Course Syllabus Part I
CIS 311 Network Security

3 Credit Hours

Course Description
This course introduces students to the goals, functional processes, tools, and techniques associated with network security. Services such as firewalls, intrusion detection mechanisms and Virtual Private Networks (VPNs) will be studied. Students will develop an understanding of telecommunications and network security protocols used to prevent, detect, and correct potential vulnerabilities associated with both the outsider and insider threat.

Course Prerequisites
None

Course Objectives

Students who successfully complete this course should be able to:

1. Apply fundamental principles of information security to problems related to network administration, threats and countermeasures, policies and standards, and security management.
2. Compare and contrast existing models for network security, including authorization, authentication, access control, network segmentation and protection protocols.
3. Differentiate types of firewalls, intrusion detection / prevention devices, remote access, cryptographic systems, and other network protection technologies in terms of principles and technical requirements.
4. Design a security plan for a sample organization that incorporates network and system security topics and technologies introduced in the course.
5. Predict trends in network security management based on current and projected architectural standards.

Grading Scale

93 – 100% = A	87 – 89% = B+	77 – 79% = C+	67 – 69% = D+
90 – 92% = A-	83 – 86% = B	73 – 76% = C	63 – 66% = D
	80 – 82% = B-	70 – 72% = C-	60 – 62% = D-
			0 – 59% = F

Topic Outline

I. Computer Network Security Principles
   a. Importance of computer and network security
   b. Underlying computer and network security concepts
   c. Threats and countermeasures
   d. Policies and standards

II. Network and Server Security
   a. Network protocols review
   b. Best practices for network security
   c. Securing servers
   d. Border security
   e. Firewall types and technologies

III. Authentication, Authorization, and Access Control
   a. Authentication overview
   b. Authentication credentials
   c. Authentication protocols
   d. Best practices for secure authentication
   e. Access control models

IV. Securing Network Transmission
   a. Transmission and emission security
   b. Analyzing security requirements for network traffic
   c. Defining network perimeters
   d. Data transmission protection protocols
   e. IPv6 and IPSec

V. Remote Access and Wireless Security
   a. Dial-up networking
   b. Virtual private networks
   c. RADIUS and TACACS
   d. Wireless networks

VI. Server Roles and Security
   a. Server roles and baselines
   b. Securing network infrastructure servers
   c. Securing application servers

VII. Intrusion Detection and Forensics
   a. Intrusion detection
   b. Honeypots
   c. Forensics

VIII. Ongoing Security Management
   a. Managing updates
   b. Auditing and logging
   c. Secure remote administration

IX. Designing a secure network architecture
   a. Design plan
   b. Tools
   c. Design considerations
   d. Deliverables

X. Technologies and trends in network security
   a. Voice over IP (VOIP) and voice communications
   b. Mobile network security