1. **IAAS221 <u>Security Foundations</u>**

2. **Credit Hours:** 3

3. **Contact Hours:** 45

4. Coordinator: Richard Comden

5. Text book: Principles of Information Security, Michael E. Whitman, Herbert J. Mattord, 2018

No other supplemental materials

6. Course information
    a. This course will provide an overview of information security from both the perspectives of the organization and that of personal computing. Topics include security management practices, physical security, security architecture, business continuity and disaster recovery planning, access control systems, security controls, cryptography, telecommunications and network security, operations security, law and ethics, and personal computer security.
    b. Recommended Prerequisite(s): CISP100

7. This is a required course

8. Specific goals for the course:

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

1. discuss effective security management practices.
2. discuss the rationale and methods for controlling access to network systems.
3. describe cryptography and symmetric & asymmetric key cryptography
4. discuss security models and operations security.
5. discuss software application and database security issues.
6. discuss disaster recovery, business continuity, and legal & ethical issues.
7. describe the threats to physical security.
8. discuss topics relevant to security for personal computers.

9. explicitly indicate which of the Student Outcomes l−6 are addressed by the course.

Course Learning Outcome	Student Objective
1. discuss effective security management practices.	4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles
2. discuss the rationale and methods for controlling access to network systems.	6. Apply computer science theory and software development fundamentals to produce computing-based solutions. [CS]

3. describe cryptography and symmetric & asymmetric key cryptography	6. Apply computer science theory and software development fundamentals to produce computing-based solutions. [CS]
4. discuss software application and database security issues.	6. Apply computer science theory and software development fundamentals to produce computing-based solutions. [CS]
5. discuss disaster recovery, business continuity, and legal & ethical issues.	4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles 6. Apply computer science theory and software development fundamentals to produce computing-based solutions. [CS]
6. describe the threats to physical security.	6. Apply computer science theory and software development fundamentals to produce computing-based solutions. [CS]
7. discuss topics relevant to security for personal computers.	6. Apply computer science theory and software development fundamentals to produce computing-based solutions. [CS]

10. Brief list of topics to be covered
    - Introduction to Information Security (3)
    - The Need for Security (4)
    - Legal, Ethical, and Professional Issues in Information Security (4)
    - Planning for Security (4)
    - Security Technology: Access Controls, Firewalls, and VPNs (5)
    - Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools (5)
    - Cryptography (4)
    - Physical Security (4)
    - Implementing Information Security (4)
    - Security and Personnel (4)
    - Information Security Maintenance (4)