Enterprise Security Policy Management

CIS 75D (CRN:43379)

SPRING 2015

COURSE DESCRIPTION

Learn how to secure your enterprise network by creating a security policy and create procedures to maintain security policy. Learn to perform risk analysis and assessment on enterprise security. System Administrators, IT Managers and Analysts would benefit from this course as well as technologists wanting to broaden their impact.

PREREQUISITE SKILLS

Prerequisites: Computer Information Systems 75A or equivalent experience.

Advisory: English Writing 211 and Reading 211 (or Language Arts 211), or English as a Second Language 272 and 273.

INSTRUCTOR INFORMATION: JIM CARR

Office Hours Held: Tuesday
Office hours: 1:45-3:00PM
Office Location: AT 203 or AT 203b
E-mail address: carrjames@fhda.edu
Website: http://moodle.jblcourses.com

ATTENDANCE POLICY

Students are required to attend all meetings:
Class Thursday, 6:00-7:50 PM in AT 204 and
Lab 8:00-9:15 PM in AT 204.

See drop policy below.

DROP POLICY

1. Students who want to be dropped from the class MUST take the initiative to follow the De Anza College drop procedures. Drop calendar deadlines can be found at https://www.deanza.edu/calendar. Do not assume you will be automatically dropped from this course. If you intend to drop the course, you must drop yourself!

2. Drop Deadline

    a. By **Friday** OF THE FIRST WEEK OF THE COURSE you must purchase the course material from the bookstore and log into the Jones and Bartlett site.
    b. Successfully complete ALL the Week 1 ASSIGNMENTS in Jones & Bartlett Moodle.

OBJECTIVES

Upon completion of this course, you will be able understand the following objectives.

1. Identify the role of an information systems security (ISS) policy framework in overcoming business challenges.

2. Recognize the relationship between business drivers and information systems security policies.

3. Understand the relationship between regulatory compliance requirements and information system security policies.

4. Analyze how security policies help mitigate risks and support business processes in various domains of a typical IT infrastructure.

5. Analyze issues related to security policy implementations and the keys to success.

6. Describe the components and basic requirements for creating a security policy framework.

7. Describe how to design, organize, implement, and maintain IT security policies.

8. Describe the different methods, roles, responsibilities, and accountabilities of personnel, along with the governance and compliance of a security policy framework.

9. Describe the different ISS policies associated with the User Domain.

10. Describe the different ISS policies associated with the IT infrastructure.

11. Describe the different ISS policies associated with risk management.

12. Describe the different ISS policies associated with incident response teams (IRTs).

13. Describe issues related to implementing ISS policies.

14. Describe issues related to enforcing ISS policies.

15. Describe the different issues related to defining, tracking, monitoring, reporting, automating, and organizing compliance systems and compliance technologies.

STUDENT LEARNING OUTCOMES FOR THIS COURSE:

- Create and refine enterprise security policy and procedures.

- Create tools to track risks, document and mitigate them.

REQUIRED COURSE MATERIALS

1. There are **two purchase options** for your Jones and Bartlett course materials in the DeAnza bookstore). ***Do not purchase these materials below from any other source because they will not include the lab code access.***

- Johnson, Rob. Security Policies and Implementation Issues, 2nd ed. Burlington, MA: Jones & Bartlett, 2015

A. Bookstore option one – eBook Bundle

Purchase a Jones and Bartlett eBook and access code in the bookstore – ISBN 978128409566

B. Bookstore option two – Textbook Bundle

Purchase a Jones and Bartlett Textbook and access code in the bookstore – ISBN 9781284064759

2. After completing one of the purchase options above, you will need to access www.jblcourses.com , then click on "**Redeem an Access Code**". You must enter the Lab Access Code (purchased in Step 1 above) and the Course Code as shown below:

3. **High speed internet connection** (not dial up) required IF you work at home.

REQUIRED COMPUTER COMPONENTS AND AVAILABILITY

Hardware Requirements: A PC computer is required to run the Jones and Bartlett software. If you do not own a PC, you may use the computers in AT 203 lab.

Software: The only software required for this class in the Jones and Bartlett software. Using an up- to-date browser, such as Firefox, will be discussed in class.

Computers in CIS Lab:
If you need help with your course, you can use the CIS lab computers. For CIS computer lab hours access **http://www.deanza.edu/buscs/lab/hours.html**

SUBMITTING WEEKLY LAB ASSIGNMENTS

This course uses a Moodle website called Jones and Bartlett (moodle.jblcourses.com). All course information including assignments, homework, course deadlines, etc. will be available to you on-line on the Jones and Bartlett course Moodle web site. When you enter your Jones and Bartlett on-line course, you will see a list of assignments that you will complete. The actual course schedule and due dates for exams and assignments are subject to change.

HOMEWORK ASSIGNMENTS

Homework assignments will include answering multiple-choice questions in a 20-question quiz based on that week's reading assignment. Students will have 30 minutes to complete the quiz. Quizzes may be retaken an unlimited number of times to improve your score. The highest score will be recorded. No feedback will be given on questions missed during this open book, open notes homework quiz. The final exam will be extracted from these same homework questions.

FINAL EXAM

The 50-question, multiple-choice, closed-book, closed-notes Final Exam will be extracted from the Quiz questions.

LAB ASSIGNMENTS

The required lab assignments can be found in Moodle are counted towards your grade

(see below).

ATTENDANCE/PARTICIPATION

Ten points will be awarded each student for class participation.

EXTRA CREDIT

Students are encouraged to present a 10-minute presentation to the class on a relevant security topic. A short slide presentation in Microsoft PowerPoint of three to five slides is required to accompany the presentation. These slides will be posted on Moodle following the presentation. Consult the instructor first with your proposed topic and when to present on the schedule. Five points will be added to the final grade for this presentation.

MOODLE PORTAL

Jones and Bartlett Moodle must be used as the portal for completing all assignments. To post any discussion questions, use moodle.jblcourses.com. The optional online portion of the class is conducted online and I will be available **Mondays from 10:00AM to 11:15AM** to answer questions you may have in Moodle or through email during this time. However, you are not restricted from asking questions only during this time period. Email me anytime.

TESTING/GRADING POLICIES/FINAL GRADES

To pass this course, you must complete exercises, quizzes and the Final Exam with the minimum scores shown below. Weekly deadlines for each assignment are posted inside the Jones and Bartlett Moodle web site.

Exams Grading Scale:

A 93% - 100%
A- 90%-92%
B+ 87%-89%
B 83%-86%
B- 80%-82%
C+ 77%-79%
C 70%-76%
D+ 67%-69%
D 63%-66%

Final Grade Mix:

The following percentages reflect how the final grade will be determined:

Attendance/Participation	10%
Quizzes	30%
Lab	30%
Final Exam	30%
	=====
Total=	100%

Extra Credit 5%

ACADEMIC INTEGRITY:

Students who submit work of others as their own or cheat on exams or other assignments will receive a failing grade in the course and will be reported to college authorities.

DISRUPTIVE CLASSROOM BEHAVIOR

Disruptive classroom behavior may include (but is not limited to) the following: talking when it does not relate to the discussion topic, sleeping, reading other material (e.g. newspapers, magazines, textbooks, from other classes), eating or drinking, monopolizing discussion time, refusing to participate in classroom activities, leaving cell phones and pagers on, texting, and engaging in any other activity not related to the classroom activity. Students who engage in disruptive behavior will be approached by the instructor. If the disruptive behavior continues, students may be asked to leave the classroom and/or eventually be dropped from the course.

NOTE TO STUDENTS WITH DISABILITIES

If you have a disability-related need for reasonable academic accommodations or services in this course, provide your instructor with a Test Accommodation Verification Form (also known as a TAV form) from Disability Support Services (DSS) or the Educational Diagnostic Center (EDC). Students are expected to give five days notice of the need for accommodations. Students with disabilities can obtain a TAV form from their DSS counselor (864-8753 DSS main number) or EDC advisor (864-8839 EDC main number).

TECHNICAL DIFFICULTIES

If you have technical problems with the Jones and Bartlett software on your home computer, please contact Jones and Bartlett Technical Support directly at www.jblcourses.com/techsupport or call 866-601-4525 OR complete your course work using our computers in the AT203 CIS lab.

RECOMMENDED RESOURCES

Web References: Links to Web references in this document and related materials are subject to change without prior notice. These links were last verified on June 16, 2014 by Jones and Bartlett.

Books, Professional Journals

Please use the following author's names, book/article titles, Web sites, and/or keywords to search for supplementary information to augment your learning in this subject.

Sandy Bacik
Building an Effective Information Security Policy Architecture (Chapters 1 and 7)

Seymour Bosworth, et al.
Security Handbook, 5th ed. (Chapters 3, 21, and 26)

Debra S. Herrmann
Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI (Chapters 3, 4, and 5)

Ronald L. Krutz, et al.
The CISM Prep Guide: Mastering the Five Domains of Information Security Management (Chapters 2 and 5, and Appendix B)

William C. Nicholson
Homeland Security Law And Policy

Harold F. Tipton, et al.
Information Security Management Handbook, 6th ed. (Chapters 2, 5, 7, 14, 16, 41, and 42)

John R. Vacca
Computer and Information Security Handbook (Chapter 15)

Barry L. Williams
Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0

Kenneth A. Bamberger
"Technologies of Compliance: Risk and Regulation in a Digital Age," Texas Law Review, March 2010, Vol. 88 Issue 4 (Pages 669-739)

S. Vydrin
"Theoretical aspects of information security", Journal of Mathematical Sciences, January 2009, Vol. 156 Issue 2 (Pages 261-275)

Information Search
Use the following keywords to search for additional online resources that may be used for supporting your work on the course assignments:

Acceptable Use Policy (AUP)
Best Fit Privilege
Business Continuity Planning (BCP)
Business Impact Analysis (BIA)
Cyberterrorism
Cyberwarfare

Disaster Recovery Planning (DRP)
Globalism
Guidelines
Incident Response
Information Assurance
Information Security Controls
Information Systems Security
Laws
Layered Security
Least Access Privilege
Local Area Network (LAN)
Nation-states
Policies
Policy Management And Maintenance
Privileged Users
Procedures
Quality Assurance (QA)
Quality Control (QC)
Regulations
Responsibilities of Users and Accountability
Risk and Control Self-Assessment (RCSA)
Risk Management
Risk Mitigation
Standards
Telecommunications
U.S. Compliancy Laws and Industry Standards
Wide Area Network (WAN)