



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 Objectives: 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. Develop a high level understanding of the basic concepts and environmental considerations in the information security policy design and development process.
2. Develop and enhance the understanding of a basic security policy development cycle, from initial research to implementation and maintenance.
3. Implement a baseline security policy document template.
4. Gain a broad exposure to real world examples of security policies and the various styles of security policy implementations.
5. Provide an acute understanding of the risk, cost and other issues they may encounter during the implementation of an information security policy plan.
6. To gain an understanding for the application of industry standards such as the NIST 800-53, ISACA, COBIT and Carnegie Mellon/CERT OCTAVE information security policy frameworks.
7. Manage the security policy development process using industry accepted project management methodologies.

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:

- Information Security Policies and Procedures – A Practitioner’s Reference: Second Edition (2004). Thomas R. Peltier. ISBN-10: 0849319587, ISBN-13: 978-0849319587. Auerbach Publications
- Beyond Fear (2006). Bruce Schneier. ISBN-10: 0387026207, ISBN-13: 978-0387026206. Springer
- Secrets and Lies: Digital Security in a Networked World (2004). Bruce Schneier. ISBN-10: 0471453803, ISBN-13: 978-0471453802. Wiley

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

- Unit 1: Course Expectations and Introduction
- 1.1 Course Expectations
 - 1.2 Introduction

Unit 2: Life Cycle and Asset Classification

2.1 Life Cycle and Asset Classification

- 2.1 Introduction to Security Policy
- 2.2 Information Security Policy Development Life Cycle
- 2.3 Information Management and Asset Classification

Unit 3: Key Policies: Access Control

3.1 Access Control Policies

- 3.1.1 Access Authorization
- 3.1.2 Auditable Events
- 3.1.3 Authentication
- 3.1.4 Biometrics/Biometric Policies
- 3.1.5 Separation of Duties
- 3.1.6 Need-To-Know Controls

3.2. Administrative Security Policies

- 3.2.1 Importance of Administrative Security Policy
- 3.2.2 Importance of Procedures

Unit 4: Key Policies: Documentation Policies

4.1 Documentation Policies

- 4.1.1 Auditing
- 4.1.2 Logging
- 4.1.3 Documentation Policies
- 4.1.3 Standards and Procedures to Support Policy

Unit 5: Key Policies: Personnel Security Policies

5.1 Personnel Security Policies

- 5.1.1 Development of Standards and Procedures to Support Personnel Security Policy
- 5.1.2 Working with HR and Legal to develop and implement Personnel Security Policies, Standards and Procedures
- 5.1.3 In-Class Activity

Unit 6: Information Security Policy Development

6.1 Information Security Policy Development

- 6.1.1. Information Security Risk Assessment
- 6.1.2 “Beyond Fear “WebCT Online – Discussion

Unit 7: Information Security Policy

- Information Security Policy
- Define information security policy
- Importance of information security policy
- Information Security Policy, Risk Mitigation, Standards and Controls
- In Class Example – Risk Assessment
- NIST 800-30
- “Beyond Fear” WebCT Online - Discussion 2

Unit 8:
Midterms

Unit 9: Risk Assessment

9.1 Risk Assessment

9.1.1 In Class Example – Risk Assessment

9.1.2 NIST 800-30

9.1.3 In Class Example – Policy based on Risk Assessment

Unit 10: NIA Certification and Accreditation Process and Policy

10.1. NIA Certification and Accreditation Process and Policy

10.1.1 Information Security Policies to support: HIPAA, SOX, Workplace Privacy

10.1.2 Effective Enterprise Governance

Unit 11: Social Psychology in Implementation of Policy

11.1 Using Social Psychology to implement policies

11.1.1 Kabay Handout

11.1.2 Policy Implications - Business Continuity and Disaster Planning

Unit 12: Security Awareness Program

12.1 Security Awareness Program

12.1.1 Class Discussion / Presentation – “Secrets and Lies”

12.1.2 Policy Implications - Incident Response (Handouts)

Unit 13: Evidence Collection and Preservation Policies

13.1 Evidence Collection and Preservation Policies

13.1.1 Guest Speaker – Forensics and Incident Response

13.1.2 Evidence Collection and Preservation Policy Requirements

13.1.3 Security Awareness Program

Unit 14: Security Awareness Program Presentations

Unit 15: Final Exams

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- 0- 59% = E
90 - 94% = A- 77 - 79% = C+ 67 - 69% = D+
87 - 89% = B+ 74 - 76% = C 64 - 66% = D
84- 86% = B 70 - 73% = C- 60 - 63% = D-

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 un-interrupted 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 an "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:

Assist "To help or support." The American Heritage College Dictionary, 3rd Edition, page 83.

Cheat "To act dishonestly, practice fraud. To violate rules deliberately." The American Heritage

College Dictionary, 3rd Edition, page 239.

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.

*****The Instructor reserves the right to make any additions/deletions or changes to this syllabus as deemed necessary.**