

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 660

1. **Abbreviated Course Title:** Security and Privacy
2. **Full Course Title:** Security & Privacy of Information & Information Systems
3. **Credits:** Three (3) graduate degree credits, 45 contact hours. Online or on-campus formats will be offered in the future.
4. **Catalog Description:** Students will develop knowledge and skills for security of information and information systems. It examines concepts and auditing security at all levels and systems platforms, presents techniques for assessing risk associated with accidental and intentional breeches of security, and studies associated issues of ethics of information and privacy considerations.
5. **Course Prerequisites:** None
6. **Rationale:** This course is designed to develop knowledge and skills for the security of information and information systems within organizations. All organizations as well as individuals involved in information/cyber systems must be kept informed and current with respect to the security and privacy of information and information systems. Lack of current knowledge in this area could have an adverse impact on national and corporate security entities. Practitioners and those managing information/cyber systems should find this course extremely beneficial in maintaining their expertise on security and privacy of information and information systems

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 many and various threats that face those responsible for the security of information systems.
 - B. ASSESS the security and privacy of information and information systems concerns within an organization.
 - C. ASSESS the risk associated with accidental and intentional breeches of security.
 - D. ASSESS the vulnerabilities of the different types of agencies reliant on information based systems.
 - E. IDENTIFY auditing security at all levels of systems platforms to include worldwide networks.

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 660

- F. DEVELOP countermeasures to threats directed at an organization’s information systems.
- G. EVALUATE the responsibilities of cyber security professionals.
- H. EVALUATE whether or not an organization’s physical security is sufficient to protect them from compromises.
- I. ANALYZE potential problems in the physical security of an organization housing information and information systems.
- J. OPERATIONALIZE the levels of and PRIORITIZE the potential vulnerabilities and threats to information-based systems.
- K. IDENTIFY areas in access control of information systems that could potentially be compromised.
- L. COMPARE and CONTRAST the categories of disruption that may affect information systems.
- M. DETERMINE the importance of using the “audit” in providing security to information systems.
- N. OUTLINE the importance of addressing security and privacy concerns.
- O. ANALYZE the responsibilities of and importance that executive management has in fully supporting cyber security professionals.
- P. REFLECT on the importance of identification and access control systems.
- Q. EVALUATE ethical and privacy issues.

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	D,G,N
2	Computer Systems Protection	Computer Security	A,G

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 660

		Framework	
3	Risk Management Planning for Computer and Information Systems	Threats; Criticality; Risk; Assets; Vulnerabilities	A,G,J
4	Categories of Disruption	Intrusion; Attacks; Malicious Code; Security Breach;	A,B,J,L
5	Identification and Access Control of Computer and Information Systems	Confidentiality, Integrity and Availability (CIA);	A,B,G,J,K,P
6	Physical Security	Protective Technology; Countermeasures	A,B,G,H,J,K
7	Use of the Audit	Monitoring and Audits	A,B,G,J,M
8	Mid-term Project/Examination		A,B,D,G,H,J,K,L, M,N,P
9	Systems Platforms	PC; Mainframe; Distributed	A,B,E,G
10	Worldwide Networks	Internet;	A,B,E,G
11	Risk Assessment Techniques	SWOT	A,B,G,I
12	Accidental and Intentional Breaches	Policy; Evaluation; Investigation	A,B,C,G
13	Countermeasures	Detection; Cryptology; Digital Signatures;	F,G
14	Ethical Issues and Privacy Considerations	Culture; Policy; Privacy; Ethics	O, Q
15	Final Project/Examination		A through Q

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 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 prepares students to be critical thinkers, defined as employing higher-order thinking: emphasizing application, analysis, synthesis and evaluation. As a graduate course, research is the common thread during the entire

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 660

curriculum. Additionally, a team approach is integrated throughout as teamwork is the reality of the Professional Security field.

Students are required to focus on concepts and auditing security at all levels and on all system platforms, including worldwide networks. They will learn techniques for assessing risk associated with accidental and intentional breaches of security. Associated issues of ethical uses of information and privacy considerations will also be covered.

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 address, analyze and discuss relevant current issues and the changes that affect the field of cyber security, in areas that include formal models for computer security, multilevel data models, multilevel database management system architectures, secure concurrency control protocols, distributed secure system architectures, integrity models and mechanisms, security policy, and requirement analysis. A course of this nature 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.

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

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 660

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 %	D,L,M,N,O,P,Q
Exams	30 %	A,B,C,D,G,H,I,J
Oral Presentations	20 %	C,D,K,L,M,N,O,P
Research Paper(s) & Project(s)	30 %	A,B,E,F,G,H,I,J,K

16. Bibliography:

a. Required Text(s):

Janssen, R. & Jensen, J. (2004). *Leveraging IT Infrastructure for HIPAA Training*. Washington, DC: EDUCAUSE Center for Applied Research Bulletin.

Kenigsberg, N. et al. (2004). *A Framework for HIPAA IT Security Compliance: Leveraging for Security*. Washington, DC: EDUCAUSE Center for Applied Research Bulletin.

LaMacchia, B. et al. (2002). *.NET Framework Security*. New York: Addison Wesley Longman, Inc.

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 660

b. Supporting Bibliography:

- Anderson, R. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken, NJ: John Wiley and Sons, Inc.
- Banan, M. (1999). *Neda's Efficient Mail Submission and Delivery (EMSD) Protocol Specification Version 1.3*. Bellevue, WA: Neda Communications, Inc.
- Biery, K. & Hager, D. (2001). *The Risks of Mobile Communications*. Retrieved February 1, 2006, from New Jersey City University, NJ, Proquest Web site:
<http://proquest.umi.com/pdqweb?did=955777295&Fmt=3&clientId=44872&ROT=309&VName=PQD>.
- Bishop, M. (2003). *Computer Security: Art and Science*. Upper Saddle River, NJ: Pearson Education, Inc.
- Cheswick, W. and Bellovin, S. (1994). *Firewalls and Internet Security: Repelling the Wily Hacker*. Cartersville, MA: Addison-Wesley.
- Clarke R. (2000). *An Artefact Ill-Fitted to the Needs of the Information Society*.
<http://www.anu.edu.au/people/Roger.Clarke/II/PKIMisFit.html>
- Curtin, M. (2001). *Developing Trust: Online Privacy and Security*. Berkeley, CA: Apress LP.
- Denning, D. (1982). *Cryptography and Data Security*. Cartersville, MA: Addison-Wesley.
- Gollmann, D. (1999). *Computer Security*. Hoboken, NJ: John Wiley and Sons, Inc.
- Internet Security Systems, Inc. (2000). *Microsoft Windows 2000 Security Technical Reference*. Redmond, WA: Microsoft Press.
- Janssen, R. & Jensen, J. (2004). *Leveraging IT Infrastructure for HIPAA Training*. Washington, DC: EDUCAUSE Center for Applied Research Bulletin.
- Karygiannis, T. & Owens, L. (2002). *Wireless Network Security 802.11, Bluetooth and Handheld Devices*. Washington, DC: Technology Administration, US Department of Commerce.
- Kenigsberg, N. et al. (2004). *A Framework for HIPAA IT Security Compliance: Leveraging for Security*. Washington, DC: EDUCAUSE Center for Applied Research Bulletin.

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 660

LaMacchia, B. et al. (2002). *.NET Framework Security*. New York: Addison Wesley Longman, Inc.

National Institute of Standards and Technology. (2004). *Special Publication 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. Washington, DC: National Institute of Standards.

Neumann, P. (1995). *Computer-Related Risks*. Cartersville, MA: Addison-Wesley.

Russell, D. & Gangemi, Sr., G. (1991). *Computer Security Basics*. Sebastopol, UK: O'Reilly and Associates.

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

Zwicky, E. et al. (2000). *Building Internet Firewalls, 2nd ed.* Sebastopol, UK: O'Reilly & Associates.

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

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 660

- 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

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