COURSE OUTLINE

CITA 250 - INFORMATION SECURITY

Revised By: Minhua Wang
A. **TITLE:** INFORMATION SECURITY  

B. **COURSE NUMBER:** CITA 250  

C. **CREDIT HOURS:** 3  

D. **WRITING INTENSIVE COURSE:** No  

E. **COURSE LENGTH:** 15 weeks  

F. **SEMESTER(S) OFFERED:** Spring  

G. **HOURS OF LECTURE, LABORATORY, RECITATION, TUTORIAL, ACTIVITY:**  
   3 lecture hours per week  

H. **CATALOG DESCRIPTION:** An introduction to various technical and administrative aspects of Information Security and Assurance. Students are exposed to the spectrum of Information Security activities, methods, methodologies, and procedures. Coverage include inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post-incident procedures, technical and managerial responses and an overview of Information Security planning and staffing functions.  

I. **PRE-REQUISITES/CO-REQUISITES:**  
   a. Pre-requisite(s): CITA 220 Data Communications and Network Technology  
   b. Co-requisite(s): none  

J. **GOALS (STUDENT LEARNING OUTCOMES):**  
   By the end of this course, the student will be able to:  

<table>
<thead>
<tr>
<th>Course Objective</th>
<th>Institutional SLO</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Specify information assets</td>
<td>2. Crit. Thinking</td>
</tr>
<tr>
<td>b. Specify threats to information assets</td>
<td>3. Prof. Competence</td>
</tr>
<tr>
<td>c. Define an Information Security strategy and architecture</td>
<td>2. Crit. Thinking</td>
</tr>
<tr>
<td>d. Exhibit an approach to plan for and respond to intruders in an information system</td>
<td>3. Prof. Competence</td>
</tr>
<tr>
<td>e. Describe legal and public relations implications of security and privacy issues</td>
<td>2. Crit. Thinking</td>
</tr>
<tr>
<td>f. Demonstrate a disaster recovery plan for recovery of information assets after an incident</td>
<td>3. Prof. Competence</td>
</tr>
<tr>
<td></td>
<td>4. Personal Skills</td>
</tr>
</tbody>
</table>

K. **TEXTS:**  
L. REFERENCES:  N/A

M. EQUIPMENT:  technology enhanced Classroom

N. GRADING METHOD:  A-F

O. MEASUREMENT CRITERIA/METHODS:
   • Exams
   • Quizzes
   • Participation

P. DETAILED COURSE OUTLINE:

I. Introduction to Information Security
   A. The History of Information Security
   B. Critical Characteristics of Information
   C. Components of an Information System
   D. Security Models
   E. Security Systems Development Cycle

II. Security Investigation
   A. Information Assets
   B. Threats
   C. Attacks
   D. Laws in Information Security
   E. Ethics in Information Security
   F. Codes of Professional Organizations in Information Security

III. Security Analysis
   A. Risk Identification
   B. Risk Assessment
   C. Risk Control Strategies

IV. Security Logical Design
   A. Information Security Policy, Standards, and Practices
   B. Information Security Blueprint
   C. Security Education, Training, and Awareness Program
   D. Continuity Strategies

V. Security Physical Design
   A. Firewalls
   B. Protecting Remote Connections
   C. Intrusion Detection and Prevention Systems
   D. Access Control Devices
   E. Introduction to Cryptography
   F. Physical Security
VI. Security Implementation
   A. Information Security Project Management
   B. Technical Aspects of Security Implementation
   C. Non-technical Aspects of Security Implementation
   D. Security and Personnel

VII. Security Maintenance
   A. Security Management Models
   B. Maintenance Model
   C. Introduction to Digital Forensics

Q. **LABORATORY OUTLINE**: N/A