COURSE INFORMATION FORM

DISCIPLINE: Computer Science & Information Systems
COURSE TITLE: Enterprise Security Management

CR.HR. 3  LECT HR. 2  LAB HR. 2  CLIN/INTERN HR. 0  CLOCK HR. 0

CATALOG DESCRIPTION
This course examines managerial aspects of computer security and risk management for enterprises. The student will acquire knowledge for accreditation, procurement, extension and operation principles for secure computing systems.

PREREQUISITES
CSIS 170

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

1. Explain the components of information security system implementation planning.
2. Differentiate between strategic organization information security planning and specialized contingency planning.
3. Describe the major components of contingency planning.
4. Develop a contingency plan.
5. Define information security policy and describe its role in an information security program.
6. Describe the functional components of an information security program.
7. Evaluate internal and external factors that influence management practices.
8. List the elements of key information security management practices.
9. Define risk management and its role in the organization.
10. Use risk management techniques to identify and prioritize risk factors for information assets.
11. Evaluate risk controls and formulate a cost-benefit analysis using existing conceptual frameworks.
12. Describe access controls.
13. Describe the security practices used to control employee behavior and prevent misuse of information.
14. Identify major national and international laws that relate to the practice of information security.
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>
<tbody>
<tr>
<td>1.</td>
<td></td>
</tr>
</tbody>
</table>
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 (1-3, 5-14)
2. Class Discussion/Participation (1-3, 5-14)
3. Exercises/Projects (1-14)
4. Written/Oral Reports (4, 11)
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. Security Planning
   A. Security Systems Development Life Cycle
   B. Strategic information security planning
   C. Specialized contingency planning

II. Contingency Planning
   A. Business Impact Analysis
   B. Incident Response Plan
   C. Disaster Recovery Plan
   D. Business Continuity Plan

III. Information Security Policy, Standards, and Practices
   A. Enterprise level
   B. Issue-specific
   C. System-specific

IV. Security Program Development
   A. Functional components
   B. Internal and external factors
   C. Security, education, training, and awareness program

V. Security Management Models and Practices

VI. Risk Management
   A. Threat analysis
   B. Risk assessment

VII. Risk Control Strategies
   A. Management
   B. Documentation

VIII. Protection Mechanisms
   A. Access controls
   B. Firewalls
   C. Intrusion detection systems
   D. Cryptography and encryption

IX. Personnel and Security
A. Information security professional certifications
B. Employee behavior
C. Misuse of information

X. Law and Ethics
   A. Modern codes of ethics
   B. National and international laws