Minnesota State University, Mankato
Curriculum Proposal

Please type or select the requested information. Print completed forms, add appropriate paper attachments, and route through MSU's curricular process for recommendations and decisions.

<table>
<thead>
<tr>
<th>College:</th>
<th>Science, Engineering and Technology</th>
<th>(Check all that apply):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department:</td>
<td>Computer and Information Sciences</td>
<td>X Undergraduate</td>
</tr>
<tr>
<td>Program:</td>
<td>Information Systems</td>
<td></td>
</tr>
<tr>
<td>Type of Change</td>
<td>COURSE PROPOSALS</td>
<td></td>
</tr>
<tr>
<td>Proposed:</td>
<td>New Course</td>
<td></td>
</tr>
<tr>
<td>Title Current:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title Proposed:</td>
<td>Information Security</td>
<td></td>
</tr>
<tr>
<td>24-Char. Abbrev:</td>
<td>Information Security</td>
<td></td>
</tr>
</tbody>
</table>

CIP # 11.040100

Course Designator and Number: ISYS 350
Number of Credits: 4

Effective Date of Change: 2007
Academic Year: 2007-08
(For Office Use Only)

Include a course or program description for the Bulletin (30-40 words maximum for courses, 100 for programs). Example:

Information system security including access control systems and methodology, business continuity and disaster recovery planning, legal issues in security, ethics, computer operations security, physical security. Security architecture and models using current standards and models.

Pre: ISYS 215 or IT 214
Fall

Rationale or Justification for change:

This new course is an integral part of our new Information Systems program and is critical to ABET accreditation for Information Systems.

***For General Education or Cultural Diversity Courses Only***

<table>
<thead>
<tr>
<th>GE Category #</th>
<th>GE Category Name (Maximum of 3 Categories)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

? For Writing Intensive Courses, attach a description of the kind and quantity of writing.

? For Upper Division Courses, include a description of the respects in which it is broad and general rather than narrow and specific, and so suitable as GE.

Attach paper copies of the following:

a. Syllabus or course outline.

b. Course's student learning outcomes associated with each GE competency or CD designation.

c. List of strategies to be used to assess students' achievement of each GE competency or CD designation.

***For New Courses***

<table>
<thead>
<tr>
<th>Course is elective.</th>
<th>Instructional Type: Lecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course is required for program</td>
<td>Information Systems (ISYS)</td>
</tr>
<tr>
<td>Pre- or Co-requisites:</td>
<td>ISYS 215 or IT 214</td>
</tr>
<tr>
<td>Other courses are being changed or eliminated. (Explain.)</td>
<td></td>
</tr>
</tbody>
</table>

Course will be offered:

X Fall Semester
X Spring Semester
X Summer Session

Course content or title is similar to courses in other departments. (Attach copy of letter of agreement with other program(s) contacted. Indicate the nature of the discussions and/or resolution of differences or potential conflicts.)

Attach paper copies of the following:

a. Syllabus or course outline.

b. Course's student learning outcomes.

c. A list of resources required to offer and support this course.

d. A description of how teaching this course will affect department staffing.

e. If 400/500 level course, an explanation of added expectations of graduate students.
### Signature Page

**Department**
- [ ] Recommended (Category/ies__)
- [ ] Not Recommended (Category/ies__)

**Comments:**

- **College Curriculum Committee**
  - [x] Recommended (Category/ies__)
  - [ ] Not Recommended (Category/ies__)

**Comments:**

- **College Dean**
  - [x] Recommended (Category/ies__)
  - [ ] Not Recommended (Category/ies__)

**Comments:**

- **General Education Subcommittee**
  - [ ] Recommended (Category/ies__)
  - [ ] Not Recommended (Category/ies__)

**Comments:**

- **Undergraduate Curriculum and Academic Policy Committee**
  - [x] Recommended (Category/ies__)
  - [ ] Not Recommended (Category/ies__)

**Comments:**

- **Faculty Association Graduate Committee**
  - [ ] Recommended
  - [ ] Not Recommended

**Comments:**

- **Graduate Dean**
  - [ ] Recommended
  - [ ] Not Recommended

**Comments:**

- **Academic Affairs Council**
  - [x] Recommended (Category/ies__)
  - [ ] Not Recommended (Category/ies__)

**Comments:**

- **Senior Vice President and Vice President for Academic Affairs**
  - [x] Approved (Category/ies__)
  - [ ] Not Approved (Category/ies__)

**Comments:**

*Revised September 2002*
Proposal: ISYS 350: Information Security

Catalog Description

In-depth examination of topics in the management of information technology security including access control systems and methodology, business continuity and disaster recovery planning, legal issues in information system security, ethics, computer operations security, physical security and security architecture & models using current standards and models.

Prerequisites

- ISYS 215(4) Fundamentals of Information Systems

Topics

Knowledge Unit 1. Security Management Practices

- Goal: to be able to demonstrate comprehension-level mastery of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify the threats, classify assets, and rate their vulnerabilities so that effective security controls can be implemented (from CBK)
- Approximate classroom hours: 3
- Mastery level 2: Comprehension
- Objectives:
  - 1.1 explain how to find an organization's information assets
  - 1.2 explain how to find threats, classify assets, and rate vulnerabilities so that effective security controls can be implemented
  - 1.3 explain how to know whether a firewall or intrusion-detection system is required
  - 1.4 explain the importance of implementing policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability

Knowledge Unit 2. Confidentiality, Integrity, Availability

- Goal: to be able to demonstrate comprehension-level mastery of how and where data can be used, how data can be accessed, and how to ensure data is accurate and reliable
- Approximate classroom hours: 3
- Mastery level 2: Comprehension
• Objectives:
  o 2.1 explain how to assign confidentiality values to data
  o 2.2 explain how to create policies used to define the standards, guidelines, and procedures used by an organization
  o 2.3 explain how to identify how and where data can be used
  o 2.4 explain why it is important that employees understand their responsibilities in the security and operation of an information system

Knowledge Unit 3. Security Architecture and Models

• Goal: to be able to demonstrate application-level mastery of concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability (from CBK)
• Approximate classroom hours: 6
• Mastery level 3: Application
• Objectives:
  o 3.1 demonstrate how to design and implement operating systems, equipment, networks, and applications so they can be monitored and secure
  o 3.2 demonstrate the ability to implement simple security with access control lists and with capability-based approach

Knowledge Unit 4. Access Control Systems and Methodology

• Goal: to be able to demonstrate application-level mastery of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system (from CBK)
• Approximate classroom hours: 6
• Mastery level 3: Application
• Objectives:
  o 4.1 write and implement a computer program that illustrates how an access control system works

Knowledge Unit 5. Applications and Systems Development Security

• Goal: to be able to demonstrate application-level mastery of controls that are included within systems and applications software and the steps used in their development. Applications refer to agents, applets, software, databases, data warehouses, and knowledge-based systems. These applications may be used in distributed or centralized environments (from CBK)
• Approximate classroom hours: 12
• Mastery level 3: Application
• Objectives:
  o 5.1 demonstrate the ability to implement an example of buffer overflow and how to guard against this problem
5.2 demonstrate the ability to implement an example of SQL injection and how to guard against this problem

Knowledge Unit 6. Telecommunications and Network Security

- Goal: to be able to demonstrate application-level mastery of structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media (from CBK)
- Approximate classroom hours: 12
- Mastery level 3: Application
- Objectives:
  - 6.1 apply responsibilities inherent in providing telecommunication services, including security, privacy, reliability and performance

Knowledge Unit 7. Cryptography/Cryptology

- Goal: to be able to demonstrate comprehension-level mastery of encryption and validation of information to ensure that it remains secure and complete, and that only authorized persons can access the encrypted data; non-repudiation (irrefutable proof that a message was created by a given individual) when used with an asymmetric key that can only belong to one person (from CBK)
- Approximate classroom hours: 6
- Mastery level 2: Comprehension
- Objectives:
  - 7.1 explain (in general terms) how information can be encrypted and validated to ensure that it remains secure and complete, and that only authorized persons can access the encrypted data
  - 7.2 explain how a "man in the middle" attack works
  - 7.3 explain how key length affects security
  - 7.4 explain how to use digital signatures to authenticate the source of a message and for non-repudiation
  - 7.5 explain the concept that encryption techniques can be subverted using many methods of attack
  - 7.6 explain the difference between symmetric and asymmetric encryption

Knowledge Unit 8. Operations Security

- Goal: to be able to demonstrate comprehension-level mastery of controls over hardware, media, and the operators with access privileges to any of these resources; mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process (from CBK)
- Approximate classroom hours: 6
- Mastery level 2: Comprehension
- Objectives:
8.1 define and explain the purpose of an intrusion-detection program
8.2 define the term "disaster recovery" and explain how it is implemented
8.3 explain how risks are assessed
8.4 explain how to identify critical information
8.5 explain how to identify threats
8.6 explain how to use countermeasures
8.7 explain how vulnerabilities are assessed
8.8 explain the importance of proper administrative and management processes that define how employees are hired/fired
8.9 explain the importance of using log files, auditing, and other forms of monitoring and observation in operations security
8.10 explain the need to put oneself "in a "cracker's shoes", then building a defensive system based on what is discovered
8.11 explain the process of penetration testing
8.12 list and explain several ways to safeguard as system against internal attack, and how to handle a successful attack

Knowledge Unit 9. Law, Investigations, and Ethics

- Goal: to be able to demonstrate knowledge-level mastery of computer crime laws and regulations, the investigative measures and techniques that can be used to determine if a crime has been committed, methods to gather evidence if it has, as well as the ethical issues and code of conduct for the security professional (from CBK)
- Approximate classroom hours: 3
- Mastery level 1: Knowledge
- Objectives:
  o 9.1 define "expert technical witness", civil law, criminal law, forensics
  o 9.2 define incident report and list important details that go into an incident report
  o 9.3 list and define several types of computer crime (e.g., access private information, destroy data, steal intellectual property)
  o 9.4 list ethical and legal issues in development, ownership, sales, acquisition, use and maintenance of computer systems and software

Knowledge Unit 10. Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)

- Goal: to be able to demonstrate knowledge-level mastery of the preservation of the business in the face of major disruptions to normal business operations; preparation, testing, and updating of specific actions to protect critical business processes from the effect of major system and network failures (from CBK)
- Approximate classroom hours: 3
- Mastery level 1: Knowledge
- Objectives:
  o 10.1 define business continuity plan
10.2 define disaster recovery plan
10.3 list the steps involved in conducting a business impact assessment

Additional topics may also be covered based on time and student interest.

**Instructional and Library**

Resources currently in place within the department and the University Library will support this new course. No new resources are required.

**Staffing**

This course will be able to be staffed by the faculty that have been designated in the proposed Department of Information Systems and Technology by the Dean of the College of Science, Engineering, and Technology, Dr. John Frey. This course will be cross-listed between the "Information Systems" and "Information Technology" programs in the new department. This course will not need assistance from faculty of the new Computer Science Department.

**Possible Textbook(s)**


Syllabus for ISYS 350: Information Security

Instructor

Name: Prof. Sample Faculty
Office: 200 Wissink Hall
Department: Information Systems and Technology, Minnesota State University, Mankato
Office hours: Monday through Friday from 1:00 to 4:00 pm
Phone: 507-389-1212
Email: sample.faculty@mnsu.edu
Course page: https://d2l.mnsu.edu/

Meeting
MTRF 10-11

Catalog Description
In-depth examination of topics in the management of information technology security including access control systems and methodology, business continuity and disaster recovery planning, legal issues in information system security, ethics, computer operations security, physical security and security architecture & models using current standards and models.

Prerequisites
- ISYS 215(4) Fundamentals of Information Systems

Topics
The following content areas will be covered.

1. Security Management Practices (about 3 hours)
2. Confidentiality, Integrity, Availability (about 3 hours)
3. Security Architecture and Models (about 6 hours)
4. Access Control Systems and Methodology (about 6 hours)
5. Applications and Systems Development Security (about 12 hours)
6. Telecommunications and Network Security (about 12 hours)
7. Cryptography/Cryptology (about 6 hours)
8. Operations Security (about 6 hours)
9. Law, Investigations, and Ethics (about 3 hours)
10. Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) (about 3 hours)

Additional topics may also be covered based on time and student interest.

**Objectives**

By the end of this course, you should be able to

- explain how to find an organization's information assets
- explain how to find threats, classify assets, and rate vulnerabilities so that effective security controls can be implemented
- explain how to know whether a firewall or intrusion-detection system is required
- explain the importance of implementing policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability
- explain how to assign confidentiality values to data
- explain how to create policies used to define the standards, guidelines, and procedures used by an organization
- explain how to identify how and where data can be used
- explain why it is important that employees understand their responsibilities in the security and operation of an information system
- demonstrate how to design and implement operating systems, equipment, networks, and applications so they can be monitored and secure
- demonstrate the ability to implement simple security with access control lists and with capability-based approach
- write and implement a computer program that illustrates how an access control system works
- demonstrate the ability to implement an example of buffer overflow and how to guard against this problem
- demonstrate the ability to implement an example of SQL injection and how to guard against this problem
- apply responsibilities inherent in providing telecommunication services, including security, privacy, reliability and performance
- explain (in general terms) how information can be encrypted and validated to ensure that it remains secure and complete, and that only authorized persons can access the encrypted data
- explain how a "man in the middle" attack works
- explain how key length affects security
- explain how to use digital signatures to authenticate the source of a message and for non-repudiation
• explain the concept that encryption techniques can be subverted using many methods of attack
• explain the difference between symmetric and asymmetric encryption
• define and explain the purpose of an intrusion-detection program
• define the term "disaster recovery" and explain how it is implemented
• explain how risks are assessed
• explain how to identify critical information
• explain how to identify threats
• explain how to use countermeasures
• explain how vulnerabilities are assessed
• explain the importance of proper administrative and management processes that define how employees are hired/fired
• explain the importance of using log files, auditing, and other forms of monitoring and observation in operations security
• explain the need to put oneself "in a "cracker's shoes", then building a defensive system based on what is discovered
• explain the process of penetration testing
• list and explain several ways to safeguard as system against internal attack, and how to handle a successful attack
• define "expert technical witness", civil law, criminal law, forensics
• define incident report and list important details that go into an incident report
• list and define several types of computer crime (e.g., access private information, destroy data, steal intellectual property)
• list ethical and legal issues in development, ownership, sales, acquisition, use and maintenance of computer systems and software
• define business continuity plan
• define disaster recovery plan
• list the steps involved in conducting a business impact assessment

Students with Disabilities

Every attempt will be made to accommodate qualified students with disabilities. If you are a student with a documented disability, please see me as early in the semester as possible to discuss the necessary accommodations, and/or contact the Disability Services Office at (507) 389-2825 (V) or 1-800-627-3529 (MRS/TTY).

Textbook

This course will use one more more of the following textbooks:


Additional readings may be assigned by the instructor.

**Grading**

Your course grade will be based on:

[Varies by faculty]

If you receive 90% or more of the possible points, you are guaranteed an A, 80% a B, et cetera. However, a score just below the grade cutoff will not necessarily earn the higher grade. Therefore, you should try to attain a score well above the cutoff to achieve the grade you want.

**Exams**

The exams will cover reading assignments, lectures, and class discussion. It is your responsibility to remember the exam schedule. If you forget to attend an exam or are more than ten minutes late for the exam, you must forfeit the grade for that exam.

You may take the exam at an alternate testing time if you participate in a university-sponsored activity that requires your attendance. You must arrange with the instructor at least a week ahead of the exam date.

If you miss an exam because of illness or family emergency, you may arrange with the instructor for a makeup exam. You must produce written proof of the reason you cannot take a test at the normally scheduled time.

**Programming Assignments**

[Varies by faculty]

**Homework**

[Varies by faculty]

**Class Policies**

**Attendance**
Late Policy

Academic Honesty

Please be aware that the University's policy for Academic Honesty appears in the Student Handbook. Each student is expected to have read this material. If you do not understand what is meant by this policy, or if you are confused by terms such as plagiarism, cheating, or collusion, please discuss this policy with me, your advisor, or another faculty member as soon as possible. I absolutely require that each student in this class will fulfill his or her academic obligations in a fair and honest manner.

Anything that you observe in other students that is of questionable integrity should be brought to my attention. You may do so anonymously if you desire (e-mail works fine for this).

For the writing of papers and program design documents, it is quite easy to define cheating in terms of traditional definitions of plagiarism; however, for the writing of computer programs, the distinction is not as obvious to many students. It is easy to use the English paper comparison when thinking about what is appropriate and what constitutes dishonest academic work when writing computer programs. Like writing a paper, you may discuss general ideas with fellow students.

You must write each programming assignment yourself. It is acceptable to discuss logic and other strategies such as the number of variables or methods, but it is NOT acceptable to show another student even a single line of your program until after the due date.

Protect your programming assignments. If another student obtains a copy of your program even though you are unaware of the infraction, you are still guilty of collusion. Do not leave an ACC workstation unattended, even for a little while. Other students monitor may your patterns and, while you are out for even a few seconds, walk up to your workstation and email a copy of your program to themselves! You should also be careful where you leave paper copies of your program. Do not leave files on ACC computers. A trash receptacle anywhere near the ACC is likely to be rummaged. Make sure you log out of the course web site when you are done using it, close all browser windows, and log out of the system.

I strongly suggest you consult your student handbook or talk with me if you are unsure as to what is acceptable academic behavior. The consequences are quite severe. Academic misconduct will automatically result in my informing Judicial Affairs, a division of Student Affairs, of the misconduct. This misconduct usually results in a failing grade for the course. (And it can be worse.)
Specific items that will be considered cheating on programming assignments are:

- Turning in work done by somebody else as your own (with or without that person's consent). This includes turning in a copy of something that can be mechanically transformed into a copy of someone else's work. Do not try to disguise cheating by simply modifying someone else's work and calling it your own. I use software that detects this type of cheating.
- Allowing someone else to turn in your work as his or her own work. This includes allowing fellow students access to your copy, even without your knowledge or consent.
- Using a solution developed by a student in a previous semester or another section.

Errors in Grading

If something has been graded incorrectly, or if a grade has been recorded incorrectly, you must request a correction no later than one week after the grade has been posted. Course grades are final, and cannot be changed unless there has been a substantial error.

Grades are based on the quality of your work and on how well you are prepared for class. While working hard is admirable, your grade will not be based on how much time you spent working on an assignment or preparing for an examination.

Weather and Other Problems

In the event inclement weather conditions or other problems cause class not be held on a given day, any work due for that day will be due at the next class meeting. It will not cause any other changes in the schedule. Weather-related closings will be made by the university and announced on the Twin Cities and local media. You can call the MSU WeatherLine at 2463 for weather-related closing or cancellation information.

Classroom Etiquette

Please turn off or silence your cell phone or pager while in class. If you are expecting an urgent call (such as from your sick child):

- Use the "silent" mode of your cell phone or pager.
- Sit right next to the door.
- Leave the room as quietly as possible when you receive the call, so you do not disturb other students.