

## Master Syllabus

### CIS 2640 - Network Security

**Division:** Business and Public Services

**Department:** Computer Information Systems

**Credit Hour Total:** 3.0

**Lecture Hrs:** 3.0

**Prerequisite(s):** CIS 1107 AND CIS 1130 OR CIS 1411

**Date Revised:** September 2016

---

### Course Description:

Intermediate computing and network security fundamentals. Topics include network vulnerabilities and attacks, network defenses, wireless network security, access control, network assessment and auditing, cryptography and organizational security. Preparation will also be given for the ComptTIA Security + exam.

### General Education Outcomes:

- Critical Thinking/Problem Solving Competency
- Information Literacy Competency
- Computer Literacy Competency

### Course Outcomes:

#### Cryptography in Networks

Use cryptography including the proper use of algorithms, digital certificates, public key cryptographic standards, key management, and cryptographic transport protocols to create secure networks.

**Assessment Method:** Locally developed exams

**Performance Criteria:** 70% or higher on a standard rubric

**Assessment Method:** Simulations

**Performance Criteria:** 70% or higher on a standard rubric

#### Network Access Control and Vulnerability Mitigation

Control access to and mitigate vulnerabilities in wired and wireless networks.

**Assessment Method:** Locally developed exams

**Performance Criteria:** 70% or higher on standard rubric

**Assessment Method:** Simulations

**Performance Criteria:** 70% or higher on standard rubric

#### Network Infrastructure Protection

Assess network vulnerabilities and attacks, identify hardware and software defenses needed to protect the infrastructure in both wired and wireless installations, and the strategies used to protect a network infrastructure.

**Assessment Method:** Locally developed exams

**Performance Criteria:** 70% or higher on a standard rubric

**Assessment Method:** Simulations

**Performance Criteria:** 70% or higher on a standard rubric

### Outline:

Network Vulnerabilities and Attacks  
Network Defense Strategies  
Wireless Network Security  
Access Control Fundamentals  
Network Authentication  
Vulnerability  
Assessments  
Conducting Security Audits  
Cryptography  
Business Continuity Planning  
Security Policy planning and implementation  
Acceptable Use Policies