STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

MASTER SYLLABUS

CITA 250 - INFORMATION SECURITY

Created by: Minhua Wang
Updated by: Minhua Wang

CANINO SCHOOL OF ENGINEERING TECHNOLOGY
DECISION SYSTEMS
FALL 2018

A. **TITLE**: INFORMATION SECURITY

B. **COURSE NUMBER:** CITA 250

C. **CREDIT HOURS: (Hours of Lecture, Laboratory, Recitation, Tutorial, Activity)**

 # Credit Hours: 3
 # Lecture Hours: 3 **per week**
 # Lab Hours: **per week**
Other: **per week**

Course Length: 15 **Weeks**

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** None

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

G. **COURSE 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.

H. **PRE-REQUISITES/CO-REQUISITES:**

a. Pre-requisite(s): CITA 165 Survey of Cybersecurity or CITA 220 Data Communications and Network Technology
b. Co-requisite(s): none
c. Pre- or co-requisite(s): none

I. **STUDENT LEARNING OUTCOMES:**

By the end of this course, the student will be able to:

Course Student Learning Outcome [SLO]	***PSLO***	***ISLO***
a. Specify information assets	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
b. Specify threats to information assets	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
c. Define an Information Security strategy and architecture	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[CA, PS] 5

d. Exhibit an approach to plan for and respond to intruders in an information system	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[CA] 5
e. Describe legal and public relations implications of security and privacy issues	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	4[ER] 5
f. Demonstrate a disaster recovery plan for recovery of information assets after an incident	2. Interpret, produce, and present work-related documents and information effectively and accurately 5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	1[W] 5

J. APPLIED LEARNING COMPONENT:
Yes X
No

- Classroom/Lab

K. TEXTS: Whitman, M., & Mattord, H. (2018). *Principles of Information Security, 6th Edition*. Boston, MA: Cengage Learning

L. REFERENCES: N/A

M. % **EQUIPMENT:** Computer lab classroom

N. % **GRADING METHOD:** A-F

O. % **SUGGESTED 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
- P. Firewalls
- Q. Protecting Remote Connections
- R. Intrusion Detection and Prevention Systems
- S. Access Control Devices
- T. Introduction to Cryptography
- U. 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. <u>LABORATORY OUTLINE</u>: N/A