MISY 4370 SPECIAL TOPICS IN MIS
FALL 2015
SESSION: FALL 2015 WEB

EAGLE PASS OFFICE 758-5015
HOME 773-3635
E-MAIL eadames@sulross.edu

OFFICE HOURS:	Eagle Pass	T	8:00 AM-4:00 PM
	Del Rio	W	4:00 PM-6:00 PM
	Uvalde	TH	4:00 PM-6:00 PM
	OR BY APPOINTMENT ANYTIME		

I will be available by phone, e-mail or in my office to offer help on any subject related to the course. As we progress in the course, I may make changes to this syllabus to accommodate any particular subject area. In that sense, this syllabus is a guideline, not a contract.

Required Text:
Information Security Principles and Practice 2e
Mark S. Merkow Jim Breithaupt, Pearson ISBN 978-0-7897-5325-0

1. **Learning Objectives**: The student will be able to:

    1. Recognize the growing importance of information security specialists to the information technology (IT) infrastructure and see how this can translate into a rewarding career. Develop a strategy for pursuing a career in information security. Comprehend information security in the context of the mission of a business. Build an awareness of 12 generally accepted basic principles of information security to help you determine how these basic principles are applied to real-life situations. Distinguish between the three main security goals. Learn how to design and apply the principle of defense in depth. Comprehend human vulnerabilities in security systems to better design solutions to counter them. Explain the difference between functional requirements and assurance requirements. Comprehend the fallacy of *security through obscurity* to avoid using it as a measure of security. Comprehend the importance of risk—analysis and risk—management tools and techniques for balancing the needs of business. Determine which side of the open disclosure debate you would take.

    Assessment: Written exam, written chapter exercise.

    2. Choose the appropriate type of policies to document a security program. Distinguish between the roles of standards, regulations, baselines, procedures, and guidelines. Organize a typical standards and policies library. Classify assets according to standard principles. Incorporate the separation of duties principle when creating a security policy. Outline the minimum pre-employment hiring practices for organizations. Analyze and manage risk. Outline the elements of employee security education, awareness, and training. List the eight types of people responsible for security in an information technology (IT) setting. Distinguish among the protection mechanisms used in a TCB. Defend the purposes of security assurance testing. Apply the Trusted Computer Security Evaluation Criteria (TCSEC) for software evaluations. Apply the Trusted Network Interpretation of the TCSEC Categorize the role of the Federal Criteria for Information Technology Security. Assessment: Written exam, written chapter exercise. Distinguish between the business continuity plan (BCP) and the disaster recovery plan (DRP). Define the scope of the business continuity plan. Identify types of disruptive events. Outline the contents of a business impact analysis (BIA). Discuss recovery strategies and the importance of crisis management.

    Assessment: Written exam, written chapter exercise.

3. Identify the types and targets of computer crime. Summarize the major types of attacks performed by cyber criminals. Understand the context of the computer in the legal system. Appreciate the complexities of intellectual property law. Distinguish between logical and physical security, and explain the reasons for placing equal emphasis on both. Recognize the importance of the Physical Security domain. Outline the major categories of physical security threats. Classify the techniques to mitigate risks to an organization's physical security. Classify the five main categories of physical security controls, including their strengths and limitations. Outline the types of controls needed for secure operations of a data center. Explain the principle of least privilege. Differentiate between the principle of least privilege and the principle of separation of duties. Define the control mechanisms commonly found in data center operations. Create a model of controls that incorporate people-based, process-based, and technology-based control mechanisms.

   Assessment: Written exam, written chapter exercise.

4. Apply access control techniques to meet confidentiality and integrity goals. Understand and implement the major terms and concepts related to access control and tie them to system security. Apply discretionary access controls (DAC) and mandatory access controls (MAC) techniques, as appropriate. Explain common terms used in the field of cryptography. Outline what mechanisms constitute a strong cryptosystem. Demonstrate how to encrypt and decrypt messages using the transposition method. Demonstrate how to encrypt messages using the substitution method.

   Assessment: Written exam, written chapter exercise.

5. Summarize the fundamentals of communications and network security and their vulnerabilities. Analyze the Transmission Control Protocol/Internet Protocol (TCP/IP). Distinguish among wide area networks (WANs), local area networks (LANs), and the Internet, intranets, and extranets. Outline the roles of packet-filtering routers, firewalls, and intrusion detection/prevention technology in network perimeter security. Describe the importance of security activities throughout the system development life cycle (SDLC) to implement secure systems. Follow the evolution of increased cybercrime and efforts to reduce cybercrime. Discuss the future of information technology (IT) software security developments and the outlook for InfoSec professionals.

   Assessment: Written exam, written chapter exercise.

2. **Assignments:** Selected questions and exercises will be assigned to help in the understanding of the course. Assignments will be submitted through the Blackboard. Do not submit assignments by e-mail.
3. **Exams**: There will be a mid-term and a final test to be administered online. The tests will be available during a time period to provide flexibility with the students schedules. See schedule below for dates.
4. **Note: It is a policy for this course that after the due date, there will be no make-up or reposition for the work required; this policy includes homework assignments, and exams. Participation in the course is mandatory. After missing four (4) submissions the student will be dropped from the course.**
5. **Course Grading: Projected Grade Distribution**

   The projected cutoff point for A's, B's, C's, and D's are based on a 90%, 80%, 70%, and 60%, respectively.

CLASS SCHEDULE FOR MISY 4370, SPECIAL TOPICS IN MIS

Date	Topic	Module/ Chapter	Assignments and tests *
Aug30	Why study information security?	1	**Submit assignments through the Blackboard** **Do not use e-mail**
Sep 6	Information security principles of success	2	
Sep 13	Certification programs and the common body of knowledge	3	
Sep 20	Governance and risk management	4	
Sep 27	Security architecture and design	5	
Oct 4	Business continuity planning and disaster recovery planning	6	
Oct 11	Law, investigations, and ethics	7	
Oct 18	Physical Security Control	8	
Oct 23	Mid-Term	1-8	
Nov 1	Operations Security	9	
Nov 8	Access Control Systems and Methodology	10	
Nov 15	Cryptography	11	
Nov 22	Telecommunications, Network, and Internet Security	12	
Nov 29	Software Development Security	13	
Dec 2	Securing the Future	14	
Dec7	Final Exam		

*** Assignments and tests will be posted on the Blackboard, assignments will be due and the tests will be available until midnight on the scheduled date.**