Syllabus: INT 678 Seminar in INT/Management of Information Security

Instructor Information
Name    Keyu Jiang, Ph.D.
Department    Information Networking and Telecommunications
Contact information:   email:   kjiang@fhsu.edu
                      Phone:  785.628.4684
                      Fax:  785.628.4098
                      Web Site:   blackboard.fhsu.edu

Online Resources:
Please refer to https://sites.google.com/site/professorjiang/ia-links.

Course Description:
This course is designed to give students an introduction to management of information security. It covers 6 Ps: Planning, Policy, Programs, Protection, People and Project management. This course examines the skills to identify and prioritize information assets and threats to information assets. This course will also examine the techniques to define an information security strategy and architecture, and to plan for and respond to intruders in an information system. Course work will include the study of legal and public relations implications of security and privacy issues. Additional discussion will be given to a disaster recovery plan for recovery of information assets after an incident. PR MIS 101 or PERM

Please see the tentative course schedule for the detail coverage.

After completing the course, students will be able to:
- Describe threats to information security;
- Identify methods, tools and techniques for combating these threats;
- Identify types of attacks and problems that occur when systems are not properly protected;
- Explain integral parts of overall good information security practices;
- Identify and discuss issues related to access control;
- Describe the need for and development of information security policies, and identify guidelines and models for writing policies;
- Define risk management and explain why it is an important component of an information security strategy and practice;
- Describe the types of contingency plan and the steps involved in developing each plan;
- Identify security issues related to personnel decisions, and qualifications of security personnel.

Prerequisites:
Basic computer literacy, MIS 101, or approval of the instructor
Text:


**Online Resources**: please refer to [https://sites.google.com/site/professorjiang/ia-links](https://sites.google.com/site/professorjiang/ia-links).

**Course Requirements**: Complete all online assignments, quizzes, and exams, and participate in online problem solving and discussion. All instruction will take place via the Blackboard website. Each week, you will be directed toward new course materials, assignments, discussions and assessments. Students are required to do course work at the level of the degree for which they are enrolled. This is especially true for the written assignment for this course.

For Graduate Students: You will be required to perform at a level significantly higher than that required of undergraduate students. Your work will be required to show mastery of the subject matter; your assignments will require thorough research and demonstrate a comprehensive, synthetic viewpoint of the subject matter and original, important thought. Your assignments will be graded using higher standards than the standards used in grading upper division undergraduates taking this course.

Graduate students are required to write a research paper. Papers should be at least 15 pages long, single spaced, 12 font of Time New Roman, in APA format with at least 15 references. The instructor reserves the right to require revisions to the paper. This is a required assignment for all students enrolled in graduate sections of this course. Failure to complete a satisfactory research paper will prevent the student from passing the course.

**Evaluation**: Will be based on quizzes, assignments, discussion participation, a paper and exams as follows:
For undergraduate students:

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussion</td>
<td>12.5%</td>
</tr>
<tr>
<td>4 Quizzes</td>
<td>12.5% each</td>
</tr>
<tr>
<td>Midterm</td>
<td>12.5%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>25%</td>
</tr>
<tr>
<td>Research Paper</td>
<td>not required</td>
</tr>
</tbody>
</table>

For graduate students:

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussion</td>
<td>10%</td>
</tr>
<tr>
<td>4 Quizzes</td>
<td>10% each</td>
</tr>
<tr>
<td>Midterm</td>
<td>10%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>20%</td>
</tr>
<tr>
<td>Research Paper (required)</td>
<td>20%</td>
</tr>
</tbody>
</table>

The grading scale is as follows:
A=90-100
B=80-89
C=70-79
D=60-69
U=0-59

**Attendance:** Attendance will be based on your participation in online discussion and on your timeliness in turning in assignments. You should check the web site at least once a week. New announcements and assignments will be posted timely, and the assignments will usually be due **before the midnight on the following Monday, if not otherwise specified.** If you have an emergency that will keep you from getting an assignment done on time, send an email to let me know.

**ADDITIONAL INFORMATION / INSTRUCTIONS**
Some additional readings included in the course schedule may require you to use the library's website as well. I also reserve the right to add or change readings during the course of this class. FHSU’s Blackboard system will serve as the backbone of this class. Since you have enrolled for this virtual course, I assume you are proficient enough with Blackboard to use it. If you are not, it is your responsibility to learn the login and navigation procedures of the Blackboard system. Please call 1-800-628-FHSU for technical support or e-mail support@fhsu.edu. As the instructor of this class, I have no technical expertise in Blackboard. Any technical questions should be directed to the Support staff, and not me.

**ACCESSIBILITY**
Fort Hays State University will ensure that no qualified person with a disability is denied the benefits of, excluded from participation in, or otherwise subjected to discrimination because of inaccessibility of education programs and activities operated by Fort Hays State University. To obtain information as to the existence and location of services, activities, and facilities that are accessible to persons with disabilities, contact the Director of Affirmative Action.

**ACADEMIC HONESTY**
Membership in the FHSU learning community imposes upon the student a variety of commitments, obligations and responsibilities. It is the policy of FHSU to impose sanctions on students who misrepresent their academic work. Classroom instructors will select appropriate sanctions or other designated persons consistent with the seriousness of the violation and related considerations.

Examples of academic dishonesty include but are not limited to: (1) Plagiarism, taking someone else’s intellectual work and presenting it as one’s own (which covers published
and unpublished sources). Using another’s term paper as one’s own; handing in a paper purchased from an individual or agency; submitting papers from living group, club or organization files; or using another’s computer program or document are all examples of plagiarism. Standards of attribution and acknowledgment of literary indebtedness are set by each discipline. In political science, students must cite all work from which they take any recognizable length of work, including but not limited to phrases, sentences, and data. Students should consult with their department or with recognized handbooks in their field if in doubt. (2) Cheating is unacceptable in any form. Examples include consultation of books, library materials or notes during tests without the instructor’s permission; use of crib sheets or hidden notes; intentional observation of another student’s test; receipt of a copy of an exam or questions or answers from an exam to be given or in progress; substitution of another person for the student on an exam or another graded activity; deliberate falsification of lab results; submission of falsified data; alteration of exams or other academic exercises; and collaboration on projects where collaboration is forbidden. (3) Falsification, forgery or alteration of any documents pertaining to assignments and examinations. (4) Students who (cooperate or in other ways promote) participate in promoting cheating or plagiarism by others (or who take credit for the work of others) will also be in violation of this policy.

Students participating in any violation of this policy must accept the consequences of their actions. Classroom instructors and/or university review/appeals committees and administrators will assess the sanctions for violation of this policy. The seriousness of the violation will dictate the severity of the sanction imposed.

Academic sanctions may include but not be limited to any of the following: (a) verbal or written warning; (b) lowering of grade for assignment/activity; (c) lowering of term grade; (d) failure of class assignment. Administrative sanctions may include but not be limited to either of the following: (a) suspension from the University; (b) dismissal from the University. I take academic honesty as the bedrock of collegiate work, and I will not accept cheating in any way, shape, or form. My personal policy is to give students grades of “U” (unsatisfactory, or fail) for both the assignment AND the course. Any incident of plagiarism is subject to the perpetrator’s immediately removal from class and failure.
Tentative Course Schedule:

**Week One – Introduction to the Management of Information Security**
We establish the foundation for understanding the field of information security by explaining the importance of information technology and identifying who is responsible for protecting an organization’s information assets.

**Week Two – Planning for Security**
We explain the importance of planning and describe the principal components of organizational planning and information security system implementation planning.

**Week Three – Planning for Contingencies and quiz #1**
We describe the need for contingency planning and explore the major components. It illustrates how to create a simple set of contingency plans using business impact analysis, and how to prepare and execute a test of those plans.

**Week Four – Information Security Policy**
We define information security policy and describe its central role in a successful information security program. We illustrate three major types of information security policy. We explain what goes into each type, and demonstrates how to develop, implement, and maintain various types of information security policies.

**Week Five – Developing the Security Programs**
We explore the various organizational approaches to information security and provide an explanation of the functional components of the information security program. Students learn how to plan and staff an organization’s information security department based on the size of the organization and other factors, as well as how to evaluate the internal and external factors that influence the activities and organization of an information security program. We also identify and describe the typical job titles and functions performed in the information security program. It concludes with an exploration of the creation and management of a security education, training and awareness program.

**Week Six – Security Management Models and Practices and quiz #2**
We describe the components of the dominant information security management models, including government-sanctioned models, and discuss how to customize them for a specific organization’s needs. Students learn how to implement the fundamental elements of key information security management practices and gain an understanding of emerging trends in the certification and accreditation of U.S. federal IT systems.

**Week Seven – Risk Assessment: Identifying and Assessing Risk and Midterm Exam**
We define risk management and its role in the organization, and demonstrate how to use risk management techniques to identify and prioritize risk factors for information assets. The risk management model presented here assesses risk based on the likelihood of adverse events and the effects on information assets when events occur. We conclude with a brief discussion on how to document the results of the risk identification process.
**Week Eight** – Risk Management: Controlling Risk
We present essential risk mitigation strategy options and open the discussion on controlling risk. This includes identifying risk control classification categories, using existing conceptual frameworks to evaluate risk controls, and formulating cost-benefit analysis. We learn how to maintain and perpetuate risk controls.

**Week Nine** – Protection Mechanisms and quiz #3
We introduce technical risk controls by exploring access control approaches, including authentication, authorization, and biometric access controls as well as firewalls and the common approaches to firewall implementation. The technical control approaches for dial-up access, intrusion detection systems, and cryptography are also covered.

**Week Ten** – Personnel and Security
We expand on the discussion of the skills and requirements for information security positions introduced in the previous weeks. It explores the various information security professional certifications, and identifies which skills are encompassed by each. We also explore the implementation of information security constraints – organization’s human resources processes.

**Week Eleven** – Law and Ethics
We learn about the legal environment and its relationship to information security. We describe the major national and international laws that affect the practice of information security, as well as the role of culture in ethics as it applies to information security.

**Week Twelve** – Information Security Project Management and quiz #4
We cover project management within the discipline of information security. It provides basic project management techniques as well as guidance of applying project management principles to an information security program.

**Week Thirteen** – Research paper topic and abstract
Due in the Assignments->Paper Topic & Abstract

**Week Fourteen** – Working on Research paper

**Week Fifteen** – Research paper
Due in the Assignments->Final Research Paper
At least 15 pages in length, including the abstract and references, with at least 15 references.

**Week Sixteen** – Course review and Final Exam