

**OAKTON COMMUNITY COLLEGE  
GENERIC COURSE SYLLABUS**

<b>I.</b>	<b><u>COURSE PREFIX</u></b>	<b><u>COURSE NUMBER</u></b>	<b><u>COURSE NAME</u></b>	<b><u>CREDIT</u></b>	<b><u>LECTURE</u></b>	<b><u>LAB</u></b>
	CNS	176	Security+ Certification	3	3	1

**II. PREREQUISITE:**

CNS 105 or consent of instructor, coordinator, or program chair

**III. COURSE (CATALOG) DESCRIPTION:**

Course provides knowledge necessary to understand core concepts of the threats to a computing infrastructure. Content includes securing a network infrastructure; understanding encryption technologies; securing communications and applications; responding to incidents; creating and maintaining a secure network infrastructure. Course prepares students to become certified in Security+ Certification examination administered by the Computing Technology Industry Association (CompTIA).

**IV. LEARNING OBJECTIVES:**

Upon completing this course, students will be able to:

1. Describe the components of risk assessment; common types of attacks and malicious code
2. Identify common threats to a computing infrastructure and common defenses against threats
3. Apply basic security guidelines and the role of security baselines
4. Describe trusted computing bases.
5. Monitor and maintain a security baseline.
6. Identify access control methods.
7. Identify authentication methods.
8. Choose authentication and access control strategies.
9. Describe basic principles and uses of cryptography. the certificate life cycle.
10. Describe how cryptography is applied.; how a public key infrastructure distributes cryptographic keys
11. Explain what certificates are and how they are used.
12. Describe practical applications of a public key infrastructure (PKI).
13. Describe how features of TCP/IP relate to network security.
14. Describe procedures for detecting intrusion attempts.
15. Respond to security incidents.
16. Identify common attacks against Web servers; Internet applications and explain how to protect against these attacks.
17. Identify common attacks against Domain Name System (DNS) and DHCP and explain how to protect against these attacks.
18. Describe how to secure instant messaging (IM).
19. Implement firewalls.

20. Identify steps for establishing site security.
21. Secure removable media; Secure mobile devices and dispose of equipment
22. Identify methods for protecting business continuity.
23. Maintain documentation, policies, and procedures.
24. Assess risks and Establish security education
25. Resolve ethical dilemmas.

## **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:**

- A. Addressing Security Threats and Vulnerabilities
- B. Creating Security Baselines
- C. Using Access Control and Authentication
- D. Using Encryption
- E. Using a Public Key Infrastructure
- F. Securing the Network Infrastructure
- G. Securing Communications
- H. Securing Network Applications
- I. Securing Internet Messaging
- J. Securing Your Network Perimeter
- K. Maintaining Operational Security
- L. Maintaining Organizational Security
- M. Detecting and Responding to Incidents

## **VII. METHODS OF INSTRUCTION:**

Methods include lectures, class exercises, class discussion, and hands-on lab exercises.

**VIII. COURSE PRACTICES REQUIRED:**

- Read course materials – textbook, and Self-Test
- Attend and participate in class lecture and lab.
- Complete required assignments, exercises, quizzes, and exams.
- Complete LAN projects.

**IX. INSTRUCTIONAL MATERIALS:**

- Textbook and Lab book: Microsoft Official Academic Learning Series
- Current Self-Test Software
- Software manuals

**X. METHODS OF EVALUATING STUDENT PROGRESS:**

Quizzes, examinations, completion of lab assignments, exercises; and several Security projects

**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.