

GROSSMONT COLLEGE

Official Course Outline

ADMINISTRATION OF JUSTICE 260 - INFORMATION SECURITY

1. <u>Course Number</u>	<u>Course Title</u>	<u>Semester Units</u>	<u>Hours</u>
AOJ 260	Information Security	3	3 hours lecture

2. Prerequisites

None.

Corequisite

None.

Recommended Preparation

None.

3. Catalog Description

This course focuses on procedures, policies, and equipment designed to protect private and government proprietary and intellectual information and investigate breaches of security. Also, this course examines the collection, analysis, and preservation of digital evidence from computer crime scenes. Emphasis is placed upon knowledge of investigative principles, applicable case law, physical and technical security, security management responsibilities, and countermeasures designed to protect and analyze information collection, storage, processing, and transmission.

4. Course Objectives

The student will:

- a. Define information security (infosec).
- b. Describe information security functions.
- c. Describe the importance of collecting and preserving digital evidence.
- d. Identify threats to proprietary information.
- e. Recognize how computers are used as tools to commit crimes.
- f. Develop tactical and strategic information protection plans.
- g. Demonstrate ability to respond to computer crime incidents without damaging electronic evidence.
- h. Evaluate information security policies and procedures.
- i. Analyze data to identify vulnerable infosec areas and take corrective action.
- j. Demonstrate the ability to accurately and thoroughly conduct and document a high-tech investigation.
- k. Discuss constitutional law related to searching and seizing of digital evidence.
- l. Evaluate statutory and case law related to computer crimes.
- m. Demonstrate ability to apply knowledge of computer forensic analysis on disk media.
- n. Identify, analyze, and develop solutions to problems in security management and computer investigations.
- o. Demonstrate ability to work collaboratively in a group setting.
- p. Utilize computer technology and access information via the Internet as appropriate.
- q. Conduct research appropriate to the discipline.
- r. Evaluate personal and professional ethical standards.

5. Instructional Facilities

- a. Access the internet.
- b. Standard classroom.
- b. Computer lab for "hands-on" activities.

6. Special Materials Required of Student

Electronic storage media.

7. Course Content

- a. Introduction to information security (infosec).
- b. Functions, duties, responsibilities of an infosec manager.
- c. Threats to information.
- d. Tactical and strategic information security planning.
- e. The infosec organization.
- f. Specific information protection applications.
  - (1) Personal security.
  - (2) Physical security.
  - (3) Computer security.
  - (4) Operations security.
- g. Future challenges for the information security manager.

8. Method of Instruction

- a. Lecture, discussion, group projects and audio visual materials as appropriate.
- b. Qualified guest speakers may be invited to lecture on their respective fields of specialization.
- c. Field trips to local public safety agencies and security organizations may be arranged.

9. Methods of Evaluating Student Performance

- a. Participation.
- b. Written assignments.
- c. Periodic examinations.
- d. Research assignments.
- e. Group projects.
- f. Oral presentations.
- g. Written final examination.

10. Outside Class Assignments

- a. Reading in required text.
- b. Critical-thinking and problem solving exercises.
- c. Research paper.
- d. Preparation for oral reports.

11. Texts

- a. Required Text(s):  
Britz, M.T. Computer Forensics and Cyber Crime: An Introduction. Upper Saddle River, NJ: Pearson-Prentice Hall, 2003.
- b. Supplementary texts and workbooks:  
None.