COURSE INFORMATION FORM

DISCIPLINE                     Computers Science & Information Systems
COURSE TITLE                   Secure E-Commerce
CR.HR. 3  LECT HR. 2  LAB HR. 2  CLIN/INTERN HR.  CLOCK HR.

CATALOG DESCRIPTION
An in-depth study of secure electronic commerce, cryptography, passwords, certification authorities, public key infrastructure, biometrics, and digital signatures. Legal and national policy secure electronic commerce issues will be discussed.

PREREQUISITES
CSIS 112

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

1. Describe the fundamental components of a network.
2. Describe web technology.
3. Evaluate privacy and security for users.
4. Describe web server security.
5. Identify security for content providers.

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.

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>ESO</th>
</tr>
</thead>
</table>

Revised 4/15/13
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.)

- Examination/Quizzes (1-5)
- Class Discussion/Participation (1-5)
- Exercises/Projects (1-5)
- Written/Oral Reports (5)
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. Fundamental network components

II. Web Technology
   A. Web security landscape
   B. World Wide Web architecture
   C. Cryptography
   D. Secure Socket Layers (SSL) and Transport Layer Security (TLS)
   E. Passwords, biometrics and digital signatures
   F. Certification Authorities (CAs) and Public Key Infrastructure (PKI)

III. Privacy and User Security
   A. Privacy—protecting techniques and technologies
   B. Backups and antitheft
   C. Mobile code

IV. Web Server Security
   A. Physical server
   B. Web applications
   C. Host server
   D. Web service
   E. SSL server certificates
   F. Computer crime

V. Content Provider Security
   A. Web content access
   B. Client-side digital certificates
   C. Code signing
   D. Privacy policies and legislation
   E. Filtering software
   F. Digital payments
   G. Intellectual property and actionable content