

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 665

1. **Abbreviated Course Title:** Information Security
2. **Full Course Title:** Information Security Strategy & Policy Development
3. **Credits:** Three (3) graduate degree credits, 45 contact hours. Online or on-campus formats will be offered in the future.
4. **Catalog Description:** Policy, planning and implementation in building a comprehensive information risk management program is emphasized. Students will develop an awareness of hacking and exploiting weaknesses. An overview of the legal framework of network security, formulation of site security policy, countermeasures to secure computers, and integrating security components into an organizational program are also emphasized.
5. **Course Prerequisites:** None
6. **Rationale:** This course is designed to develop the knowledge and skills regarding policy, planning and implementation for building a comprehensive information risk management program plan. All organizations as well as individuals involved in information assurance/cyber systems must be cognizant of information security strategy and the development of appropriate policies and procedures to prevent compromises of these systems. Practitioners and managers of information assurance/cyber systems should find this course extremely beneficial in building an awareness of the threat of hacking and the weaknesses exploited. An overview of the legal framework of network security, formulation of site security policy, countermeasures to secure computers, and integration of security components into an organizational program as well as the procedures for the implementation of these measures to secure computers in an organization are emphasized.

Students aspiring to advance or seek a career in the security field or law enforcement should have a thorough understanding of current and relevant issues and changes in Cyber Security and how it ties in with National and Corporate Security, as it affects all sectors of our information-based, technically reliant society.

7. **Student Learning Outcomes and Course Goals:** Students who successfully complete this course will be able to...
 - A. ANALYZE the factors involved in establishing information security strategy and policy development.
 - B. DEVELOP an information security strategy and policy.
 - C. ASSESS the vulnerabilities of information security strategies and policies.
 - D. EXPLAIN “Information Security Strategy and Policy Development.”

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 665

- E. IDENTIFY “Information Risk Management.”
- F. INFER the best way to implement information security strategy policies and procedures.
- G. EVALUATE whether or not an organization’s information security strategies, policies, and procedures are adequate and current.
- H. COMPARE and CONTRAST the components necessary to build and implement a risk management program.
- I. ANALYZE the levels of and prioritize the potential vulnerabilities and threats to information-based systems.
- J. JUDGE the strengths and areas requiring improvement within an organization’s information security strategies and policies.
- K. DETERMINE the necessary security components needed to establish sound strategies, policies, and procedures.
- L. ARTICULATE and RATIONALIZE the need for establishing a legal framework for corporate and computer security.
- M. COMPILE the procedures that are required to integrate security components into policies and procedures of an organization.
- N. RATIONALIZE the need for organizational acceptance of information security strategy and policy.
- O. COMMUNICATE the responsibilities of and importance that executive management has in fully supporting cyber security professionals.

8. Instructional Procedures:

- Lecture
- Hands-on in class/lab exercises
- Group discussion and interaction
- Group and individual assignments/projects
- Student presentations

9. Course Content:

UNIT	TOPIC	SUBTOPICS	OUTCOMES
1	Introduction	Knowledge Base Background	A,D
2	Information Risk	Planning; Coordination;	A,E

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 665

	Management	Implementation	
3	Building a Risk Management Program	Define; Development; Present	A,H
4	Policy Planning	Contingencies; CONOPS; Continuity; Legal; Emergency Destruction	H
5	Implementing Policy	Implementation; Enforcement	H
6	Hacking and Information Systems	Configuration Management; Protective Technologies;	I
7	Assessment and Identification of Strengths	Advantages; Maxi-min Decision Matrix	C,F,G,J
8	Mid-term Project/Examination		A through J
9	Assessment and Identification of Weaknesses	Disadvantages; Maxi-min Decision Matrix	C,F,G,I
10	Legal Framework for Corporate And Computer Security	Laws; Legal Planning; Reporting	A,L
11	Formulating and Implementing a Site Security Policy	Awareness; Education;	K
12	Security Components	Physical; Communications; Information Assurance;	K
13	Integrating Security Components into Policies and Procedures	Systems Approach	M
14	Organizational Acceptance of Information Security and Strategy Policy	Security Culture Development; Policy; Executive Leadership Involvement	F,K,N,O
15	Final Project/Examination		A through O

Due to the nature of IA/Cyber Security courses, use of personal computers and University computer labs are **REQUIRED**. See CITI and computer lab links:

- <http://www.njcu.edu/programs/citi/>
- <http://www.njcu.edu/ac/home.htm>
- <http://www.njcu.edu/ac/labs/proflabs.htm>

10. Undergraduate General Studies Courses: (Not Applicable)

11. Graduate Course Status: This course is part of a carefully planned program sequence that embraces graduate-level pedagogy. Specifically, the design includes a

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 665

curriculum core, specialization and capstone for each graduate student. Item #6 covers the content rationale of this course and this item emphasizes the graduate status. Professional Security Studies students are developed into critical thinkers, defined as employing higher-order thinking: emphasizing application, analysis, synthesis and evaluation. As a graduate course, research is the common thread throughout the entire curriculum. Additionally, a team approach is integrated throughout as teamwork is the reality of the Professional Security field.

Students are required to build an awareness of the threat of hacking and the weaknesses that are targeted and exploited. They must also have an overview of the legal framework pertaining to computer and network security. Students should have the ability to formulate a site security policy, implement the steps that can be taken to secure computers in an organization. They must also understand how to integrate all these security components into an organizational program.

12. Programmatic/Departmental Outcomes:

Programmatic: This course fulfills the mission of the Security Program to provide students with greater knowledge, skills and abilities in the field of Professional Security Studies that will enable them to...

- Become lifelong learners for personal and professional enrichment
- Be effective and productive leaders and/or managers in their respective careers in the security field

Departmental: Students completing a course of studies in the graduate Security Studies Program must understand the policy, planning and implementation for building a comprehensive information risk management program. Information security strategy and policy development reflects the comprehensive, challenging nature and quality of the Professional Security Studies Department.

13. Degree Requirements: This course has been included as a required course for those specializing in the Cyber Security track in the Professional Security Studies Program.

14. Specialized Accreditation, Certification, and Licensure: This course has been mapped against the National Security Agency's (NSA) certification requirements for *Information Systems Security Officers, CNSSI 4014* (Committee on National Security Systems Instructions – CNSSI).

15. Assessment/Evaluation of Student Outcomes and Determining Student Grades:
a. Describe how students will be assessed on an ongoing basis and how their performance will be evaluated. Describe examinations, term or research papers, special projects, class performance, seminar presentations, and portfolios in relation to student learning outcomes (Item 7). Include type of examination, nature of papers and projects, etc.

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 665

The following sets forth the assessment/evaluation tool being used and the nature of the assignment(s) used to evaluate student outcomes:

ASSESSMENT/EVALUATION TOOL	NATURE OF ASSIGNMENTS USED TO EVALUATE STUDENT OUTCOMES
Class Participation	-Class discussions of assigned readings -Presentation of group responses to issues discussed in each class
Exams	-Written essay examinations to mid-term and final examination
Oral Presentations	-Individual presentation of research paper(s) -Presentation of group project
Research Paper(s) & Project(s)	-Individually assigned research paper(s) -Participation in group project

b. Please indicate the percentage assigned to each assessment/evaluation tool.

ASSESSMENT/EVALUATION TOOL	% OF TOTAL GRADE	OUTCOMES
Class Participation	20 %	F,L,M,N,O
Exams	30 %	A,C,D,E,G,H,I,K,L,M,N,O
Oral Presentations	20 %	B,H,L,M,N,O
Research Paper(s) & Project(s)	30 %	A,B,C,F,J,K

16. Bibliography:

a. Required Text(s):

Herold, R. (2005). *Managing an information security and privacy awareness training program*. Boca Raton, FL: CRC Press.

Kelly, L. & McCumber, J. (2004). *Assessing and Managing Security Risks in IT Systems*. Boca Raton, FL: CRC Press.

Litchko, J. & Payne, A. (2004). *Know Cyber Risk: By Managing Your IT Security*. Kensington, MD: Know Book Publishing.

Additional Required Resources: IA/Cyber Security Education Resources and Links for central access point for all historical documents (THESE ARE REQUIRED FOR ALL IA/CYBER SECURITY COURSES!!!):

<http://web.njcu.edu/sites/profstudies/securitystudies/Content/links.asp>

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 665

b. Supporting Bibliography:

- Alberts, C. & Dorofee, A. (2002). *Managing Information Security Risks: The OCTAVE Approach*. Cambridge: Pearson.
- Axelrod, C. (2004). *Outsourcing Information Security (Computer Security Series)*. Norwood, NJ: Artech House, Incorporated.
- Bock, J., Stromquist, P., Fischer, T., & Smith, N. (2002). *.NET Security*. Berkeley, CA: Apress.
- Boyce, J. Jennings, D., & Jennings, D. (2001). *Information Assurance: Managing Organizational IT Security Risks*. Philadelphia: Elsevier.
- Brenton, C. & Hunt, Cameron. (2001). *Active Defense: A Comprehensive Guide to Network Security*. San Francisco: Sybex, Incorporated.
- Doll, M., Doll, M., Rai, S., & Granado, J. (2002). *Defending the Digital Frontier: A Security Agenda*. Hoboken, NJ: John Wiley & Sons.
- Herold, R. (2005). *Managing an information security and privacy awareness training program*. Boca Raton, FL: CRC Press.
- Kelly, L. & McCumber, J. (2004). *Assessing and Managing Security Risks in IT Systems*. Boca Raton: CRC Press.
- Litchko, J. & Payne, A. (2004). *Know Cyber Risk: By Managing Your IT Security*. Kensington, MD: Know Book Publishing.
- Mitnick, K.D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Hoboken, NJ: John Wiley & Sons.
- Peltier, T. R. (2000). *Information Security Risks Analysis*. New York: CRC Press.
- Perlman, R. & Skoudis, E. (2001). *Computer Hack: A Step By Step Guide to Computer Attacks and Effective Defenses*. Harlow, CA: Pearson.
- Pfleeger, C. P. & Pfleeger, S. L. (2002). *Security in Computing*. Upper Saddle River, NJ: Prentice Hall.
- Phillips, B. (2001). *The Complete Book of Electronic Security*. New York: McGraw-Hill.

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 665

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. Hoboken, NJ: John Wiley & Sons.

Stallings, W. (2002). *Cryptology and Network Security: Principles and Practice*. Harlow, CA: Pearson.

Stein, L. D. (1997). *Web Security-A Step By Step Reference Guide*. Boston: Addison, Wesley.

Stinson, D. (2002). *Cryptology: Theory and Practice*. New York: CRC Press.

Vacca, J. R. (2002). *Computer Forensics: Computer Crime Scene Investigation*. Hingham, MA: Charles River Media.

c. Relevant Periodical Sources:

American Society for Industrial Security, International. *Security Journal*.
American Society for Industrial Security, International. *Security Management*.
Business News Publishing Company. *Security*.
Federal Bureau of Investigation. *The Law Enforcement Bulletin*.
[Http://www.wired.com](http://www.wired.com). *Wired*.

d. Relevant Online Materials (if not noted above):

American Society for Industrial Security, International: <http://www.asisonline.org>
Computer Security Organizations: www.sans.org
Federal Bureau of Investigation: <http://www.fbi.gov>
Improving CyberSecurity Research in the United States:
http://www7.nationalacademies.org/cstb/project_cybersecurity.html
Journal of Security Administrators: www.wiu.edu/users/mfkac/jsa
National Security Agency: <http://www.nsa.gov>
Society of Competitive Intelligence Professionals: www.scip.org

17. Enrollment and Scheduling: This course will be offered once a year with a minimum of 10 students and a maximum of 25 per class.

18. Resources:

- a. Supplies & Materials: Smart Board and/or projector for power point, blackboard, chalk and erasers
- b. Equipment:
 - 1.) Smart board and/or projector for power point
 - 2.) Dedicated Information Technology Classroom
- c. Space Allocation: Dedicated space to handle information technology/cyber security laboratory classroom as instructors will need the latest hard and software that will enable them to provide students with the knowledge, skills and abilities necessary in this field

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 665

19. Budget: The department's current budget will need to be augmented to cover cost of laboratory classroom and materials.