Demonstrate how to properly inspect, use, and maintain safe operating procedures with tools and equipment.	4	3	2	1	0

Benchmark 2.0: Working knowledge of basic computer components and the digital theory behind their operation.

	Competencies					
2.1	Demonstrate understanding of electrical circuits and devices, and relate to the physical laws (such as Ohm’s Law and power laws) that govern behaviors of electrical circuits and devices. Accurately apply these physical laws to solve problems. For example, calculate the resistance of a DC circuit with a given DC voltage and current.	4	3	2	1	0

2.2	Assemble the required connections of electronic test equipment to properly test the operation of basic electronic circuit behavior and performance, using equipment such as a digital multimeter. For example, demonstrate the proper use of a digital multimeter by measuring resistance of a circuit in a typical computer system; compare this finding by calculating the resistance given the voltage and current.	4	3	2	1	0
2.3	Distinguish between the binary and hexadecimal counting systems. Using appropriate units, provide examples of each system and identify specific instances when IT professionals rely on them.	4	3	2	1	0
2.4	Explain the functions of gates in logic circuits (e.g., AND, OR, NOT).	4	3	2	1	0
Benchmark 3.0: Career Awareness in Information Technology						
	Competencies					
3.1	Research various occupations in information technology industries, such as programmers, web designers, webmasters, networking administrators, computer systems administrators, telecommunications line installers, and informational security analysts.	4	3	2	1	0
3.2	Explore various professional societies related to information technology and identify the services and benefits provided by each member.	4	3	2	1	0
Benchmark 4.0: Understanding of the history behind the internet and operating systems.						
	Competencies					
4.1	Drawing on multiple sources, research the history of the Internet. Discuss both the benefits and disadvantages of the Internet to society, as well as potential implications for the future.	4	3	2	1	0
4.2	Drawing on multiple sources (i.e., internet, textbooks, videos, and journals), research the history and development of operating systems (e.g., Microsoft Windows, Linux, UNIX).	4	3	2	1	0
Benchmark 5.0: Working knowledge of Information Technology terminology and related concepts.						
	Competencies					
5.1	Demonstrate an understanding of basic web terminology and concepts. Practice explaining these terminologies and concepts by creating methods to help students learn and remember the information.	4	3	2	1	0
5.2	Demonstrate a basic understanding of computer hardware components. Identify these components using pictures or actual models and briefly explain the function of each. Components should include, but are not limited to: a. Hardware used for input and output, b. Hardware inside the computer case, c. Motherboard, d. Processor and the chipset, e. Storage devices (e.g., primary, secondary), f. Expansion cards, and g. Electrical system.	4	3	2	1	0
5.3	Demonstrate a basic understanding of computer networking. For example, explain the types of networks and what a client-server environment is.	4	3	2	1	0

Benchmark 6.0: Understand the importance of proper organization of materials in Information Technology.						
	Competencies					
6.1	Understand and demonstrate the effective use of file and folder management techniques to maintain directory structure for a web site. Describe the most efficient methods for digital file management, including the use of site root and subfolders for assets (e.g. images, templates, CSS).	4	3	2	1	0
Benchmark 7.0: Working knowledge of programming languages, their development, and various implementations						
	Competencies					
7.1	Explore and identify various languages, such as Python, HTML, PHP, C++, Visual Basic, Java, JavaScript, and C #. Explain how programmers use these languages to solve a variety of IT problems, furnishing examples of how they are applied.	4	3	2	1	0
7.2	Using various resources, research, identify, and explain the steps involved in the software development life cycle, including but not limited to: planning, designing, coding, testing, deployment, and maintenance. Explain why it is an iterative process and always involves refinement.	4	3	2	1	0
7.3	Demonstrate an understanding of how batch files function within a programming environment. Identify common commands to create code for batch files (e.g. title, echo, echo off, pause, CLS, ipconfig, and ping).	4	3	2	1	0

Information Technology

Course:	Network Systems I	**Course #:**	TBD	**Credit:**	1.0
Pathways & CIP Codes:	Network Systems (11.0901)				
Course Description:	**Technical Level:** a course designed for students who have chosen to pursue a Network Systems program of study to introduce the basic conceptual and practical skills necessary to identify, install, and manage relevant hardware and software in network systems. ****Prerequisite Network Systems I or demonstration of all competencies therein**				

Directions: *The following competencies are required for full approval of this course. Check the appropriate number to indicate the level of competency reached for learner evaluation.*

Rating Scale:

4. Exemplary Achievement: Student possesses outstanding knowledge, skills, or professional attitude.
3. Proficient Achievement: Student demonstrates good knowledge, skills, or professional attitude. Requires limited supervision.
2. Limited Achievement: Student demonstrates fragmented knowledge, skills, or professional attitude. Requires close supervision.
1. Inadequate Achievement: Student lacks knowledge, skills, or professional attitude.
0. No Instruction / Training: Student has not received instruction or training in this area.

Student: ____

Graduation Date: ____

I certify that the student has received training in the areas indicated.

Instructor Signature: _____________________________________

Sample Indicators for LEAs can be found at (link to resource document)

Benchmark 1.0: Foundations						
	Competencies					
1.1	Demonstrate knowledge of the history and general characteristics of network operating systems including basic network terminology.	4	3	2	1	0
1.2	Identify the basic components of a network operating system and the basic point-to-point network topologies (e.g., star, mesh, bus, ring, hybrid).	4	3	2	1	0
1.3	Identify and demonstrate an understanding of the different types of networks (e.g. LAN, MAN, WAN, VPN, EPN, SAN, PAN).	4	3	2	1	0
1.4	Demonstrate knowledge of the principles and operation of wire (coaxial, fiber optics, etc.), analog and digital circuits, and wireless systems.	4	3	2	1	0

Benchmark 2.0: Network Operating Systems and Open Systems Interconnection (OSI)						
	Competencies					
2.1	Explain the Open Systems Interconnection (OSI) Model and the flow of data through it, define the functions, and identify	4	3	2	1	0

	the associated hardware components.					
2.2	Identify the basic functions of a network operating system (NOS), research various types (e.g. Microsoft Windows server, Linux enterprise server, UNIX, etc.), and synthesize findings to demonstrate knowledge that includes, but is not limited to: a. Optimal software requirements b. Client support features c. Organization of network elements d. Sharing applications e. Managing system resources (e.g., memory, multitasking, multiprocessing) f. The importance of considering future needs	4	3	2	1	0

Benchmark 3.0: Network Hardware and Installation						
	Competencies					
3.1	Identify basic network hardware (e.g. routers, switches) and demonstrate knowledge of their components, architecture, and function.	4	3	2	1	0
3.2	Configure and install a basic network (wired or wireless) using available materials, hardware, and software.	4	3	2	1	0

Benchmark 4.0: Security Risks and Troubleshooting						
	Competencies					
4.1	Research and describe the most common network security risks associated with: people; data transmission and hardware; protocols and software; and internet access. Investigate and distinguish among the following common prevention methods to secure a network system. a. Physical security b. Security in network design c. Network operating system security d. Encryption e. Authentication protocols f. Wireless network security Synthesize findings to identify security requirements for the installed network and develop a security plan that demonstrates knowledge of basic security software (e.g. firewalls, intrusion detection systems, etc.) and the roles both software and hardware play in network security.	4	3	2	1	0
4.2	Demonstrate knowledge of basic troubleshooting theory using appropriate hardware and software (e.g. cable tester, butt set, multimeter, protocol analyzer, throughput testers, connectivity software, etc.).	4	3	2	1	0
4.3	Identify and demonstrate knowledge of most common network problems including but not limited to: a. Wireless problems (e.g., interference, signal strength, configurations, latency) b. Router and switch problems (e.g., switching loop, bad cables, port configuration)	4	3	2	1	0

	c. Physical connectivity problems (e.g., connectors, wiring, split cables, cable placement)					
4.4	Demonstrate the application of troubleshooting theory in various network system problems. For each network system problem given, students should model the following, including but not limited to: a. Gather information from users or the system, back up data, and document findings b. Verify the problem exists and how many users are affected c. Isolate the cause of the problem and generate alternative solutions d. Determine whether escalation is necessary e. Plan a solution and resolve the problem Upon verification the problem was resolved, students should document findings (including an explanation of the common symptoms, diagnostic procedures, and specific tools used that led to the resolution) and develop a preventative maintenance plan.	4	3	2	1	0

Course:	Network Systems II	**Course #:**	TBD	**Credit:**	1.0
Pathways & CIP Codes:	Information Support and Services (11.0901)				
Course Description:	**Technical Level:** a course designed for students who have chosen to pursue a Network Systems program of study to emphasize more advanced conceptual and practical skills necessary to identify, install, and manage relevant hardware and software in network systems. This should be a dual enrollment course with the student completing post-secondary credit hours in the Computer Support Specialist certification track (KBOR). Students should be completing preparatory competencies toward successful completion of the CompTIA Network+ or CompTIA A+ exams and attainment of certification. ****Prerequisites Network Systems I and Network Systems II or demonstration of all competencies therein**				

Directions: *The following competencies are required for full approval of this course. Check the appropriate number to indicate the level of competency reached for learner evaluation.*

Rating Scale:

4. Exemplary Achievement: Student possesses outstanding knowledge, skills, or professional attitude.
3. Proficient Achievement: Student demonstrates good knowledge, skills, or professional attitude. Requires limited supervision.
2. Limited Achievement: Student demonstrates fragmented knowledge, skills, or professional attitude. Requires close supervision.
1. Inadequate Achievement: Student lacks knowledge, skills, or professional attitude.
0. No Instruction / Training: Student has not received instruction or training in this area.

Student: ____

Graduation Date: ____

I certify that the student has received training in the areas indicated.

Instructor Signature: ____________________________________

Sample Indicators for LEAs can be found at (link to resource document)

Benchmark 1.0: CompTIA Network+						
	Competencies					
1.1	Design and implement functional networks.	4	3	2	1	0
1.2	Configure, manage, and maintain essential network devices.	4	3	2	1	0
1.3	Use devices such as switches and routers to segment network traffic and create resilient networks.	4	3	2	1	0
1.4	Identify benefits and drawbacks of existing network configurations.	4	3	2	1	0
1.5	Implement network security, standards and protocols.	4	3	2	1	0
1.6	Troubleshoot network problems.	4	3	2	1	0
1.7	Support the creation of virtualized networks.	4	3	2	1	0

Benchmark 2.0: CompTIA A+						
	Competencies					
2.1	Configure, install and upgrade operating systems, including: Windows, Apple OS X, Linux, iOS, Android and Windows Mobile.	4	3	2	1	0
2.2	Install and image virtual machines.	4	3	2	1	0
2.3	Set up and troubleshoot peripheral devices.	4	3	2	1	0
2.4	Assemble and disassemble computing hardware.	4	3	2	1	0
2.5	Set up and support basic home and small office networks.	4	3	2	1	0
2.6	Implement cybersecurity controls appropriate to helpdesk and technical support roles.	4	3	2	1	0
2.7	Troubleshoot and support end-user access to applications and data.	4	3	2	1	0

Course:	Cybersecurity I	**Course #:**	TBD	**Credit**:	1.0
Pathways & CIP Codes:	Programming and Software Development (11.0201); Network Systems (11.0901); Information Support and Services (11.0301)				
Course Description:	Application Level: a course intended to teach students the basic concepts of cybersecurity. The course places an emphasis on security integration, application of cybersecurity practices and devices, ethics, and best practices management. The fundamental skills in this course cover both in-house and external threats to network security and design, how to enforce network level security policies, and how to safeguard an organization's information. This should be a dual enrollment course with the student completing post-secondary credit hours in the Computer Support Specialist certification track (KBOR). Students should be completing preparatory competencies toward successful completion of the CompTIA Security+ exam and attainment of certification.				

Directions: *The following competencies are required for full approval of this course. Check the appropriate number to indicate the level of competency reached for learner evaluation.*

Rating Scale:

4. Exemplary Achievement: Student possesses outstanding knowledge, skills, or professional attitude.
3. Proficient Achievement: Student demonstrates good knowledge, skills, or professional attitude. Requires limited supervision.
2. Limited Achievement: Student demonstrates fragmented knowledge, skills, or professional attitude. Requires close supervision.
1. Inadequate Achievement: Student lacks knowledge, skills, or professional attitude.
0. No Instruction / Training: Student has not received instruction or training in this area.

Student: ______________________________________

Graduation Date: ______________________________________

I certify that the student has received training in the areas indicated.

Instructor Signature: ______________________________________

Sample Indicators for LEAs can be found at (link to resource document)

Benchmark 1.0: Foundations						
	Competencies					
1.1	Analyze ethical security practices, including but not limited to the issues of data security, confidentiality, integrity, availability, authentication, nonrepudiation, physical security, HIPPA Laws, Payment Card Industry (PCI) Compliance, and the importance of ISO27000 standards.	4	3	2	1	0
1.2	Analyze security threats, vulnerabilities, and exploits. Research common ways that threats, vulnerabilities, and exploits impact an organization.	4	3	2	1	0
1.3	Preform a simulated risk assessment by using the common industry framework from ISO. Analyze and describe the risk mitigation techniques of acceptance, mitigation, avoidance, and transfer.	4	3	2	1	0

1.4	Explain the core concepts of access control as they relate to authentication and authorization and describe the core principles of access controls.	4	3	2	1	0
1.5	Research and describe the most common various methods and technology used to secure networks. Investigate and distinguish among the following common methods to secure a network. This can include but is not limited to: a. VPNs for remote access b. Firewalls c. Perimeter network designs d. Preventative technologies	4	3	2	1	0

Benchmark 2.0: Threats and Security						
	Competencies					
2.1	Research and describe the most common security threats to computer systems, such as social engineering, malware, phishing, viruses, etc. Investigate and distinguish among the following common prevention methods to secure a computer system. For a given scenario, identify the most applicable best practice to secure a workstation as well as describe methods for data destruction and disposal. Implement these practices and write a justification for each scenario solution. Provide supporting evidence for each solution, drawing on technical texts and industry standards. Prevention methods include but are not limited to: a. Physical security (e.g., lock doors, tailgating, biometrics, badges, key fobs, retinal, etc.) b. Digital security (e.g., antivirus, firewalls, antispyware, user authentication, etc.) c. User education d. Principles of least privilege	4	3	2	1	0
2.2	Differentiate between threats and vulnerabilities and what constitutes a network attack and identify how to differentiate between the different types of application attacks.	4	3	2	1	0
2.3	Identify and describe the differences among various methods to create baseline security measures. Utilizing existing tools on a system, such as the Microsoft Baseline Security Analyzer, outline the steps taken to create a security measure.	4	3	2	1	0
2.4	Demonstrate the methods used to protect against unauthorized use of files. Configure file and folder permissions using both Windows and Linux environments.	4	3	2	1	0
2.5	Analyze common methods and use of cryptology to protect data. Compare and contrast general methods used, and explain how their designs and functionalities support the security of data.	4	3	2	1	0

Benchmark 3.0: CompTIA Security+						
	Competencies					
3.1	Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.	4	3	2	1	0
3.2	Monitor and secure hybrid environments, including cloud, mobile, and IoT.	4	3	2	1	0
3.3	Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance.	4	3	2	1	0
3.4	Identify, analyze, and respond to security events and incidents.	4	3	2	1	0

Information Technology

Course:	Cybersecurity II	**Course #:**	TBD	**Credit**:	1.0
Pathways & CIP Codes:	Programming and Software Development (11.0201); Network Systems (11.0901); Information Support and Services (11.0301)				
Course Description:	**Application Level:** a course that challenges students to develop advanced skills in concepts and terminology of cybersecurity. This course builds on previous concepts introduced in Cybersecurity I while expanding the content to include malware threats, cryptography, wireless technologies and organizational security. This should be a dual enrollment course with the student completing post-secondary credit hours in the Computer Support Specialist certification track (KBOR). Students should be completing preparatory competencies toward successful completion of the CompTIA Security+ exam and attainment of certification. ****Prerequisite Cybersecurity I or demonstration of all competencies therein**				

Directions: *The following competencies are required for full approval of this course. Check the appropriate number to indicate the level of competency reached for learner evaluation.*

Rating Scale:
4. Exemplary Achievement: Student possesses outstanding knowledge, skills, or professional attitude.
3. Proficient Achievement: Student demonstrates good knowledge, skills, or professional attitude. Requires limited supervision.
2. Limited Achievement: Student demonstrates fragmented knowledge, skills, or professional attitude. Requires close supervision.
1. Inadequate Achievement: Student lacks knowledge, skills, or professional attitude.
0. No Instruction / Training: Student has not received instruction or training in this area.

Student: ____

Graduation Date: ______________________________________

I certify that the student has received training in the areas indicated.

Instructor Signature: ___________________________________

Sample Indicators for LEAs can be found at (link to resource document)

Benchmark 1.0: Malware and Attack Types						
	Competencies					
1.1	Conduct research to determine various forms of malware and analyze methods to handle malware, such as how to control access to secured resources and computer resources.	4	3	2	1	0
1.2	Analyze and differentiate among various types of attacks on systems and networks. Different types of attacks can include but are not limited to: a. Virus b. Worms c. Trojans d. Unpatched software e. Password cracking f. Advanced persistent threat	4	3	2	1	0

	g. Reconnaissance/footprinting h. Infiltration i. Network breach j. Network exploitation k. Attack for effects (e.g., deceive, disrupt, degrade, and destroy) l. DoS/DDoS, session hijacking m. HTTP spoofing n. DNS attacks o. Switch attacks p. Man-in-the-middle (MITM) attacks q. Cross site scripting r. Drive-by-attack					

Benchmark 2.0: Cryptography						
	Competencies					
2.1	Analyze cryptographic tools, procedures for use, and products including but not limited to: PKI, Certificates, PGP, and Certificate authorities.	4	3	2	1	0

Benchmark 3.0: Security Protocols and Security Awareness						
	Competencies					
3.1	Analyze attack methods on wireless networks and demonstrate the use of wireless security protocols. Evaluate the capabilities of WPA, WPA-2, and WEP and the effectiveness of the security protocols and demonstrate how to use them appropriately.	4	3	2	1	0
3.2	Research and analyze security awareness in an organization. Demonstrate knowledge of the mitigation of the following, including but not limited to: a. Security policy training and procedures b. Personally identifiable information c. Information classifications d. Data labeling, handling, and disposal e. Compliance with laws, best practices, and standards f. User habits g. Threat awareness h. Use of social networking	4	3	2	1	0
3.3	Analyze and define the impact of security incidents on an organization. Define what a disaster recovery (DR) plan is and how to develop one.	4	3	2	1	0
3.4	Explore and identify various assessment methods including but not limited to network penetration and vulnerability	4	3	2	1	0

	testing.					
3.5	Identify and explain the uses for security testing tools. Demonstrate and compare the effectiveness of Nessus and Nmap.	4	3	2	1	0
3.6	Demonstrate each of the following concepts: a. Evaluate the patch status of a machine b. Demonstrate knowledge of packet-level analysis in order to install and view packets c. Perform secure data destruction (e.g., Secure Erase, BCWipe)					
3.7	Utilizing prior fundamentals, demonstrate proper secure network configuration and administration. Use common tools and design a network utilizing secure protocols, and evaluate the network upon completion. The plan should address, but is not limited, to the following: a. Applying and implementing secure network administration principles b. Demonstrating knowledge of how network services and protocols interact to provide network communications in order to securely implement and use common protocols c. Identifying commonly used default network ports d. Setting up a Network Address Translation (NAT) device e. Configuring a Virtual Private Network (VPN) f. Configuring a remote access policy Layer 2 Tunneling Protocol (L2TP) and Point-toPoint Tunneling Protocol (PPTP) g. Demonstrating knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol (TCP/IP), Dynamic Host Configuration Protocol (DHCP) and directory services (e.g., Domain Name System (DNS) by setting up common protocols, e.g., Secure Shell (SSH), netstat, Simple Mail Transfer Protocol (SMTP), nslookup, Telnet, DNS/Bind, FTP, IIS/Web Pages, DHCP/DNS server h. Locating open ports by completing a port scan i. Demonstrating the knowledge and use of network statistics (netstat)					

Benchmark 4.0: CompTIA Security+						
	Competencies					
4.1	Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions	4	3	2	1	0
4.2	Monitor and secure hybrid environments, including cloud, mobile, and IoT					
4.3	Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance					
4.4	Identify, analyze, and respond to security events and incidents					

Information Technology

Course:	Work-Based Learning Experience in Network Systems	**Course #:**	TBD	**Credit:**	1.0
Pathways & CIP Codes:	Network Systems (11.0901)				
Course Description:	**Application Level:** a capstone course intended to provide students with opportunities to apply the skills and knowledge learned in previous CTE and general education courses within a professional work environment. The course allows students to earn high school credit for select models of work-based learning, which allow students to interact with industry professionals in order to extend and deepen classroom work and support the development of postsecondary and career readiness knowledge and skills. Competencies during the experience, verified by the WBL coordinator or district representative, should continue to align with attainment of appropriate CompTIA certification(s).				

Directions: *The following competencies are required for full approval of this course. Check the appropriate number to indicate the level of competency reached for learner evaluation.*

Rating Scale:

4. Exemplary Achievement: Student possesses outstanding knowledge, skills, or professional attitude.
3. Proficient Achievement: Student demonstrates good knowledge, skills, or professional attitude. Requires limited supervision.
2. Limited Achievement: Student demonstrates fragmented knowledge, skills, or professional attitude. Requires close supervision.
1. Inadequate Achievement: Student lacks knowledge, skills, or professional attitude.
0. No Instruction / Training: Student has not received instruction or training in this area.

Student: ____

Graduation Date: ______________________________________

I certify that the student has received training in the areas indicated.

Instructor Signature: ___________________________________

Sample Indicators for LEAs can be found at (link to resource document)

Benchmark 1.0: Employability Skills						
	Competencies					
1.1	Understand and demonstrate all appropriate work-based personal and professional expectations, including but not limited to: a. Demonstrate information literacy b. Use technology effectively and appropriately c. Communicate clearly and effectively, verbally and in writing d. Demonstrate critical thinking and problem solving e. Collaborate and work productively as a team member f. Demonstrate creativity and innovation g. Demonstrate initiative and self-direction	4	3	2	1	0

	h. Demonstrate professionalism and ethical behavior i. Demonstrate appropriate interpersonal and social skills j. Demonstrate adaptability and flexibility k. Demonstrate productivity and accountability					
1.2	Understand and demonstrate adherence to appropriate professional safety standards.	4	3	2	1	0
1.3	Plan and navigate education and career paths aligned with personal goals.	4	3	2	1	0
1.4	Develop and implement a personalized learning plan (e.g. within the IPS) and reflect on experiences with an electronic, exportable portfolio.	4	3	2	1	0

Benchmark 2.0: CompTIA Network+						
	Competencies					
2.1	Design and implement functional networks.	4	3	2	1	0
2.2	Configure, manage, and maintain essential network devices.	4	3	2	1	0
2.3	Use devices such as switches and routers to segment network traffic and create resilient networks.	4	3	2	1	0
2.4	Identify benefits and drawbacks of existing network configurations.	4	3	2	1	0
2.5	Implement network security, standards and protocols.	4	3	2	1	0
2.6	Troubleshoot network problems.	4	3	2	1	0
2.7	Support the creation of virtualized networks.	4	3	2	1	0

Benchmark 3.0: CompTIA A+						
	Competencies					
3.1	Configure, install and upgrade operating systems, including: Windows, Apple OS X, Linux, iOS, Android and Windows Mobile.	4	3	2	1	0
3.2	Install and image virtual machines.	4	3	2	1	0
3.3	Set up and troubleshoot peripheral devices.	4	3	2	1	0
3.4	Assemble and disassemble computing hardware.	4	3	2	1	0
3.5	Set up and support basic home and small office networks.	4	3	2	1	0
3.6	Implement cybersecurity controls appropriate to helpdesk and technical support roles.					
3.7	Troubleshoot and support end-user access to applications and data.					

Benchmark 4.0:						
	Competencies					
4.1	Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.	4	3	2	1	0
4.2	Monitor and secure hybrid environments, including cloud, mobile, and IoT.	4	3	2	1	0

4.3	Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance.	4	3	2	1	0
4.4	Identify, analyze, and respond to security events and incidents	4	3	2	1	0