Western Technical College

10151100 Introduction to Cybersecurity

Course Outcome Summary

Course Information

Description	Introduction to Cybersecurity explores the field of cybersecurity, specifically the importance of cybersecurity, data confidentiality, best practices for using the internet and social media safely, and potential career opportunities in this growing field.
Career Cluster	Law, Public Safety, Corrections and Security
Instructional Level	Associate Degree Courses
Total Credits	1
Total Hours	18

Textbooks

No textbook required.

Course Competencies

1. Explore the role of information assurance and data integrity.

Assessment Strategies

1.1. Written Product

Criteria

You will know you are successful when

1.1. you describe legal issues in cybersecurity.
1.2. you describe ethical issues in cybersecurity.
1.3. you evaluate cybersecurity jobs

Learning Objectives

1.a. Explain the value of personal and organizational data
1.b. Differentiate between personal and corporate cybersecurity laws
1.c. Characterize ethical and unethical behavior
1.d. Review cybersecurity job titles and requirements for specialized skills certifications

2. Describe the threat landscape.

Assessment Strategies

2.1. Written Product

Criteria

You will know you are successful when

2.1. you describe the impact of sensitive data exposure.
2.2. you describe how data is accessed illegally.
2.3. you describe the consequences of a security breach.

Learning Objectives

2.a. Summarize how multiple techniques are used to compromise a target
2.b. Identify what causes and facilitates data breaches

3. Examine cyber attack concepts and techniques.

Assessment Strategies

3.1. Written Product

Criteria

You will know you are successful when

3.1. you evaluate system vulnerabilities and exploits.
3.2. you describe types of malware and symptoms.
3.3. you describe methods of infiltration.

Learning Objectives

3.a. Categorize security vulnerabilities
3.b. Identify vulnerability terminology
3.c. Identify malware types and their symptoms
3.d. Characterize infiltration methods

4. Analyze the technologies used to reduce risk and protect data.

Assessment Strategies

4.1. Written Product

Criteria

You will know you are successful when

4.1. you identify malware and firewall tools.
4.2. you create a defense strategy to monitor and protect data.
4.3. you implement virus and malware protection tools.
4.4. you implement strong authentication methods.

Learning Objectives

4.a. Summarize techniques used to protect devices and networks
4.b. Review technologies used to maintain data integrity
4.c. Evaluate authentication and its role in safeguarding online privacy