INF 711: Security Policies
University at Albany, State University of New York
Center for Information Forensics and Assurance
Fall 2005

Instructor Information
Name: Sanjay Goel
Email: goel@albany.edu
Phone: (518) 442-4925
Office Location: BA 310b
Office Hours: Monday 12:30-2:00 or by Appointment

Class Information
Time: 8:00am-5:00pm
Location: CIFA Teaching Laboratory (ES-B19)
Dates: December 8-9, 2005
Credit(s): 1
Call #: 8838
Available Lab(s): CIFA Teaching Laboratory

Course Overview
This course provides students with an introduction to information security policies. Students will be introduced to sociological and psychological issues in policy implementation in general and then provided a focused dialogue on information security specific policies. The class discusses the entire lifecycle of policy creation and enactment and presents the students with issue specific policies in different domains of security. The structure of the policy is also discussed to assist the students design and modify policies. Several examples from different domains are incorporated in the curriculum to assist the students learn in context of real life situations.

Course Prerequisites
The prerequisite or co-requisite is the INF 710: Information Security Risk Assessment course. It is assumed that students will have a general background of computer security. It would be helpful if students have some knowledge of the following topics:
Security Vulnerabilities
Network Architecture
Software Design

Learning Objectives
Students should be able to:
Understand the lifecycle of policy enactment
Create and modify security policies
Create a dissemination plan for the policy
Critique the security policy for its effectiveness and completeness

Course Format
Each class comprises of theoretical elements as well as case analysis. Please come prepared with the readings since the class will move at a brisk pace. Readings will be announced approximately a week before class. All the information will be posted on this webpage. Students are expected to use critical thinking skills as they go through the material rather than accepting facts at face value.

The class should require approximately 40 hours of work. This should work out to roughly 15 hours of lecture, discussion, quiz time, and case study work, 3 hours of break, 12 hours for the project and 10 hours of readings.

Grading
Quizzes: 30%
Class Participation (case analysis/discussion): 20%
Project: 50%

Quizzes
A quiz will be offered at the end of each day of class. These quizzes will be multiple choice and will encompass the material learned earlier in the class.

Class Participation
Students will be expected to participate actively in class discussion and in the case studies. For each case study, groups will be formed which will analyze the case and present their analysis to the entire class. The groups will be graded based on their performance. Clear instructions will be provided on the scope of the discussion and arguments.

Project
The students will get a take home project at the end of the class on the second day which will involve the creation of a policy. Students need to complete and submit this via email to the instructor. More details will be given during the class.

Reference Books
Reference: Writing Information Security Policies by Scott Barman

Course Schedule

Date	Topics	Readings
12/08/05	Unit 1 General Overview of Policies Security Policy Lifecycle Unit 2 Security Policies I Network, Communications, Web, etc.	TBD
12/09/05	Unit 3 Security Policies II Software and Data Unit 4 Security Policy: Audit and Compliance Unit 5 Case Study	TBD