ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 2204 Security+

Date: Fall 2021

Credit Hours: 3

Prerequisite(s): CSN 1225

Delivery Method:	☒ **Lecture**	**2 Contact Hours (1 contact = 1 credit hour)**
	☐ **Seminar**	**0 Contact Hours (1 contact = 1 credit hour)**
	☒ **Lab**	**2 Contact Hours (2-3 contact = 1 credit hour)**
	☐ **Clinical**	**0 Contact Hours (3 contact = 1 credit hour)**
	☒ **Online**	
	☐ **Blended**	
	☒ **VCM**	

Offered: ☒ **Fall** ☐ **Spring** ☐ **Summer**

CATALOG DESCRIPTION and IAI NUMBER (if applicable):
This course focuses on CompTIA's Security+ Certification exam. Currently the SY0-601 exam consists of six domains: Threats, Attacks and Vulnerabilities; Architecture and Design; Implementation; Operations and Incident Response; and Governance, Risk, and Compliance. This course is designed to provide you with the foundational knowledge necessary to prepare you to sit for the Security+ certification exam.

ACCREDITATION STATEMENTS AND COURSE NOTES:

None

COURSE TOPICS AND CONTENT REQUIREMENTS:

1. Threats and Threat Intelligence
2. Risk Management
3. Security Assessments
4. Malware
5. Cryptography
6. Access Control Management
7. Secure Network Design
8. Endpoint Security
9. Secure Applications
10. Secure Mobile
11. Cloud
12. Incident Response

INSTRUCTIONAL METHODS:

1. Lecture
2. Discussion
3. Video
4. Readings
5. Case Studies
6. CompTIA's CertMaster Learn & Labs

EVALUATION OF STUDENT ACHIEVEMENT:

Students must:

1. Participate in class discussions or demonstrate by work completed the recorded videos of class were reviewed
2. Complete readings, assignments, quizzes, exams, hands-on CompTIA labs, and other assignments given at the instructor's discretion
3. Ask questions about any misunderstood area either in class, during office hours, or of the tutor.

A = 90 – 100
B = 80 – 89
C = 70 – 79
D = 60 – 69
F = 0 – 59

INSTRUCTIONAL MATERIALS:

Textbooks

Textbooks used in Security+ are at the discretion of full-time faculty.
Part-time faculty members are to use the textbook designated for Security+ by the Program Coordinator for Cybersecurity and the Dean of Workforce Development.

Resources

- CertMaster Learn and CertMaster Labs for Security+
- Case Studies

Computer Applications:

1. Word Processing software
2. Web Browser:
    a. CompTIA sites
3. Online Course Management Software
4. IVCC email account

Other:

1. Audio/video resources

LEARNING OUTCOMES AND GOALS:

Institutional Learning Outcomes

☐ ILO 1: Communication – to communicate effectively;

☒ ILO 2: Inquiry – to apply critical, logical, creative, aesthetic, or quantitative analytical reasoning to formulate a judgement or conclusion;

☐ ILO 3: Social Consciousness – to understand what it means to be a socially conscious person, locally and globally;

☐ ILO 4: Responsibility – to recognize how personal choices affect self and society.

Course Outcomes and Competencies

Outcome 1: Understand the different types of threats, attacks, and vulnerabilities
Competency 1.1: Discuss the different forms of malware
Competency 1.2: Understand the different types of attacks
Competency 1.3: Understand the benefits of vulnerability scanning

Outcome 2: Describe the various technologies and tools used with Security
Competency 2.1: Discuss the basic security components
Competency 2.2: Use Command Line and Software Security tools
Competency 2.3: Analyze Security output

Outcome 3: Explain the frameworks used in Security Architecture and Design.
Competency 3.1: Explain Defense in Depth
Competency 3.2: Describe Secure Network Topologies
Competency 3.3: Understand Cloud Technologies and virtualization
Competency 3.4: Understand redundancy, fault tolerance and high availability

Outcome 4: Understand Identity and Access Management
Competency 4.1: Discuss Access Control and Access Management
Competency 4.2: Understand Account Management

Outcome 5: Identify the components in a Risk Management Plan
Competency 5.1: Assess Security Policies
Competency 5.2: Perform a Business Impact Analysis
Competency 5.3: Understand the Risk Management Process

Outcome 6: Explain Cryptography and PKI
Competency 6.1: Explain the difference between weak and Strong Cryptography
Competency 6.2: Understand Algorithms
Competency 6.3: Understand Wireless Security Protocols
Competency 6.4: Understand the components and concepts of PKI Infrastructures