SOUTHEAST COMMUNITY COLLEGE
ADVANCED TECHNOLOGIES & SKILLED TRADES DIVISION
Computer Information Technology Program
Revision Date: November 10, 2025

I. CATALOG DESCRIPTION

Course Number:	INFO1491
Course Title:	Network Security Fundamentals
Prerequisite(s):	INFO1171, INFO1283
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

1. Security Overview
2. Defense Planning
3. Using the Simulator

B. Threats, Attacks, and Vulnerabilities

1. Understanding Attacks
2. Malware
3. Social Engineering
4. Vulnerability Concerns

C. Physical

1. Physical Threats
2. Device and Network Protection
3. Environmental Controls

D. Networks and Hosts Design and Diagnosis

1. Manageable Network Plan
2. Windows System Hardening
3. File Server Security
4. Linux Host Security

E. Devices and Infrastructure

1. Security Appliances
2. Demilitarized Zones
3. Firewalls
4. Network Address Translation
5. Virtual Private Networks
6. Web Threat Protection
7. Network Access Control
8. Network Threats
9. Network Device Vulnerabilities
10. Network Applications
11. Switch Security and Attacks
12. Using VLANs
13. Router Security

F. Identity, Access, and Account Management

1. Access Control Models
2. Authentication
3. Authorization
4. Windows User Management
5. Active Directory Overview
6. Hardening Authentication
7. Linux Users
8. Linux Groups
9. Remote Access
10. Network Authentication

G. Cryptography and PKI

1. Cryptography
2. Cryptography Implementations
3. Hashing
4. File Encryption
5. Public Key Infrastructure

H. Wireless Threats

1. Wireless Overview
2. Wireless Attacks
3. Wireless Defenses

I. Virtualization, Cloud Security, and Securing Mobile Devices

1. Host Virtualization
2. Virtual Networking
3. Software-Defined Networking
4. Cloud Services
5. Cloud Security
6. Mobile Devices
7. Mobile Device Management
8. BYOD Security
9. Embedded and Specialized Systems

J. Securing Data and Applications

1. Data Transmission Security
2. Data Loss Prevention
3. Web Application Attacks
4. Application Development and Security

K. Security Assessments

1. Penetration Testing
2. Monitoring and Reconnaissance
3. Intrusion Detection
4. Security Assessment Techniques
5. Protocol Analyzers
6. Analyzing Network Attacks
7. Password Attacks

L. Incident Response, Forensics, and Recovery

1. Incident Response
2. Mitigation of an Incident
3. Log Management
4. Windows Logging
5. Digital Forensics
6. File and Packet Manipulation
7. Redundancy
8. Backup and restore

M. Risk Management

1. Organizational Security Policies
2. Risk Management
3. Email

N. Governance and Compliance

1. Audits
2. Controls and Frameworks
3. Sensitive Data and Privacy

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%).