COURSE SYLLABUS

Course Name: IA 329:
Policy Development in Information Security

Instructor:

Office Hours:
Office:
Telephone:
FAX Number:
Internet/E-Mail Address:

Course Description: This course serves the essential aspects for developing sound information security policy. Organizational objectives, threats, risk mitigation and cost-benefit analysis is explored. The student will utilize industry accepted methodologies to create practical security policy that will communicate the organization’s asset protection objectives.

Purpose: Information in today's organizations faces a multitude of complex threats to its confidentiality, availability and integrity. These threats, as well as regulatory restrictions, customer privacy concerns, organizational objectives and culture, are key determinants for the development of sound information security policy. The interactions of asset protection goals, security and organizational objectives, as well as risk considerations, will be critical factors during the information security policy development process.

Organizational awareness of security policy objectives will enable successful implementation of the organization’s detailed procedures and standards. Threats originate from both inside and outside the organization. To mitigate the risk associated with these threats, an organization must have a well documented and clearly communicated information security policy.

Security policy must be a high level statement of goals and objectives. The policy must communicate the organizational strategy for asset protection. After the information security policy is accepted by management and communicated to the entire organization, the policy should be used as a guiding set of principles that drive the formation of the greater detailed documents such as procedures, standards and guidelines. These detailed documents are then used to manage the organization's assets with a fine level of granularity.

Scope: The scope of the material to be covered includes:
1. Regulatory Requirements for Policy
2. Policy development process and life cycle
3. Organizational responsibility to procedures, standards, and guidelines
Course Goals:

1. Compare and Contrast information systems security and information assurance
2. Describe information systems security policies and their importance in organizations
3. Describe governance and its importance in maintaining compliance with laws
4. Explain what policies are and how they fit into an organization

Course Objectives/Outcomes: This course will assist students in their career preparation as information system security managers. Upon successful completion of this course students should be able to:

1. You will be able to learn the importance of information security policies and the role they play in the business activities, ensuring sound and secure information.
1.1 You will be able to learn the importance of Information Security Policies and the role they play in business activities to ensure sound, secure information.
2. Using the Nayana Communications case study, the student will provide a risk mitigation strategy to further reduce risk for the organization.
2.1 You will be able to explore the concept of good policy implementation and describe factors relating to its success.
3. You will explore the concepts of business considerations as applied to a scenario.
3.1 You will learn how some frameworks inter-relate in industry specific organizations.
3.2 You will explore different frameworks and show how they inter-relate.
4. You will learn the reasons why SoD is a critical requirement for policy framework compliance.
4.1 You will also learn how to develop SoD policies.
5. You will research information security policy framework approaches. You will analyze policies for the specified organization.
5.1 You will identify the method for creating a security policy framework.
5.2 You will learn how using a security awareness policy (SAP) can increase the level of security understanding within the organization.
5.3 You will learn the topics to include in the SAP.
5.4 You will be able to create a report detailing user access policies based on research.
5.5 You will be able to explain the details of user policy creation in organizations.
6. You will learn how different policies affect the information technology (IT) infrastructure.
6.1 You will learn how security policies reduce the overall organizational risk.
6.2 You will examine information technology (IT) infrastructure policies.
6.3 You will describe IT infrastructure policies based on the scenario given.
7. You will learn approaches on how to plan for impacts that could potentially cause disruptions.
7.1 You will learn to create BIA, BCP, and DRP.
7.2 You will learn various aspects of how risk management impacts the business model.
8. You will learn what types of support services would be deployed when an incident occurs.
8.1 You will explore support services that would be required when an incident impacts the operational performance of an organization.
8.2 You will learn what types of support services would be deployed when an incident occurs.
8.3 You will explore support services that would be required when an incident impacts the operational performance of an organization.
9. You will explore and discuss security awareness policy creation, training, and application.
9.1 You will learn how to approach or what approaches are possible regarding a security awareness policy (SAP).
9.2 You will explore policy creation and enforcement actions.
9.3 You will describe policy monitoring and enforcement strategies.
10. You will explore various methods for tracking, monitoring, and reporting for organizational compliance.
10.1 You will learn why these systems can reduce the manual methods and thus provide a value add to the compliance process.
10.2 You will research automated information technology (IT) systems and create a report detailing one or two of them.
10.3 You will do research and align a selected automated IT system.

Course Description

The course includes a discussion on security policies that can be used to help protect and maintain a network, such as password policy, e-mail policy and Internet policy. The issues include organizational behavior and crisis management.

Major Instructional Areas
1. Security policy requirements
2. Security policy framework
3. Creation of security policies
4. Implementation issues
5. Security policy controls

Course Objectives
1. Identify the role of an information systems security (ISS) policy framework in overcoming business challenges.
2. Analyze how security policies help mitigate risks and support business processes in various domains in the information technology (IT) infrastructure.
3. Describe the components and basic requirements for creating a security policy framework.
4. Describe the different methods, roles, responsibilities, and accountabilities of personnel, along with the governance and compliance of security policy framework.
5. Describe the different ISS policies associated with the user domain.
6. Describe the different ISS policies associated with the IT infrastructure.
7. Describe the different ISS policies associated with risk management.
8. Describe the different ISS policies associated with incident response teams (IRT).
9. Describe different issues related to implementing and enforcing ISS policies.
10. Describe the different issues related to defining, tracking, monitoring, reporting, automating, and configuration of compliance systems and emerging technologies.

**Required Texts 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 texts are:


**Support Text (not required)**


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

Chapter 1, Information Systems Security Policy Management
1.1 What is Information Systems Security
1.1.1 Information Systems Security Management Life Cycle
1.2 What is Information Assurance
1.2.1 Confidentiality
1.2.2 Integrity
1.2.3 Nonrepudiation
1.3 What is Governance
1.4 Why is Governance Important
1.5 Where Do Information Systems Security Policies Fit Within An Organization
1.6 When Do You Need Information Systems Security Policies
1.7 Why Enforcing And Winning Acceptance For Policies Is Changing

Chapter 2, Business Drivers for Information Security Policies
2.1 Why Are Business Drivers Important?
2.2 Maintaining Compliance
2.3 Mitigating Risk Exposure
2.4 Minimizing Liability Of The Organization
2.5 Implementing Policies To Drive Operational Consistency

Chapter 3, U.S. Compliance Laws and Information Security Policy Requirements
3.1 U.S. Compliance Laws
3.2 Whom Do The Laws Protect
3.3 Which Laws Require Proper Security Controls Including Policies
3.4 Aligning Security Policies And Controls With Regulations
3.5 Industry Leading Practices And Self-Regulation
3.6 Important Industry Standards
3.6.1 Payment Card Industry Data Security Standard (PCI DSS)
3.6.2 Statement On Auditing Standard 70 (SAS 70)
3.6.3 Information Technology Infrastructure Library (ITIL)

Chapter 4, Business Challenges Within the Seven Domains of IT Responsibility
4.1 The Seven Domains of a Typical IT Infrastructure
4.1.1 User Domain
4.1.2 Workstation Domain
4.1.3 LAN Domain
4.1.4 LAN to Wan Domain
4.1.5 WAN Domain
4.1.6 Remote Access Domain
4.1.7 System Application Domain
4.2 Information Security Business Challenges and Security Policies
4.3 Policies that Mitigate Risk Within the Seven Domains

Chapter 5, Information Security Policy Implementation Issues
5.1 Human Nature in the Workplace
5.2 Organization Structure
5.3 The Challenge of User Apathy
5.4 The Importance of Executive Management Support
5.5 The Role of Human Resources
5.6 Policy Roles, Responsibilities and Accountability
5.7 When Policy Fulfillment is Not Part of Job Descriptions
5.8 Impact on Entrepreneurial Productivity and Efficiency
5.9 Tying Security Policy to Performance Accountability
5.10 Success is Dependent Upon Proper Interpretation and Enforcement

Chapter 6, IT Security Policy Frameworks
6.1 What is an IT Policy
6.2 What is a Program Framework Policy or Charter
6.3 Business Considerations for Framework
6.4 Information Assurance Considerations
6.5 Information Systems Security Considerations

Chapter 7, How to Design, Organize, Implement, and Maintain IT Security Policies
7.1 Policies and Standards Design Considerations
7.2 Document Organization considerations
7.3 Considerations for Implementing Policies and Standards
7.4 Policy Change Control Board
7.5 Maintaining your Policies and Standards Library

Chapter 8, IT Security Policy Framework Approaches
8.1 IT Security Policy Framework Approaches
8.2 Roles, Responsibilities and Accountability for Personnel
8.3 Separation of Duties
8.4 Governance and Compliance

Chapter 9, User Domain Policies
9.1 The Weakest Link in the Information Security Chain
9.1.1 Social Engineering
9.1.2 Human Mistakes
9.1.3 Insiders
9.2 Six Types of Users
9.3 Why Govern Users with Policies
9.4 Acceptable Use Policy
9.5 The Privileged-Level Access Agreement
9.6 Security Awareness Policy (SAP)

Chapter 10, IT Infrastructure Security Policies
10.1 Anatomy of an Infrastructure Policy
10.2 Workstation Domain Policies
10.3 LAN Domain Policies
10.4 LAN-WAN Domain Policies
10.5 WAN Domain Policies
10.6 Remote Access Domain Policies
10.7 System Application Domain Policies
10.8 Telecommunications Policies

Chapter 11, Data Classification and Handling Policies and Risk Management Policies
11.1 Data Classification Policies
11.2 Data Handling Policies
11.3 Identify Business Risks Related to Information Systems
11.4 Business Impact Analysis (BIA) Policies
11.5 Risk Assessment Policies
11.6 Business Continuity Planning Policies
11.7 Disaster Recovery Plan Policies

Chapter 12, Incident Response Team (IRT) Policies
12.1 Incident Response Policy
12.2 Incident Classification
12.3 The Response Team Charter
12.4 Incident Response Team Members
12.5 Responsibilities During an Incident
12.6 Procedures for Incident Response

Chapter 13, IT Security Policy Implementations
13.1 Implementation Issues for IT Security Policy
13.2 Security Awareness Policy Implementations
13.3 Information Dissemination – How to Educate Employees
13.4 Overcoming Technical Hindrances
13.5 Overcoming Nontechnical Hindrances

Chapter 14, IT Security Policy Enforcement
14.1 Organizational Support for IT Security Policy Enforcement
14.2 An Organization’s Right to Monitor User Actions and Traffic
14.3 Compliance Law: Requirement or Risk Management
14.4 What is Law and What is Policy
14.5 What Automated Security Controls can be Implemented Through Policy
14.6 Legal Implications of IT Security Policy Enforcement
14.7 Who is Ultimately Liable for Risk, Threats, and Vulnerabilities

Chapter 15, IT Policy Compliance Systems and Emerging Technologies
15.1 Defining a Baseline Definition for Information Systems Security
15.2 Tracking, Monitoring, and Reporting IT Security Baseline Definition and Policy
15.3 Automating IT Security Policy Compliance
15.4 Emerging Technologies and Solutions

**Student Requirements:** The overall goal of this course is to provide a practical educational experience in the fundamentals and application of policy development to the information security field. 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.

**Assessment and Evaluation:**
- Online Discussions: (2 @ 10 each) 20 points
- Mid-Term Exam: 20 points
- Group Presentation and Discussion: 20 points
- Final project and presentation – Security Awareness Program: 40 points
- Total Points: 100

**Grading Scale:**
95 - 100% = A  
80 - 83% = B  
70 - 73% = C  
60 - 63% = D  
0 - 59% = E

Notes on Requirements and Grading:

- Class sessions will involve an interactive 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. Verifiable emergencies will only be considered.

General Policies:

- Attendance and punctuality is mandatory. Class will start at the given time.
- All cell phones, pagers and any other miscellaneous forms of communication must be turned off prior to the start of class and remain turned off until after class is completed. This is out of courtesy for the other students and to insure an uninterrupted class.
- Speak to the instructor as needed.
- 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.
- Late work is not 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, for lost disks or damaged files is not sufficient reason for extensions.
- Class sessions will involve some lecture, Online discussions, and/or group facilitated activities. Therefore, it is the student’s responsibility to have completed the scheduled reading assignment prior to the class session. The student must also complete the assigned chapter activities/projects during scheduled class sessions. Active listening is also part of learning. Students are expected to have textbooks and other needed materials with them. Students should not expect to excuse lack of participation because they did not have their textbooks, and/or other materials.
• Be prepared to conduct discussions online through Caucus or another form of online viewing such as e-mail.
• Students are expected to complete all assignments in a neat, accurate and professional manner; otherwise, materials will not be accepted. This includes the word processing of all assignments with spell checking and proofreading mandatory. This also includes stapling your materials if needed so they do not become loose.
• All assignments will be graded for compliance to the instructor’s directions.
• Final grades will not be given in person, by telephone, e-mail, fax or any other communications medium except that of University standard written grading at the end of the semester.
• Attendance/participation is required therefore it is the student’s responsibility to obtain all missed instruction from another class member. The instructor will not repeat instructions or demonstrations for any student missing class. Keep in mind that attendance is mandatory.
• A grade of “I” will be given only in accordance with Eastern Michigan University’s Undergraduate school guideline.
• By University policy the instructor has the option of failing a student who does not attend class on the day of the final examination set by the university. Attendance at final periods during which students are presenting their work is required of all students and failure to attend is considered lack of participation.

**Academic Dishonesty**

In any university-level course, a statement of policy recognizing academic dishonesty should be unnecessary. However, it should be noted that the policy of the Department of Business and Technology Education is that, any student found to have engaged in any activity constituting academic dishonesty, will receive and “E” for the course in which the activity occurred. This policy relates to all forms of work associated with the course requirements; including examinations, quizzes, laboratory work, and all other assignments. It is the student’s responsibility to review the page(s) of the graduate catalog in order to determine those activities, which constitute academic dishonesty at Eastern Michigan University, which include both cheating and plagiarism. This policy will be strictly enforced.

Definition Reminders:


**Plagiarism:**
The Internet is a valuable tool, but not a replacement for your own thoughts for all papers and assignments in this class. Do NOT cut and paste from the Internet, you must formulate your own ideas based on the literature. Anything you use directly, should be quoted with citations noted.
Please read this web page: http://owl.english.purdue.edu/owl/resource/589/02/ It will give you guidelines. If you are in doubt, ask!

Here are a couple of links, there is a large volume of material in these 2 links, keep them for reference …
• Plagiarism Guidance: http://www.emich.edu/halle/plagiarism.html
• Citation and reference help: http://www.emich.edu/halle/style_guides.html

ASSIGNMENTS DUE will be accepted only during the class session during which it is due, or during which you present your project.
Print all components of the finished assignment, tables, queries, forms, presentations, and reports. These should be assembled in logical order. Grading also includes: Correctness and accuracy of work, contents, professionalism, APA formatting, and other factors emphasized in the course or in the final project description.