JAMESTOWN COMMUNITY COLLEGE
State University of New York

INSTITUTIONAL COURSE SYLLABUS

Course Title: Introduction to Cybersecurity

Course Abbreviation and Number: CSC 1520 **Credit Hours:** 3 **Course Type:** Lecture

Course Description: Students will be introduced to the basics of computer security, also known as cybersecurity. The course will also provide students with a basic understanding of the types of security weaknesses and the defense strategies needed to minimize those vulnerabilities. This course combines the theoretical knowledge with the hands-on practical exercises to ensure students are well-equipped to tackle real-world cybersecurity challenges.This course introduces the topics covered by the CompTia Security+ Certification. Additional coursework will be needed prior to taking the CompTia Security+ exam. Prerequisite/Corequisite: CSC 1580, CSC 2510 strongly recommended.

No requisites.

Student Learning Outcomes:

Students who demonstrate understanding can:

1. Design a basic computer network using the fundamental components needed to connect to the Internet.
2. Identify the major weaknesses in computer systems and networks.
3. Categorize the major techniques used by hackers to gain access to computer systems.
4. Select the appropriate tools to minimize specific cybersecurity threat.

Topics Covered:

- Introduction to computers
- Introduction to computer networks, including the Internet
- Major security weaknesses in computer systems, including the people who use these systems
- Motivations of hackers and attackers
- Types of attacks, including identity theft, cyber stalking, fraud, abuse, data theft, social engineering, cyber terrorism, and industrial espionage
- Techniques used to attach computer systems, including viruses, worms, Trojan horses, phishing, buffer overflow, wiretapping, replay, name spoofing, DoS and DDoS, SYN flood, key breaking, port scanning, packet interceptions, and man-in-the-middle
- Tools used to protect computer systems, including anti-virus software, hashing, encryptions, digital signatures, digital certificates, firewalls, intrusion detection systems, deep packet inspection, virtual private networks, and access control.
- Security policies
- Introduction to computer system forensics
- Case studies of several security breaches

Information for Students

- Expectations of Students
  - Civility Statement
  - Student Responsibility Statement
  - Academic Integrity Statement
- Accessibility Services
  Students who require accommodations to complete the requirements and expectations of this course because of a disability must make their accommodation requests to the Accessibility Services Coordinator.
- Get Help: JCC & Community Resources
- Emergency Closing Procedures
- Course grade is determined by the instructor based on a combination of factors, including but not limited to, homework, quizzes, exams, projects, and participation. Final course grade can be translated into a grade point value according to the following:

A=4.0	B+=3.5	B=3	C+=2.5	C=2	D+=1.5	D=1	F=0

- Veterans and active duty military personnel with special circumstances (e.g., upcoming deployments, drill requirements, VA appointments) are welcome and encouraged to communicate these to the instructor.

Effective Date: Fall 2024