ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 1201 Managing Information Security

Date: August 28, 2018

Credit Hours: 3

Prerequisite(s): Co-requisite: 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**	

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

IAI Equivalent –***Only for Transfer Courses***-go to *http://www.itransfer.org*:

CATALOG DESCRIPTION:
Organizations must be able to apply effective strategies to secure their networks and keep personnel and customers data safe and secure. This course introduces the topic of cybersecurity and how it has evolved throughout history. This course covers the key principles and practices of information security. The course discusses topics such as access control, risk management, application security including anti-virus and cryptography. The course covers network security, physical security and social engineering.

GENERAL EDUCATION GOALS ADDRESSED

[See last page for Course Competency/Assessment Methods Matrix.]

Upon completion of the course, the student will be able:

[Choose up to three goals that will be formally assessed in this course.]

☐ To apply analytical and problem solving skills to personal, social, and professional issues and situations.
☐ To communicate successfully, both orally and in writing, to a variety of audiences.
☐ To construct a critical awareness of and appreciate diversity.
☒ To understand and use technology effectively and to understand its impact on the individual and society.
☐ To develop interpersonal capacity.
☐ To recognize what it means to act ethically and responsibly as an individual and as a member of society.
☐ To recognize what it means to develop and maintain a healthy lifestyle in terms of mind, body, and spirit.
☒ To connect learning to life.

EXPECTED LEARNING OUTCOMES AND RELATED COMPETENCIES:

[Outcomes related to course specific goals. See last page for more information.]

Upon completion of the course, the student will be able to:

1. Discuss the key principles and practices of Information Security
    a. Understand access controls
    b. Explain the pillars of security and security concepts
    c. Understand the role of an Information Systems Management strategy
2. Identify application security strategies
    a. Understand protection methodologies within application security
3. Understand network security
    a. Discuss firewalls, VPNS and cloud computing
4. Understand physical security and protection methods
    a. Discuss physical and technical controls
5. Understand Social Engineering
6. Explain current cybersecurity threats and the future of cybersecurity

MAPPING LEARNING OUTCOMES TO GENERAL EDUCATION GOALS

[For each of the goals selected above, indicate which outcomes align with the goal.]

Goals	Outcomes
First Goal	
To understand and use technology effectively and to understand its impact on the individual and society.	1. Understand Social Engineering. 2. Explain current cybersecurity threats and the future of cybersecurity.

Second Goal	
To connect learning to life.	1. Discuss the key principles and practices of Information Security a. Understand access controls b. Explain the pillars of security and security concepts c. Understand the role of an Information Systems Management strategy 2. Identify application security strategies a. Understand protection methodologies within application security 3. Understand network security a. Discuss firewalls, VPNS and cloud computing 4. Understand physical security and protection methods a. Discuss physical and technical controls

COURSE TOPICS AND CONTENT REQUIREMENTS:
History of Cybersecurity
Information Security Management
Access Control
Administrative, Application, Network and Physical Security
Social Engineering

INSTRUCTIONAL METHODS:
- Lecture
- Lab

INSTRUCTIONAL MATERIALS:
The InfoSec Handbook (Rao and Nayak, 2014) PDF Format
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-100.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

STUDENT REQUIREMENTS AND METHODS OF EVALUATION:
A= 90-100
B= 80-89
C= 70-79
D= 60-69
F= 0-59

OTHER REFERENCES

Course Competency/Assessment Methods Matrix

(Dept/# Course Name)	Assessment Options																																
For each competency/outcome place an "X" below the method of assessment to be used.	**Assessment of Student Learning**	Article Review	Case Studies	Group Projects	Lab Work	Oral Presentations	Pre-Post Tests	Quizzes	Written Exams	Artifact Self Reflection of Growth	Capstone Projects	Comprehensive Written Exit Exam	Course Embedded Questions	Multi-Media Projects	Observation	Writing Samples	Portfolio Evaluation	Real World Projects	Reflective Journals	Applied Application (skills) Test	Oral Exit Interviews	Accreditation Reviews/Reports	Advisory Council Feedback	Employer Surveys	Graduate Surveys	Internship/Practicum /Site Supervisor Evaluation	Licensing Exam	In Class Feedback	Simulation	Interview	Written Report	Assignment
Assessment Measures – Are direct or indirect as indicated. List competencies/outcomes below.	**Direct/ Indirect**	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	I	I	I	I	D	D							
1. Discuss the key principles and practices of Information Security.								X					X					X														X
1a. Understand access controls.								X					X					X														X
1b. Explain the pillars of security and security concepts.								X					X																			
2. Understand the role of an Information Systems Management strategy.								X					X																		X	X
2a. Understand protection methodologies within application security.					X			X					X					X														X
3. Understand network security.					X			X					X																			
3a. Discuss firewalls, VPNS and cloud computing.								X					X					X														X

4. Understand physical security and protection methods.								X					X					X													X
4a. Discuss physical and technical controls.								X					X					X													X
5. Understand Social Engineering.					X			X					X					X											X		X
6. Explain current cybersecurity threats and the future of cybersecurity.													X					X												X	X