# Cybersecurity I Course No. 10020 Credit: 1.0

|  |  |  |  |
| --- | --- | --- | --- |
| **Student name:**  |  | **Graduation Date:** |  |

Pathways and CIP Codes:Programming & Software Development (11.0201); Network Systems (11.0901); Information Support & Services (114.0301)

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.

## Benchmark 1: Foundations

### Competencies

| **#** | **DESCRIPTION** | **RATING** |
| --- | --- | --- |
| 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. |  |
| 1.2 | Analyze security threats, vulnerabilities, and exploits. Research common ways that threats, vulnerabilities, and exploits impact an organization. |  |
| 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. |  |
| 1.4 | Explain the core concepts of access control as they relate to authentication and authorization and describe the core principles of access controls. |  |
| 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, and d. Preventative technologies. |  |

## Benchmark 2: Click or tap here to enter text.

### Competencies

| **#** | **DESCRIPTION** | **RATING** |
| --- | --- | --- |
| 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, and d. Principles of least privilege. |  |
| 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. |  |
| 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. |  |
| 2.4 | Demonstrate the methods used to protect against unauthorized use of files. Configure file and folder permissions using both Windows and Linux environments. |  |
| 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. |  |

## Benchmark 3: Click or tap here to enter text.

### Competencies

| **#** | **DESCRIPTION** | **RATING** |
| --- | --- | --- |
| 3.1 | Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions. |  |
| 3.2 | Monitor and secure hybrid environments, including cloud, mobile, and IoT. |  |
| 3.3 | Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance. |  |
| 3.4 | Identify, analyze, and respond to security events and incidents. |  |

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

Instructor Signature:

For more information, contact:

CTE Pathways Help Desk

(785) 296-4908

pathwayshelpdesk@ksde.org



900 S.W. Jackson Street, Suite 102

Topeka, Kansas 66612-1212

[https://www.ksde.org](https://www.ksde.org/)

The Kansas State Department of Education does not discriminate on the basis of race, color, national origin, sex, disability or age in its programs and activities and provides equal access to any group officially affiliated with the Boy Scouts of America and other designated youth groups. The following person has been designated to handle inquiries regarding the nondiscrimination policies: KSDE General Counsel, Office of General Counsel, KSDE, Landon State Office Building, 900 S.W. Jackson, Suite 102, Topeka, KS 66612, (785) 296-3201.