



## COURSE SYLLABUS

### Course Name: IA 544: Administrative Information Security Procedures

Instructor: \_\_\_\_\_

Office Hours: \_\_\_\_\_

Office: \_\_\_\_\_ Telephone: \_\_\_\_\_ FAX Number: \_\_\_\_\_

Internet/E-Mail Address: \_\_\_\_\_

---

**Course Description:** Development and evaluation of administrative policies and procedures required to administer an information system in a secure environment will be explored. Emphasis will be on writing information security policies that comply with federal information security guides and directives as well as applicable regulations, developing business continuity/disaster recovery and incident response plans, developing security awareness programs, and risk management.

**Course Prerequisites:** IA 542

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

1. Develop administrative policies and procedures required to administer an information system in a secure environment.
2. Develop plans for business continuity/disaster recovery and incident response.
3. Establish support objectives in areas such as human resources/personnel, training, and end-user support systems.
4. Develop an information security awareness program.
5. Develop and apply criteria by which to evaluate the effectiveness of policies, and procedures.
6. Demonstrate an understanding of the principles of information system risk management.

**Student Requirements:** The overall goal of this course is to provide a practical educational experience in the fundamentals and application of administrative information security procedures and systems. The highest level of student gain will be achieved by participation in the team-based directed exercise(s) and by participation in classroom activities as well as individual assignments. Each student will be required to actively participate in the class exercises and contribute to the overall team effort. Students will be given reading assignments as well as assigned written projects.

**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. The required text is:

- Primary Text: Computer Security Handbook, fourth edition ed. Bosworth, Seymour, Kabay, M. E. pub. Wiley, Parts 4 and 6 (Required text for the entire MLS/IS program)
- Complementary text: Writing Information Security policies Barman, Scott pub New Riders
- 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 an interactive team 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.

**General Policies:**

- **SPEAK TO THE INSTRUCTOR IF YOU ARE HAVING DIFFICULTY MEETING COURSE DEADLINES OR NEED ASSISTANCE.**
- 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.
- **No late work will be 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. Lost disks or damaged files are not sufficient reason for extensions.

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

**Week 1:**

- **Introductions**
- **Course review and intro Introduction to information security**
- **Human factors in the information security environment**
- **Review of regulatory requirements**

**Week 2:**

- **The roles and structures of policies, procedures, standards and guidelines**
- **Developing information security policies that address organizational and regulatory requirements**

**Week 3:**

- Sources of policy, regulatory and other industry standard references
- Specific policy areas: rogue code, ethics, internet acceptable use, identification and authentication, email use, encryption

**Week 4:**

- Policy compliance and enforcement
- Policy review and evaluation

**Week 5:**

- Operations security, production controls, application security planning, implementation and evaluation

**Week 6:**

- Developing security awareness programs
- Developing and applying appropriate metrics to measure the success of an awareness program

**Week 7:**

- Mid Term Exam

**Week 8:**

- Business continuity planning
- Disaster recovery

**Week 9:**

- Incident response
- Working with law enforcement

**Week 10:**

- Risk management approaches

**Week 11:**

- Conducting a formal incident root cause analysis (post mortem)

**Week 12:**

- Conducting a formal risk analysis

**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 the subjects covered this term.

The focus of the final project is to develop a set of top level information security policies OR a business resumption/disaster recovery plan OR an incident response plan OR an information security awareness program for a fictitious organization. Students working in teams will define the target organization in detail including such elements as:

- Size
- Line of business
- Number and types of locations
- Risks to the organization

If your target organization is subject to regulatory requirements, these must be addressed in your program. 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.

**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 and other factors emphasized in the course. The project must be complete when turned in.

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