

# ITCT 235-SECURITY+ 3 CREDITS

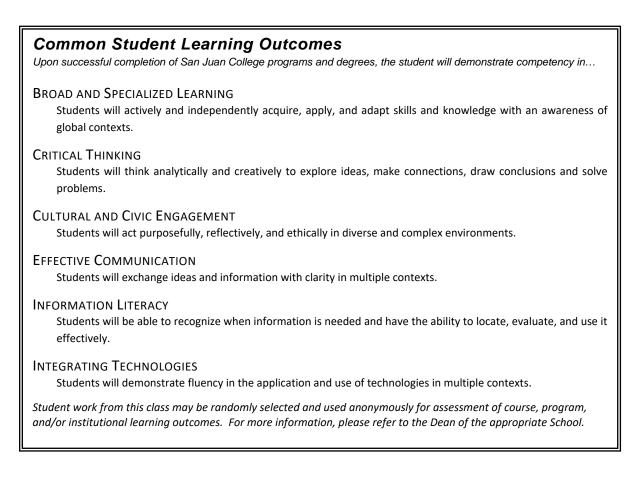
## **SYLLABUS**

## CATALOG DESCRIPTION

This course is a study of encryption technologies, system and network security, firewall implementation, intrusion detection and prevention. It also covers operating system, user account, and file resource security, assessing risk, auditing, and security control procedures. This course may be used as preparation for an industry certification exam.

Prerequisites: ITCT 115

Semester Offered: Spring



#### **Course Learning Outcomes**

Upon successful completion of the course, the student will be able to...

#### 1. Network Security

A copy of this approved syllabus is on file in the dean's office. Updated 2017-05-01

- 1.1. Implement security configuration parameters on network devices and other technologies.
- 1.2. Given a scenario, use secure network administration principles.
- 1.3. Explain network design elements and components.
- 1.4. Given a scenario, implement common protocols and services.
- 1.5. Given a scenario, troubleshoot security issues related to wireless networking.

#### 2. Compliance and Operations Security

- 2.1. Explain the importance of risk related concepts.
- 2.2. Summarize the security implications of integrating systems and data with third parties.
- 2.3. Given a scenario, implement appropriate risk mitigation strategies.
- 2.4. Given a scenario, implement basic forensic procedures.
- 2.5. Summarize common incident response procedures.
- 2.6. Explain the importance of security related awareness and training.
- 2.7. Compare and contrast physical security and environmental controls.
- 2.8. Summarize risk management best practices.
- 2.9. Given a scenario, select the appropriate control to meet the goals of security.

#### 3. Threats and Vulnerabilities

- 3.1. Explain types of malware.
- 3.2. Summarize various types of attacks.
- 3.3. Summarize social engineering attacks and the associated effectiveness with each attack.
- 3.4. Explain types of wireless attacks.
- 3.5. Explain types of application attacks.
- 3.6. Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.
- 3.7. Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.
- 3.8. Explain the proper use of penetration testing versus vulnerability scanning.

#### 4. Application, Data and Host Security

- 4.1. Explain the importance of application security controls and techniques.
- 4.2. Summarize mobile security concepts and technologies.
- 4.3. Given a scenario, select the appropriate solution to establish host security.
- 4.4. Implement the appropriate controls to ensure data security.
- 4.5. Compare and contrast alternative methods to mitigate security risks in static environments.

#### 5. Access Control and Identity Management

- 5.1. Compare and contrast the function and purpose of authentication services.
- 5.2. Given a scenario, select the appropriate authentication, authorization or access control.
- 5.3. Install and configure security controls when performing account management, based on best practices.

### 6. Cryptography

- 6.1. Given a scenario, utilize general cryptography concepts
- 6.2. Given a scenario, use appropriate cryptographic methods.
- 6.3. Given a scenario, use appropriate PKI, certificate management and associated components.