SOUTHEAST COMMUNITY COLLEGE
CONSTRUCTION MANUFACTURING AND TECHNOLOGY DIVISION
Computer Information Technology Program
Revision Date: August 22, 2022
Syllabus Statements

I. CATALOG DESCRIPTION

Course Number:	INFO1491
Course Title:	Network Security Fundamentals
Prerequisite(s):	INFO1151, INFO1171, INFO1281
Corequisite(s):	INFO1448, ELEC2760
Catalog Description:	Students examine information security basics focusing on the threats, trends, and ramifications related to security practices and procedures. Various methodologies and devices are introduced that are used to secure and defend an enterprise network.
Credit Hours:	3
Class Hours:	45
Lab Hours:	0
Total Contact Hours:	45

II. COURSE OBJECTIVES: *Course will:*

A. Utilize the CompTIA Security+ Exam objectives as a learning framework.
B. Introduce information security terminology and concepts.
C. Describe types of malware and social engineering attacks.
D. Examine the use of cryptography to secure data, communications, and devices.
E. Describe network-based attacks and defenses, including WLAN security.
F. Examine client and mobile device security including their applications.
G. Introduce identity, account, and access management processes and controls.
H. Explore Risk Management concepts and common security assessment methods.

III. STUDENT LEARNING OUTCOMES AND GENERAL EDUCATION LEARNING OUTCOMES:

A. Student Learning Outcomes: *Student will be able to:*

1. Recognize the domains and objectives of the current CompTIA Security + Exam.
2. Define the major areas involved in Information Security. –B
3. Identify types of attacks, threat actors, and security defenses on Enterprise networks.
4. Explain attacks using malicious software (malware) and social engineering methods.
5. Distinguish among commonly used cryptographic algorithms.
6. Practice implementing cryptography to protect systems and data.
7. Set up defenses to protect systems and devices against common network attacks.
8. Differentiate between the types of security needed for wireless versus wired networks.
9. Explain how to secure client-side and server-side applications.
10. Recognize the vulnerabilities associated with mobile and embedded systems and the IOT.
11. Identify common authentication methods and best practices for access control.
12. Perform Risk Analyses to create security policies, responses, and controls.
13. Use security tools to investigate vulnerabilities, incidents, and risks associated with systems and networks.

B. General Education Learning Outcomes (GELOs)
- **1.** GELO #3: Critical Thinking & Problem Solving
  Outcome 2: Synthesize information to arrive at reasoned solutions to problems.

IV. CONTENT/TOPICAL OUTLINE

- **A.** Introduction to Security
- **B.** Malware and Social Engineering Attacks
  - **1.** Different types of malware and payload operations of malware
  - **2.** Types of psychological and physical social engineering attacks
- **C.** Basic Cryptography
  - **1.** Hash, symmetric, and asymmetric cryptographic algorithms
  - **2.** Various ways cryptography is used
- **D.** Advanced Cryptography
  - **1.** Implementing cryptography, digital certificates, and the Public Key Infrastructure (PKI)
- **E.** Networking and Server Attacks
- **F.** Securing networks through devices, design and technology
  - **1.** Routers, Firewalls, IDPS', Proxies, DMZs, VPNs, NAT,DLP, and NAC
- **G.** Administering a Secure Network
  - **1.** Secure network protocols, analyzing security data, and securing network platforms
- **H.** Wireless Network Security
  - **1.** Wireless attacks, vulnerabilities in IEEE 802.11, and wireless security solutions
- **I.** Client and Application Security
- **J.** Mobile and Embedded Device Security
  - **1.** Types of mobile devices and deployments
  - **2.** Securing Embedded devices and Internet of Things (IoT)
- **K.** Authentication and Account Management
- **L.** Access Management
  - **1.** Best Practices for access control and identity and access services
- **M.** Vulnerability Assessment and Data Security
  - **1.** Vulnerability scanning and penetration testing
  - **2.** Data Privacy and Data Security practices
- **N.** Business Continuity
  - **1.** Environmental controls, digital forensics, and incident response procedures
- **O**. Risk Mitigation
  - **1.** Strategies and practices for managing and reducing risk

V. INSTRUCTIONAL MATERIALS

Classroom Course:

- **A.** Required Text(s): TestOut Security Pro, (Refer to CID and/or instructor for current edition, this must be purchased through SCC's bookstore)
- **B.** Other Resources: Network Security Fundamentals Supplemental Materials and Trial and shareware programs/utilities downloadable from the Internet.
- **C.** Computer and Internet access

VI. METHODS OF PRESENTATION/INSTRUCTION

- **A.** Methods of presentation typically include a combination of the following:
  - **1.** Technology enhanced lecture
  - **2.** Classroom discussions
  - **3.** Interactive group activities

4. Audio visual materials

VII. METHODS OF EVALUATION

A. Methods of evaluation, although determined by the individual instructor, traditionally includes a combination of the following:

1. Attendance and/or participation activities
2. Homework and hands-on assignments
3. Quizzes
4. Exams
5. Research Projects

VIII. SPECIFIC COURSE REQUIREMENTS

A. This course will not qualify as a prerequisite if the student receives a final grade below a C (70%).