INFORMATION TECHNOLOGY CAREER CLUSTER DESIGN

Programming and Software Development Pathway

CIP CODE 11.0201

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
Introduction to Computer Coding	31001	0.5
Introduction to Physical Computing	31002	0.5

TECHNICAL LEVEL

Title	Code	Credit
Technical Introduction to Computer Science	41010	1
Computer Programming	10152	1
Database Applications	10053	1
Web Page Design	10201	1
Data System/Processing	10054	1
Computer Programming Other Language	10156	1
AP Computer Science Principles	31904	1

APPLICATION LEVEL

Title	Code	Credit
CyberSecurity I	10020	1
# CyberSecurity II	10900	1
AP Computer Science A	10157	1
IB Computing	10159	1
Particular Topics in Computer Programming	10160	1
Work-based Learning in Programming and Software Development	10198	1

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

Information Technology

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 Programming and Software Development	**Course #:**	TBD	**Credit**:	1.0
Pathways & CIP Codes:	Programming and Software Development (11.0201)				
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.				

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: Employablity 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 h. Demonstrate professionalism and ethical behavior	4	3	2	1	0

	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