ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 1201 Managing Information Security

Date: Fall 2021

Credit Hours: 3

Prerequisite/Co-requisite(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):
Organizations must be able to apply effective strategies to secure their networks and keep personnel and customer data safe and secure. This course covers the key principles and practices of information security. The course discusses topics such as threats, vulnerabilities, countermeasures, risk management, compliance, cybersecurity frameworks, disaster recovery, incident response and business continuity.

ACCREDITATION STATEMENTS AND COURSE NOTES:
None

COURSE TOPICS AND CONTENT REQUIREMENTS:
1. Risk Management
    a. Risk Assessments
    b. Threats / Vulnerabilities
    c. Countermeasures
2. Compliance
3. Cybersecurity Frameworks
4. Disaster Recovery
5. Incident Response
6. Business Continuity

INSTRUCTIONAL METHODS:
1. Lecture
2. Discussion
3. Group Work
4. Readings
5. Case Studies
6. Student Presentations

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, presentations, 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 Managing Information Security are at the discretion of full-time faculty.
Part-time faculty members are to use the textbook designated for Managing Information Security by the Program Coordinator for Cybersecurity and the Dean of Workforce Development.

Resources
Case Study from "*Information Security Management Principles," 3rd Edition*, supported by the BCS, The Chartered Institute for IT.

Computer Applications:
1. Word Processing software
2. Spreadsheet software
3. Presentation software
4. Online course management system
5. IVCC Email

Other:
1. Audio/video resources
2. Online resources

LEARNING OUTCOMES AND GOALS:

Institutional Learning Outcomes

☒ Communication – to communicate effectively;
☒ Inquiry – to apply critical, logical, creative, aesthetic, or quantitative analytical reasoning to formulate a judgement or conclusion;
☐ Social Consciousness – to understand what it means to be a socially conscious person, locally and globally;
☐ Responsibility – to recognize how personal choices affect self and society.

Course Outcomes and Competencies

Outcome 1: Discuss the key principles and practices of Information Security
Competency 1.1: Understand access controls
Competency 1.2: Explain the pillars of security and security concepts
Competency 1.3: Understand the role of an Information Systems Management strategy

Outcome 2: Identify application security strategies
Competency 2.1: Understand protection methodologies within application security

Outcome 3: Understand network security
Competency 3.1: Discuss firewalls, VPNS and cloud computing

Outcome 4: Understand physical security and protection methods
Competency 4.1: Discuss physical and technical controls

Outcome 5: Understand Social Engineering
Competency: 5.1: Create a training document on social engineering for an organization

Outcome 6: Understand Cybersecurity Frameworks
Competency 6.1: Understand the Risk Management Process
Competency 6.2: Create a Risk Management Matrix
Competency 6.3: Categorize Risk by probability and impact
Competency 6.4: Recommend countermeasures and controls