ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 1203 Intro to Cybersecurity

Date: Fall 2021

Credit Hours: 2

Prerequisite(s): None

Delivery Method:		
☒ **Lecture**	**1.5 Contact Hours**	**(1 contact = 1 credit hour)**
☐ **Seminar**	**0 Contact Hours**	**(1 contact = 1 credit hour)**
☐ **Lab**	**1 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 is aimed to educate students about the main threats to data security. It also equips the students with the basic knowledge to keep devices and data secure in daily life. It teaches basic techniques of being secure both online and offline. This course prepares students to sit for EC Council's entry level certification: "Certified Secure Computer User" (CSCU). The certification voucher and taking this certification is included towards the end of this course.

ACCREDITATION STATEMENTS AND COURSE NOTES:
None

COURSE TOPICS AND CONTENT REQUIREMENTS:
1. Introduction to Data Security
2. Data Security Threats
3. Operating Systems Security
4. Internet and Social Networking Sites Security
5. Email Communication and Mobile Device Security
6. Cloud and Network Connection Security

INSTRUCTIONAL METHODS:
1. Lecture
2. Testing
3. Group Discussions
4. Quizzes

EVALUATION OF STUDENT ACHIEVEMENT:
Students must:
1. Participate in class discussions on Live Zoom sessions or demonstrate by work completed the recorded videos of class were reviewed
2. Complete readings, assignments, quizzes, and other assignments given at the instructor's discretion
3. Register and sit for EC-Council's CSCU certification exam.

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

Resources
Computer Applications:
1. Online Course Management Software
2. IVCC email account
3. Web Browser
    a. Vital Source Site

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: Student understands the need for and importance of data security.
Competency1.1: Student will understand different kinds of threats to data.
Competency1.1: Student can explain about the elements of security

Outcome 2: Implement Operating System security measures on their computers.
Competency 2.1: Student can explain the concept of operating system and its functionalities

Outcome 3: Student understands Malware and its symptoms.
Competency 3.1: Student can step through the Ransomware decryption process
Competency 3.2: Student can explain the reasons for Ransomware being a major threat for companies

Outcome 4: Student can make an informed decision about choosing the antivirus most relevant to their needs.
Competency 4.1: Student can explain various types of malware
Competency 4.2: Student can describe common symptoms of a virus affected machine
Competency 4.3: Student can step through the process to find and fix the viruses

Outcome 5: Student understands the risks associated with different online activities.
Competency 5.1: Student can explain the different concepts: Internet, Web Browser and Internet Security

Outcome 6: Student understands why and how to secure web browsers.
Competency 6.1: Student can explain the steps involved in securing Edge, Firefox, Safari, and Chrome

Outcome 7: Student can Identify safe websites.
Competency 7.1: Student can explain the difference between a safe and dangerous website

Outcome 8: Student understands safeguards against the threats associated with online social networking.
Competency 8.1: Student can discuss phishing scams in social media
Competency 8.2: Student can discuss safety measures to avoid responding to fake messages
Competency 8.3: Students understands how to make their social networking accounts secure.

Outcome 9: Student understands the threats associated with email communications and proper safeguards
Competency 9.1: Student can discuss email security

Outcome 10: Student understands the threats to mobile devices and how to safeguard against them.
Competency 10.1: Student can explain why mobile devices have become major targets for attackers
Competency 10.2: Student can explain the main security risks mobile devices face

Outcome 11: Student understands the threats associated with cloud accounts and proper safeguards
Competency 11.1: Student can explain why hackers love the cloud
Competency 11.2: Student can discuss how hackers are participating in hacking attempts to infiltrate the cloud.
Competency 11.3: Student can make an informed decision about a cloud service provider to meet requirements.
Competency 11.4: Student can discuss cloud concepts and types of cloud functionality
Competency 11.5: Student can discuss the terms cloud computing and cloud services

Outcome 12: Student understands the various types of networks and the threats associated with them.
Competency 12.1: Student can identify various types of networks
Competency 12.2: Student can match threats to various networks

Outcome 13: Student can configure a home network.
Competency 13.1: Student can discuss various networking concepts
Competency 13.2: Student can explain how to setup a wireless network connection on various OS

Outcome 14: Students can make their networks secure.
Competency 14.1: Student can discuss threats associated with wireless network security

Outcome 15: Student understands the threats to data and the need for data backups.
Competency 15.1: Student can explain data backup concept and types of backups
Competency 15.2: Student can explain how to backup and restore data on their computers.
Competency 15.3: Student can step through the process of backing up and restoring data on a computer
Competency 15.4: Student understands how to destroy data permanently.
Competency 15.5: Student can discuss safe data destruction concepts
Competency 15.6: Student can describe how to handle data destruction as it applies to identity theft