

OAKTON COMMUNITY COLLEGE GENERIC COURSE SYLLABUS

I.	<u>COURSE PREFIX</u>	<u>COURSE NUMBER</u>	<u>COURSE NAME</u>	<u>CREDIT</u>	<u>LECTURE</u>	<u>LAB</u>
	CNS	170	Principles of Information Security	3	3	1
	(Formerly LAN 183)					

II. PREREQUISITE:

CNS 111 (Formerly 111) or LAN 171 or consent of instructor, coordinator or program chair.

III. COURSE (CATALOG) DESCRIPTION:

This course provides students with a balance between security management and the technical components of security. The course covers the Security Systems Development Life Cycle (SecSDLC). This structured methodology provides a supportive framework to guide students through an examination of the components of the information domain of Information Security Network. This course also assists students in preparation for the appropriate Network or Information Security Certification examinations.

IV. LEARNING OBJECTIVES:

Upon completion of this course the student will:

1. Understand Information Security
2. Understand how Information Security came to mean what it does today
3. Comprehend the history of Computer Security
4. Comprehend how Computer Security evolved into Information Security
5. Understand the key terms and critical concepts of Information Security
6. Outline the phases of the Security Systems Development Life Cycle (SecSDLC)
7. Understand the role of professionals involved in information security in an organizational

V. ACADEMIC INTEGRITY:

Students and employees at Oakton Community College are required to demonstrate academic integrity and follow Oakton's Code of Academic Conduct. This code prohibits:

- cheating
- plagiarism (turning in work not written by you, or lacking proper citation)
- falsification and fabrication (lying or distorting the truth)
- helping others to cheat
- unauthorized changes on official documents
- pretending to be someone else or having someone else pretend to be you
- making or accepting bribes, special favors, or threats, and
- any other behavior that violates academic integrity.

There are serious consequences to violations of the academic integrity policy. Oakton's policies and procedures provide students a fair hearing if a complaint is made against you. If you are found to have violated the policy, the minimum penalty is failure on the assignment and, a disciplinary record will be established and kept on file in the office of the Vice President for Student Affairs for a period

of 3 years.

Details of the Code of Academic Conduct can be found in the Student Handbook.

VI. OUTLINE OF TOPICS:

1. Introduction to Information Security
2. Security Investigation Phase
3. Legal, Ethical and Professional Issues in Information Security
4. Security Analysis
5. Risk Management: Identifying and Assessing Risk
6. Risk Management Assessing and Controlling Risk
7. Logical Design
8. Planning for Continuity
9. Physical Design
10. Physical Security
11. Implementing Security
12. Security and Personnel
13. The Security Function within an Organization's Structure
14. Information Security Maintenance

VII. METHODS OF INSTRUCTION:

Methods include lectures, class exercises and class discussion, perform lab exercise and projects.

VIII. COURSE PRACTICES REQUIRED:

Read course materials - textbook and current journals
Attend and participate in class lecture and lab
Complete required assignments, exercises, quizzes, and exams

IX. INSTRUCTIONAL MATERIALS:

- Textbook and Lab book: Appropriate Book in the Principles of Information Security
- Current Self-Test Software
- Software manuals

X. METHODS OF EVALUATING STUDENT PROGRESS:

Quizzes, examinations, completion of lab assignments, exercises, and LAN project

XI. OTHER COURSE INFORMATION:

If you have a documented learning, psychological, or physical disability you may be entitled to reasonable academic accommodations or services. To request accommodations or services, contact the ASSIST office in the Learning Center. All students are expected to fulfill essential course requirements. The College will not waive any essential skill or requirement of a course or degree program.