COURSE INFORMATION FORM

DISCIPLINE: Computer Science and Information Systems
COURSE TITLE: Network and Systems Security
CR.HR: 3 LECT HR: 2 LAB HR: 2 CLIN/INTERN HR: CLOCK HR: 

CATALOG DESCRIPTION
This course will introduce students to network and systems security by exploring vulnerabilities, threats, attacks, and countermeasures. Students will also learn fundamental security design principles and implementation techniques. This course maps to many of the objectives on the CompTIA Security+ certification exam.

PREREQUISITES
CSIS 112 or CSIS 161 with a grade of C or better and
CSIS 170 with a grade of C or better (or concurrent enrollment)

EXPECTED STUDENT OUTCOMES IN THE COURSE (ESO)
Upon completion of this course, the student will be able to:

1. Apply network security and secure network administration fundamentals.
2. Describe social engineering techniques.
3. Describe information system vulnerabilities.
4. Describe different types of attacks and their characteristics.
5. Describe fundamental security design principles.
6. Apply appropriate countermeasures.
7. Apply cryptography methods for confidentiality, integrity, and non-repudiation.

GENERAL EDUCATION OUTCOMES (ESO)
Specify which general education outcomes, if any, are substantially addressed by the course. Numbers in parentheses identify the Expected Student Outcomes linked to the specific General Education Outcome.

Outcomes ESO

Revised 1/15/16
PROGRAM-LEVEL OUTCOMES

CAREER AND TECHNICAL EDUCATION PROGRAM OUTCOMES
Specify which Career and Technical program outcomes, if any, are substantially addressed by the course by completing the “Career and Technical Education template” to show the relationship between course and program outcomes to assessment measures.

1. Use industry specific software and/or apply troubleshooting skills to solve problems.

CLASS-LEVEL ASSESSMENT MEASURES
Student accomplishment of expected student outcomes may be assessed using the following measures. (Identify which measures are used to assess which outcomes.)

1. Examination/Quizzes (1-7)
2. Class Discussion/Participation (1-7)
3. Exercises/Projects (1-7)
4. Written/Oral Reports (1-7)

CATALOG NO. CSIS 178

COURSE OUTLINE FORM

DISCIPLINE Computer Science & Information Systems

COURSE TITLE: Network and Systems Security
Individual instructors may order this outline as fits the needs of their individual courses. In addition, they may place more emphasis on some areas than on others. What is assured is that this particular list is covered in the course. Other topics may be added to a course as the instructor sees fit, and as time and interest allow. An *asterisk can be used to mark an item as optional.

I. Network Security
   A. Network device security
   B. Secure network administration principles
   C. Secure network components and design principles
   D. Common protocols and services
   E. Secure wireless networking

II. Threats and Vulnerabilities
   A. Malware
   B. Types of attacks
   C. Social engineering
   D. Mitigation and deterrent techniques
   E. Penetration testing and vulnerability scanning

III. Application, Host, and Data Security
   A. Application security control
   B. Mobile device security
   C. Host security concepts
   D. Data security concepts

IV. Access Control
   A. Authentication and authorization
   B. Account management
V. Cryptography

A. Confidentiality

B. Integrity

C. Non-repudiation