COURSE INFORMATION FORM

DISCIPLINE
Computer Science and Information Systems

COURSE TITLE
Principles of Information Assurance

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

CATALOG DESCRIPTION
This course introduces the field of information security and assesses the information security environment within which organizations function.

PREREQUISITES
CSIS 110 with a grade of C or better

EXPECTED STUDENT OUTCOMES IN THE COURSE (ESO)

Upon completion of this course, the student will be able to:

1. Define the components of an information system.
2. Describe the security investigation phase.
3. Assess security analysis.
4. Describe and analyze logical design.
5. Describe and analyze physical design.
6. Describe security implementation.
7. Describe maintenance and change.
8. Describe and apply basic risk management concepts.
9. Describe and apply contingency planning fundamentals.
### 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>

### 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.
2. Create and defend solutions to real life business challenges.
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 (1-9)
2. Class Discussion/Participation (1-9)
3. Exercises/Projects (1-9)
4. Written/Oral Reports (1-9)
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. Introduction to Information Security
   A. History of information security
   B. Components of an information system
   C. Systems development life cycle
   D. Security systems development life cycle

II. Security Investigation Phase
   A. Need for security
   B. Threat types
   C. Attack types
   D. Law and ethics in information security
   E. Certifications and professional organizations
   F. Security Analysis

III. Risk management
   A. Risk identification
   B. Risk assessment
   C. Risk control strategies

IV. Logical Design
   A. Information security policy, standards and practices
   B. Information security blueprints
   C. Security education, training and awareness
   D. Planning for continuity
   E. Disaster recovery planning
   F. Law enforcement involvement
V. Physical Design
   A. Firewalls
   B. Intrusion detection systems
   C. Analysis tools
   D. Cryptography and encryption-based solutions
   E. Protocols for secure communications
   F. Interception of data

VI. Implementation
   A. Project planning
   B. Staffing needs
   C. Credentials of information security professionals

VII. Maintenance and Change
   A. ISO network management model
   B. Planning and risk assessment
   C. Vulnerability assessment
   D. Monitoring external and internal environments