ITM 641: Information Security Policies Syllabus

Sanjay Goel
School of Business
University at Albany, State University of New York

INSTRUCTOR INFORMATION

Name: Sanjay Goel
Email: goel@albany.edu
Phone: (518) 442-4925
Office Location: BA 310b, University at Albany
Office Hours: TBD

CLASS INFORMATION

Time: N/A
Location: Online
Dates: TBD
Credit(s): 3
Call #: TBD

RESOURCES

Course Website: The course website is located at the West Lafayette Open Campus Blackboard web system: http://www.itap.purdue.edu/tlt/blackboard/open.cfm
Click on "Log On" and sign in using the User name and Password assigned to you via email.

Readings: Reference readings will be posted at the end of each presentation. Available readings will be accessible via http://eres.ulib.albany.edu
You must click on "Electronic Reserves & Reserve Pages" and then type in "ITM641" in the empty box. Click under the Course Number section (which is hyperlinked) you will be asked to input a password. The password to access this information will be provided via email and is case-sensitive. All of the readings is divided by Unit and contains readings in pdf format or web links to readings.

Reference Books:

Writing Information Security Policies by Scott Barman

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 Format

The class is taught in an online format where the students can learn at their own pace. The learning environment is very interactive containing, instructor video, discussion groups, and interactive quizzes. Students learn the basic elements of security policies as well as the process of enacting security policies. It is assumed that the students have a good understanding of risk analysis, which will assist the students in understanding security policies. To illustrate the concepts context is build through use of examples and case studies. Students are expected to use critical thinking skills as they go through the material rather than accepting facts at face value. Even though the course is spread over several weeks, it is important that students stay on schedule so that they can participate with other students in discussions. The class should require approximately 120 hours of work. This should work out to roughly 45 hours of video and lecture material, 6 hour worth of quizzes, 9 hours for discussion postings, 36 hours for the final project,

and 24 hours of readings. 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.

Course Prerequisites

The prerequisite or co-requisite is the ITM 640 (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:

1. Computer Networks
2. Computer Architecture
3. Software Design
4. Risk Analysis (assets, threats, vulnerabilities, and controls)

Learning Objectives

Students should be able to:

1. Understand the lifecycle of policy enactment
2. Develop and modify security policies
3. Create a dissemination plan for the policy
4. Critique a security policy for its effectiveness and completeness

ASSESSMENT & GRADING

Academic Integrity Compliance: Students MUST comply with all University standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** If a student is discovered to NOT comply with academic integrity standards, the student will be reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive either a warning, be told to rewrite the plagiarized material, receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Examples of violations include: Giving or receiving unauthorized help before, during, or after an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), Submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being (and has in the past been) submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (for example, the words, ideas, information, code, data, evidence, organizing principles, or style of presentation of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, the purchase of prepared research, papers, or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources,

the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations.

If you ever have any questions about whether you could be violating academic integrity standards - ASK!

Grading Rubric

Quizzes/Exams (20%) – Please work individually on all quizzes/exams. Two exams will be offered after during the course. Please go to the Toolbar and click "Other Tools". Select "Assessments" and you will see the exams. This will be graded automatically via Blackboard.

Discussion Postings (30%) – Even though this is an online course, it is expected that students will be able to learn from each other and participate in a discussion. To promote this, you will be assigned discussion postings, which will be graded. Discussions will be able to be created and viewed by going to the "Discussions" link on the top right hand corner of the page. In addition to discussion postings, responses to other student posts are also required. Initial postings will generally be due on Wednesday and responses to other postings should be up by the Sunday of that week.

Project (50%) – The students will get a project to complete at the end of the class creating a security policy.. The project will be due ***INSERT DATE*** through the Blackboard interface (taking into account the other course students are also taking). To do this, go to "Other Tools" on the Toolbar on the right-hand corner and click on "Assignments". More details will be given during the course.

COURSE SCHEDULE

Unit	Topics	Readings
1	General Overview of Policies, Policy Lifecycle, and Writing Security Policies	TBD
2	Information Classification and Privacy Policies	TBD
3	Network Security and Email Policies	TBD
4	Application, Operating System and Software Security Policy	TBD
5	Encryption and Key Management Policy	TBD
6	Exam I	TBD
7	Disaster Recovery and Business Continuity	TBD
8	Security Policy: Audit and Compliance	TBD
9	Acceptable Use Policies and Training /Awareness	TBD
10	Security Policy: Enforcement and Effectiveness	TBD
11	Internet Censorship (Case Analysis)	TBD
12	Intellectual Property Protection (Case Analysis)	TBD
13	International Cooperation in Cyber Crime (Cyber Crime Treaty)	TBD
14	Exam II	TBD

Detailed Schedule

Week 1
Theme General Overview of Policies, Policy Lifecycle, and Writing Security Policies

Comment [DP1]: I wasn't sure about all the topics for security policies or the detailed topic descriptions. Does audit and compliance also include legislation discussion?

Instead of encryption policy maybe we should have a cryptography policy which includes encryption and discussion of key management?

Also based on a SANS document other areas include for the technical policy sections: administration/management, security devices (anti-virus, firewall, IDS), peripherals (copiers, fax, printers, VoIP, phones, usb, cd, dvd's), physical security, network security, application security, OS security and business planning / administration security, which includes the following:
Acceptable Use
Acquisition / Procurement Assessment
Business Continuity
Disaster Recovery
Email Usage
Audit
Customer Authentication
Privacy
Third-Party / Service Provider
Patching
Risk Assessment
Information Sensitivity / Privacy
Information Management (including retention policies)
Password
Access Reverification

Maybe we can discuss this?

Topics Policy Structure
Exercises

Week 2
Theme Information Classification and Privacy Policies
Topics
Exercises

Week 3
Theme Network Security and Email Policies
Topics
Exercises

Week 4
Theme Application, Operating System and Software Security Policy
Topics
Exercises

Week 5
Theme Encryption and Key Management Policy
Topics
Exercises

Week 6
Theme Exam I
Topics
Exercises

Week 7
Theme Disaster Recovery and Business Continuity
Topics
Exercises

Week 8
Theme Security Policy: Audit and Compliance
Topics
Exercises
.

Week 9
Theme Acceptable Use Policies and Training /Awareness
Topics
Exercises

Week 10
Theme Security Policy: Enforcement and Effectiveness
Topics Metrics and data collection
Exercises

Week 11
Theme Internet Censorship (Case Analysis)

Topics
Exercises

Week 12
Theme Intellectual Property Protection (Case Analysis)
Topics
Exercises

Week 13
Theme International Cooperation in Cyber Crime (Cyber Crime Treaty)
Topics
Exercises

Week 14
Theme Exam II
Topics
Exercises