WILMINGTON UNIVERSITY
COLLEGE OF TECHNOLOGY
BASIC COURSE INFORMATION

COURSE TITLE: Web and Data Security

COURSE NUMBER: SEC 410

Minimum Grade Policy
The Computer & Network Security program has set a minimum passing grade of "C-" for program core courses. Students receiving a grade lower than "C-" in any required core course must retake that course.

I. MAJOR INSTRUCTIONAL GOALS:

During this course, students should improve their understanding of:

GOAL #1: Network Security and Firewalls

Learning Outcomes - The student will:

A. Learn about establishing an effective security policy, identifying different types of hacker activities, understanding the hacker's mind-set, and preventing and managing hacker penetration.
B. Learn about authentication procedures, encryption standards and implementations, ports and protocols that hackers manipulate.
C. Learn how to engage in proactive detection and response/reporting methods.

GOAL #2: Operating system security

Learning Outcomes - The student will:

A. Learn about issues such as protecting a current Windows server environment and Linux systems from attacks.
B. Learn about reconfiguring the operating system to fully protect it.
C. Learn about scanning hosts for known security concerns.
D. Have a solid understanding of the security architectures used by a current Windows server environment and Linux.

GOAL #3: Security auditing, attacks, and threat analysis

Learning Outcomes - The student will:
A. Learn how to perform different phases of a security audit, including how to prevent unauthorized users from controlling company networks.
B. Learn how to prevent hackers from controlling your network, and how to generate effective audit reports that can help organizations improve their security and become current with industry security standards.
C. Learn how to recommend industry-standard security solutions for your enterprise.

II. LEARNING ACTIVITIES:

Web and Data Security is designed to educate users in the technologies, terms, and processes related to Internet security. Divided into four distinct parts, this course will teach individuals about the concepts and techniques related to general security, network security, operating system security, and methods for testing security. Both UNIX and Microsoft Windows operating systems are covered, providing a broad range of information essential for every Web professional. Throughout the course the student will see security-related issues through the eyes of a fictitious IT staff, demonstrating the kind of real-world situations that security professionals experience in the workplace. In addition, students may use the text for the course to prepare for the CIW Security Professional exam. This course will focus on the following:

- Describe some of the incidents of network security breaches
- Explain the types and motivations of people/groups that carry out this sort of intrusion
- Describe how an intruder might gain information on security weaknesses and describe some of the tools that might be used to capitalize on those weaknesses
- Explain how Denial of Service attacks are carried out and analyze the potential threat to their organization from these types of intruders
- Describe the characteristics of a security response team and evaluate the need for such a team within their organization or if such a team exists evaluate its correct effectiveness.
- Analyze the potential impact on their organization of infringement of regulations
- Make informed recommendations on necessary changes to practice or procedure or explain why no such changes are necessary.
- Evaluate the need for changes to existing security policies and procedures
- Apply the knowledge gained to create a plan for implementing new or updated procedures.
- Describe the four main areas of data security
- Identify the difference between symmetric crypto and asymmetric crypto
• Review existing procedures to identify improvements and where appropriate apply these improvements

• Describe the role of a firewall and its potential functions and analyze the pros and cons of this form of security and its appropriateness to their organization.

III. SUPPLEMENTAL OBJECTIVES

Will consist Network Security articles and a structured external assignment on constructing a IT Network Security Implementation Plan. Details of the assignments will be discussed the first week of class.

IV. CLASS PARTICIPATION:

Students are expected to attend class and participate actively and in a positive way. Questions and relevant observations are encouraged and enrich the experience of the entire class.

Computers in the classrooms are intended to be used as tools to enhance the students' learning experience. Instant messaging, gaming, emailing, and surfing the web are distractions to the student, the surrounding students, and the instructor and constitute inappropriate behavior. Students are ethically obliged to avoid these and similar practices.