



COURSE SYLLABUS

Course Name: IA 542: Information System Security for Managers

Instructor: _____

Office Hours: _____

Office: _____ Telephone: _____ FAX Number: _____

Internet/E-Mail Address: _____

Opening Statement: This document is meant to serve as an information statement for your reading and use for this course. It also serves to identify timelines, requirements etc. The instructor reserves the right to make any additions/deletions or changes to this document or course as deemed necessary.

Course Description: Provides the manager with a broad overview of the threats to the security of information systems, the responsibilities and the basic tools for information security, and areas of training and emphasis needed in organizations to reach and maintain a state of acceptable security. Included are topics such as management's role in information security, foundations of information security, and privacy, regulatory, legal and policy issues. The course provides an introduction to the components of information security and provides an overview of hardware, software and firmware components of an information security system and their integration into an organization's information system operations for information security managers.

Course Prerequisites/Corequisites: None

Course Objectives: Upon successful completion of this course, students should be able to:

1. Demonstrate foundation knowledge of information security's role in the organization
2. Demonstrate knowledge of the profession, its organizations, goals and leadership roles, literature/publications, issues, and research foundations.
3. Demonstrate knowledge of various information security positions, responsibilities, qualifications, and role of professional certification.
4. Demonstrate knowledge of the foundations of information security including legal, regulatory and policy issues, understanding general threats against information systems, management responsibilities and liabilities, policy development, risk management, privacy, and encryption policies in a global environment.
5. Outline the components of a comprehensive information security program and identify policies, procedures, and staffing requirements for selected components.

Student Requirements:

Text and Handouts: Students will receive reading assignments that may include handout material, and/or research searches, and are responsible to read and act on the material as directed.

- Primary Text: Computer Security Handbook, fourth edition ed. Bosworth, Seymour, Kabay, M. E. pub. Wiley, Part 1, Part 7 and Part 8 (Required text for the entire MLS/IS program)
- Complementary text: Writing Information Security policies Barman, Scott pub New Riders
- Supplementary text: Enterprise Security – the Manager's Defense Guide Clark, David Leon pub Addison Wesley, Part 1 and Part 2 (Required supplementary text for the entire MLS/IS program)

- Various handouts as determined by your instructor

Assessment and Evaluation: The final grade for the class will be based on the following requirements as directed by your instructor:

- Team based development, presentation and evaluation of a final project, including a complete bibliography, and areas of further research will account for 40% of each student's grade.
- Student participation in class activities and individual assignments will account for 20% of the student's grade.
- Mid term and final exams will account for 20% each of the student's grade

All points are cumulated, converted to percent form, and converted to letter grades based on this straight scale: 94% and above, A; 90% and above A-; 87% and above, B+; 84% and above, B; 80% and above, B-; 77% and above, C+; 74% and above, C; 70% and above, C-; 67% and above, D+; 64% and above, D; 60% and above, D-; below 60%, E.

Notes on Requirements and Grading:

- Class sessions will involve interactive approach and student activities. Students are expected to have textbooks and other assigned materials with them. Students should not expect to excuse lack of participation because they did not have their textbooks, or other misc. materials including disks, or backup files (in case a file is lost or damaged).

Attendance at all times is required of all students, and failure to attend is considered lack of participation. Verifiable emergencies will only be considered.

General Policies:

- Attendance and punctuality is mandatory. Class will start at the given time.
- All cell phones, pagers and any other miscellaneous forms of communication must be turned off prior to the start of class and remain turned off until after class is completed. This is out of courtesy for the other students and to insure an un-interrupted class.
- Speak to the instructor as needed.
- Students should comply with expectations for use of the college and university laboratories and classrooms, with standards for fair information practices, and with licensing provisions of the software in use.
- Students must complete their own work when given an individual assignment. During team-based assignments they will work with one another to solve problems and develop the team-based project. Students who submit the work of other students, including companies and organizations, as their own (Plagiarism), will be penalized to the full extent permitted by University policy.
- Late work is not accepted. Oral presentations may not be made up.
- Inability to prepare for an assignment and poor time management are not considered valid reasons for late work or re-scheduling. In addition, students must back up work, for lost disks or damaged files is not sufficient reason for extensions.
- Class sessions may involve some lecture, Caucus/Online, with mostly group-facilitated activities. Therefore, it is the student's responsibility to have completed the scheduled reading assignment prior to the class session. The student must also complete the assigned chapter activities/projects during scheduled class sessions. Active listening is also part of learning. Students are expected to have textbooks and other needed materials with them. Students should not expect to excuse lack of participation because they did not have their textbooks, and/or other materials.
- Be prepared to conduct discussions online through Caucus or another form of online viewing such as e-mail.
- Students are expected to complete all assignments in a neat, accurate and professional manner; otherwise, materials will not be accepted. This includes the word processing of all assignments with

spell checking and proofreading mandatory. This also includes stapling your materials if needed so they do not become loose.

- All assignments will be graded for compliance to the author's directions.
- Final grades will not be given in person, by telephone, e-mail, fax or any other communications median except that of University standard written grading at the end of the semester.
- Attendance/participation is required therefore it is the student's responsibility to obtain all missed instruction from another class member. The instructor will not repeat instructions or demonstrations for any student missing class. Keep in mind that attendance is mandatory.
- A grade of "I" will be given only in accordance with Eastern Michigan University's Graduate school guideline.
- By University policy the instructor has the option of failing a student who does not attend class on the day of the final examination set by the university. Attendance at final periods during which students are presenting their work is required of all students and failure to attend is considered lack of participation.

Course Content and Schedule: This schedule is an approximate timeline for the student.

Week 1

- **Introductions**
- **Course review and intro Introduction to information security**
- **Application of information security in eBusiness**

Week 2

- **Information security in the context of the law**
- **Information security in the context of the organization and business drivers**
- **Regulatory issues - introduction**

Week 3

- **Project and team selection**
- **Ten areas of the CISSP common body of knowledge**

Week 4

- **Role of the security manager**
- **Describing security events**

Week 5

- **Privacy issues**
- **International use of encryption**

Week 6

- **The role of standards**
- **BS7799/ISO17799**
- **The Common Criteria – ISO15408**

Week 7

- **Mid Term Exam**

Week 8

- **HIPAA**
- **GLBA**
- **Sarbanes-Oxley**
- **The Patriot Act**

Week 9

- **Awareness programs**
- **Training programs**

Week 10

- **Security policy development**
- **Internal standards, practices and guidelines**
- **Developing a security plan**

Week 11

- **Risk management**

Week 12

- **Introduction to security architectures: the manager's view**
- **Extended information security framework**

Week 13

- **Project Work Session**

Week 14

- **Team Project Presentations and Business documents turned in.**
***No late projects or presentations will be accepted.

Week 15

- **Final Exam**

Overview of the Semester Project:

Grading: There are 40 points for the semester project and presentation.
There are 60 points for participation in class activities, assignments and exams.

The final project will be developed in teams with a team leader giving an oral presentation of the project to the class. Each student will write a portion of the team report and will be responsible for his or her contribution to the overall project. Each team will provide a final written team report with each team member's contribution identified individually.

More on Planning the Project:

Each team will develop a word processed business document, **completed in APA or MLA format**, which will be presented using PowerPoint and will at minimum include the following:

- Cover page with all Team Members Names, etc.
- Table of contents
- Names of Team members and their individual responsibilities
- The Team Leader is responsible for submitting each team member's participation and contributions to the project, which is to be included in the final document package.
- Statement of the problem. What are the issues you are dealing with and why.
- Summary statement focusing on the organization.
- Solution Statement: How will you deal with the problems, issues, etc.
- Bibliography
- Areas of further research, including a preliminary research proposal on a significant information security problem related to Systems Auditing.

The focus of the final project is to develop a comprehensive security program for your organization or for a fictitious one. The security program should include the following components at a minimum:

- Policies, standards and guidelines
- Training and awareness
- Security architecture design
- Risk management
- Security plan
- Funding plan

If your target organization is subject to regulatory requirements, these must be addressed in your program. You are not required to create the elements needed to implement the program, only to develop the program itself. You will present your plan in teams to the rest of the class in the context of “selling” the project to management. The class will critique the plan and determine if it should be approved for implementation. The class members evaluating the plan will play the role of the target company’s management.

You will need to use NON-CONFIDENTIAL data for your project. Please do not UNDER ANY CIRCUMSTANCES use data that would breach any confidentiality.

Final Project Documentation: A complete project with two hard (paper) copies being submitted as a total business document. Including a copy of the PowerPoint presentation. All projects must be secured in a lightweight (paper) binder.

Academic Dishonesty

In any university-level course, a statement of policy recognizing academic dishonesty should be unnecessary. However, it should be noted that the policy of the Department of Business and Technology Education is that, any student found to have engaged in any activity constituting academic dishonesty, will receive and “E” for the course in which the activity occurred. This policy relates to all forms of work associated with the course requirements, including examinations, quizzes, laboratory work, and all other assignments. It is the student’s responsibility to review the pages(s) of the graduate catalog in order to determine those activities, which constitute academic dishonestly at Eastern Michigan University, which include both cheating and plagiarism... This policy will be strictly enforced,

Definition reminders:

Assist” To help or support.” The American Heritage College Dictionary, 3rd Edition, page 83.
Cheat “To act dishonest, practice fraud. To violate rules deliberately.” The American Heritage College Dictionary, 3rd Edition, page 239.

DUE: Accepted only during the class session during which you present your project.

Print all components of the finished project, tables, queries, forms and reports. These should be assembled in logical order. Grading also includes: Correctness and accuracy of work, contents, professionalism, APA formatting and other factors emphasized in the course or in the final project description... The team leader’s evaluation of each individual team member is also to be submitted at this time.

*****The Instructor reserves the right to make any additions/deletions or changes to this syllabus as deemed necessary.**

