WILMINGTON UNIVERSITY
COLLEGE OF TECHNOLOGY
BASIC COURSE INFORMATION

COURSE TITLE: Data Integrity and Disaster Recovery
COURSE NUMBER: SEC 420

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: Understanding the process, the planning, and the principles of disaster recovery.

Learning Outcomes - The student will:

A. Understand how an organization develops a disaster recovery and business continuity planning philosophy as well as disaster recovery/business continuity plans.
B. Understand how to organize the disaster recovery planning team; be able to describe the fundamental building blocks of disaster recovery planning.
C. Understand how to prioritize the business activities most critical to the organization.

GOAL #2: Understanding the development of the disaster recovery team, the results of a disaster, and how to protect essential assets.

Learning Outcomes - The student will:

A. Be able to determine how the disaster recovery planning team develops recovery procedures for each facility the organization operates; be able to determine the various agencies an organization needs to work with to recover from a disaster, including law enforcement, emergency services, utilities, business partners, and suppliers.
B. Understand disasters that can result from cyber attacks and hackers, rather than from natural occurrences or accidents
C. Understand how to protect special assets (hazardous materials, controlled substances, historic documents, trade secrets) in the event of a disaster.

GOAL #3: Understanding how a disaster plan is put into effect, the testing involved in a disaster recovery, the transition in a disaster, and the knowledge gained from performing the disaster recovery functions.

Learning Outcomes - The student will:
A. Understand how an organization puts its plan into effect, including development of an implementation plan, assessing the value of mitigation steps, assigning responsibilities for implementation, establishing an implementation schedule, and training employees.

B. Understand how to develop testing scenarios to evaluate how well disaster recovery plans and procedures actually work.

C. Understand how to transition into maintenance mode after the plan is implemented.

D. Understand how to capture the knowledge and experience gained during an actual disaster.

II. LEARNING ACTIVITIES:

The goal of this course is to provide a thorough, step-by-step process for learning the fundamentals of disaster recovery planning. Disaster recovery planning is the process of assessing risks that an organization faces, then developing, documenting, implementing, testing, and maintaining procedures that help the organization quickly return to normal operations and minimize losses after a disaster. This course will enable individuals to become disaster recovery planning team leaders and members. The disaster recovery planning process covered in this course is broken down into eight major steps:

1) Organizing the team
2) Assessing risks in the enterprise
3) Establishing roles across departments and organizations
4) Developing policies and procedures
5) Documenting disaster recovery procedures
6) Preparing to handle disasters
7) Training, testing, and rehearsal
8) Ongoing management.

III. SUPPLEMENTAL OBJECTIVES:

Will consist Disaster Recovery articles and a structured external assignment on constructing an IT Disaster Recovery 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.