Management of Information Security and Forensics

CS 307

Catalog Description

PREREQUISITE: *CS 201.* Study of information security and digital forensics using practical case studies. Emphasis is on developing security policies, security management and practices, utilization of digital forensic tools and techniques, risk management, security project management, and protection mechanisms. Major components of the course are hands-on projects on digital forensic investigation and security management case studies.

Course Objectives

- To develop an understanding of basic information security and forensics terminologies and concepts.
- To understand the practical realities of threats to information security and the methods, tools, and techniques used to mitigate them.
- To be able to identify the types of attacks, their underlying nature, and the problems and solutions associated with them.
- To be able to understand risk management, its importance, and its development.
- To understand the relevance of information security policies, the models, and the guidelines for their development.
- To understand digital forensics and investigation and to be able to perform an in-depth analysis and to report significant findings.

Course Materials

- Textbook
  - Title: Management of Information Security, 2nd ed.
  - Author: Whitman and Mattord
  - Publisher: Course Technology
  - Date: 2008
- Software
  - Powerpoint reader

    - PDF reader
    - Internet Browser (MS Internet Explorer or Mozilla Firefox)
- Supplementary Resources
    - **http://csrc.nist.gov/publications/nistpubs/**
    - **http://www.niap-ccevs.org/cc-scheme**
    - **http://www.cnss.gov**

Detailed Course Outline

Topic		**Lecture Hours**
I	**Introduction to the Management of Information Security**	**2**
a	NSTISSC Security model	1
b	Principles of Information Security Management	0.5
b	INFOSEC and OPSEC	0.5
II	**Planning for Security**	**1.5**
a	Values, Vision, and Mission Statements	0.5
b	Strategic Planning	0.5
c	Planning for Security Implementation	0.5
III	**Planning for Contingencies**	**3**
a	Contingency Planning	0.75
b	Business Impact Analysis	0.75
c	Incident Response Plan	0.5
d	Disaster Recovery Plan	0.5
e	Business Continuity Plan	0.5
IV	**Information Security Policy**	**4.5**
a	Policy, Standards, and Practices	0.5
b	Enterprise Policy	0.5
c	Issue Specific Policy	0.5
d	System Specific Policy	0.5
e	Guidelines for Effective Policy	0.5
f	Developing Security Policy	0.5
g	Compliance, Enforcement, Distribution, and Automated Tools	1.5
V	**Developing Security Program**	**2**

Topic		**Lecture Hours**
a	Organizing for Security	0.5
b	Components of the Security Program	0.5
c	Information Security Roles and Titles	0.5
d	Implementing Security Education, Training, and Awareness Programs	0.5
VI	**Security Management Models and Practices**	**4**
a	Security Management Models	1
b	Security Management Practices	0.5
c	Metrics in Information Security Management	0.5
d	Emerging Trends in Certification and Accreditation	1
e	Certification and Accreditation	1
VII	**Risk Management: Identifying and Assessing Risk**	**1.5**
a	Risk Management	0.5
b	Risk Identification	0.5
c	Risk Assessment	0.5
VIII	**Risk Management: Controlling Risk**	**2**
a	Risk Control Strategies	0.5
b	Managing Risk	0.5
c	Cost Benefit Analysis	0.5
d	OCTAVE Method	0.5
IX	**Protection Mechanism**	**6**
a	Access Control	1
b	Firewalls	0.5
c	Intrusion Detection Systems	0.5
d	Remote Access Protection	0.5
e	Wireless Network Protection: WEP, WPA	0.5
f	Scanning and Analysis tools	1
g	Cryptography	2
X	**Personnel and Security**	**3**
a	Staffing and Security Functions	1
b	Information Security Professional Credentials:	1

Topic		Lecture Hours
	CISSP, CISA, CISM, GIAC, SCP, CCE, CIFI, SSCP	
c	Employment Policies and Practices	0.5
d	Security Custodian	0.5
XI	**Laws and Ethics**	**3**
a	Legal Environment	0.25
b	Relevant US Laws	1.25
c	International Laws and Legal Bodies	0.5
d	Policy vs Law	0.25
e	Professional Organizations and their Codes of Ethics	0.5
f	Organizational Liability	0.25
XII	**Information Security Project Management**	**2**
a	Project Management	1
b	Project Management Tools	1
XIII	**Digital Forensics and Investigations**	**2.5**
a	Digital Forensic Processes	0.5
b	Areas of Investigation	0.25
c	Methods of Acquisition	0.5
d	Forensic Analysis	0.5
e	Forensic Tools	0.5
f	Forensic Reports	0.25
XIV	**Case Study Report**	**1**

Course Policy

Examination Proctoring

The JSU policy for proctoring of examination for an online course is found in the following link:

http://distance.jsu.edu/DLProctoring.htm

Please note that, if a student lives in the Jacksonville area or nearby, the instructor will make arrangement for that student to take the exam on campus. Otherwise, the student must seek someone to act as a testing agent or proctor. The student is responsible for any cost associated with exam proctoring.

Grading Policy

Test 1	25%
Test 2	25%
Online discussion participation	5%
Homeworks/Case Study	15%
Final Exam	30%

Grading scale (Percentage)	
A	90 - above
B	80 - 89
C	70 - 79
D	60 - 69
F	below 60

Other Course Policies

Any individual who qualifies for reasonable accommodations under the Americans With Disabilities Act or Section 504 of the Rehabilitation Act of 1973 should contact the Instructor immediately.

Course Syllabus

The syllabus for this course can be downloaded **here** in PDF format.