Course Syllabus Part I
CIS 312 Securing Access Control

3 credit hours

Course Description

This course provides the student with the basic topics associated with controlling how resources are accessed in an information system. Topics include organizational access control models, security models, and hardware and software controls that can be used to support those models. Additional topics include access models, and securing system access with passwords, smart cards and biometric devices to assist in securing system access and ensure confidentiality, integrity, and availability of data. Technologies such as remote authentication and Public Key Infrastructure (PKI) are also explored.

Course Prerequisites

None

Course Objectives

1. Demonstrate an understanding of confidentiality, authentication, and integrity as they apply to information security.
2. Describe traditional access control models and technologies.
3. Describe traditional security models and technologies.
4. Demonstrate an understanding of physical and logical controls.
5. Describe remote access technologies and identify the security issues associated with remote access.
6. Identify threats to control practices and technologies.

Grading Scale

94 – 100% = A
90 – 93% = A-

87 – 89% = B+
83 – 86% = B
80 – 82% = B-

77 – 79% = C+
73 – 76% = C
70 – 72% = C-

67 – 69% = D+
63 – 66% = D
60 – 62% = D-
0 – 59% = F

Topic Outline

I. Fundamentals of Information Security (Obj. I)
    a. Confidentiality
    b. Authentication
    c. Integrity.

II. Access Control Models (Obj. 2)
    a. Mandatory access control
    b. Discretionary access control
    c. Role-based access control
    d. Rule-based access control
    e. Task-based access control

III. Security Models (Obj. 3)
    a. Bell-LaPadula model
    b. Biba
    c. Clark-Wilson model
    d. Information flow model

IV. Physical and Logical Controls (Obj. 4)
    a. Physical controls
        I. Smart cards
        2. Biometric devices
        3. Tokens
    b. Logical controls
        1. Firewalls
        2. Access control lists
        3. Public Key Infrastructure (PKI)
        4. Security zones

V. Remote Access (Obj. 5)
    a. Radius
    b. Virtual Private Networks (VPNs)
    c. Remote access services

VI. Threats (Objs. I, 4, 6)
    Man-in-the-middle attacks
    a. Password attacks
        1. Brute force
        2. Dictionary
    b. Denial of service attacks
    c. Back door attacks
    d. Replay attacks
    e. Spoofing