

**COLLEGE OF PROFESSIONAL STUDIES**  
*Professional Security Studies Department-Graduate*  
**SECU 610**

1. **Abbreviated Course Title:** Cyber Security
2. **Full Course Title:** Cyber Security
3. **Credits:** Three (3) graduate degree credits, 45 contact hours. Online or on-campus formats will be offered in the future.
4. **Catalog Description:** This course provides an overview of Cyber Security. It exposes the dimensions of our network, information-based society, reviews the impact of information security on institutions, privacy, business and government risks, the development of legislation and examines the dimensions of networks, protocols, operating systems and associated applications.
5. **Course Prerequisites:** (None).
6. **Rationale:** This course will provide students with a working knowledge of cyber security and the significant role it has in the security field. All organizations as well as individuals must consider the important dimensions of our network, information-based society for their safety. Cyber security also significantly impacts national and corporate security entities, and never has it been more critical than during the post September 11, 2001 era.

Students aspiring to advance or seek a career in the security field or law enforcement should have a thorough understanding of 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 responsibilities involved with Cyber Security.
  - B. APPLY the knowledge learned in developing cyber security policies and procedures.
  - C. APPRAISE whether or not corporate and national security entities are working together in the post September 11, 2001 era.
  - D. ASSESS the vulnerabilities of the many different entities reliant on information based systems.
  - E. RECOGNIZE the importance of understanding the potential adverse impact that breaches/compromises of information systems would have on organizations.

**COLLEGE OF PROFESSIONAL STUDIES**  
**Professional Security Studies Department-Graduate**  
**SECU 610**

- F. DISCUSS and ANALYZE what and how corporate and national security entities have addressed the need to maintain and continually upgrade their informational and technological systems.
- G. EVALUATE the responsibilities that cyber security professionals have with respect to protecting information, communications and related hard and software.
- H. COMPARE and CONTRAST the levels of and prioritize the potential vulnerabilities and threats to information-based systems.
- I. REFLECT the responsibilities of and importance that executive management has in fully supporting cyber security professionals in establishing and enforcing policies and procedures.

**8. Instructional Procedures:**

- Lecture
- Case Studies
- Group discussion and interaction
- Group and individual assignments/projects
- Student presentations

**9. Course Content:**

UNIT	TOPIC	SUBTOPICS	OUTCOMES
1	Introduction	History, Knowledge Base, Background	A
2	Information-based Systems	Security, Trusted Systems	C,F,G,H
3	Cyber Systems Protection	Defense in depth	C,F,G,H
4	Design Reference Threat	SWOT Analysis	G,H,I,
5	Network Protocols	Cryptology, authentication, access control, identity management	B,G,I
6	Operating Systems & Associated Applications	Anti-virus, anti-spy, firewalls, system backups	B,D,H,I
7	Effects of Policies and Procedures	Policy, Practice, Future Research	A,C,D,E,F,H
8	Mid-term Project/Examination		A through I
9	Working With Other Security Sectors	Relationship building, sharing resources, staff development	B,C,E,G
10	Cyber and Corporate Security	Copyright and Patent	B,C,E,I

**COLLEGE OF PROFESSIONAL STUDIES**  
**Professional Security Studies Department-Graduate**  
**SECU 610**

		infringement,	
<b>11</b>	Cyber and National Security	United Nation Initiatives, Federal, State	<b>B,C,E,I</b>
<b>12</b>	Disaster Recovery	Contingency Planning	<b>D,E,G,H</b>
<b>13</b>	Organizational Continuity Planning	Procedures, off-site continuity, system redundancy	<b>D,E,F,G,I</b>
<b>14</b>	Current Legislation Affecting Info Systems	Local, State, National	<b>A,B,F,G,I</b>
<b>15</b>	Final Project/Examination		<b>A through I</b>

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

Students are required to analyze, apply, appraise, demonstrate, design, discuss, evaluate, identify and understand the many complexities that go into making decisions and/or taking actions in case of a cyber security event.

**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

**COLLEGE OF PROFESSIONAL STUDIES**  
**Professional Security Studies Department-Graduate**  
**SECU 610**

Departmental: Students completing a course of studies in the graduate Security Studies Program must understand the role and impact that Cyber Security plays in today’s society as it has become a target of hackers and disgruntled employees, but also of international and domestic terrorist groups. This course is reflective of the comprehensive, challenging nature and quality of the Professional Security Studies Department.

- 13. Degree Requirements:** This is a required “core course” in the graduate program in Professional Security Studies.
- 14. Specialized Accreditation, Certification, and Licensure:** This course in conjunction with SECU 655, 660 and 665 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). Departmental goals include NSA certification for Information Assurance and designation as a *Center of Excellence* which can take 3-4 years to complete and represents the first *CNSSI 4014* in the state of NJ (only the University of New Haven, CT in the tri-state area has this certification).
- 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:

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.**

**COLLEGE OF PROFESSIONAL STUDIES**  
**Professional Security Studies Department-Graduate**  
**SECU 610**

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

**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.

Peltier, T. R. (2000). *Information Security Risks Analysis*. Boca Raton, FL: CRC Press.

**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>

**b. Supporting Bibliography:**

Alberts, C. & Dorofee, A. (2002). *Managing Information Security Risks: The OCTAVE Approach*. Cambridge, MA: Pearson.

Axelrod, C. (2004). *Outsourcing Information Security (Computer Security Series)*. Norwood, CT: 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.

**COLLEGE OF PROFESSIONAL STUDIES**  
***Professional Security Studies Department-Graduate***  
**SECU 610**

- 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, FL: 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, Inc.
- Peltier, T. R. (2000). *Information Security Risks Analysis*. Boca Raton, FL: CRC Press.
- Perlman, R. & Skoudis, E. (2001). *Computer Hack: A Step By Step Guide to Computer Attacks and Effective Defenses*. Upper Saddle River, NJ : 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.
- Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. Hoboken, NJ: John Wiley & Sons, Inc.
- Stallings, W. (2002). *Cryptology and Network Security: Principles and Practice*. Upper Saddle River, NJ: Pearson.
- Stein, L. D. (1997). *Web Security-A Step By Step Reference Guide*. Boston: Addison, Wesley.
- Stinson, D. (2002). *Cryptology: Theory and Practice*. Boca Raton, FL: 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*.

**COLLEGE OF PROFESSIONAL STUDIES**  
*Professional Security Studies Department-Graduate*  
**SECU 610**

Federal Bureau of Investigation. *The Law Enforcement Bulletin*.  
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](http://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](http://www7.nationalacademies.org/cstb/project_cybersecurity.html)

Journal of Security Administrators: [www.wiu.edu/users/mfkac/jsa](http://www.wiu.edu/users/mfkac/jsa)

National Security Agency: <http://www.nsa.gov>

Society of Competitive Intelligence Professionals: [www.scip.org](http://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: Sufficient at this time only for this core course

**19. Budget:** The department's current budget is sufficient at this time to handle only this core course. Additional resources will however, be required for those choosing to specialize in the "cyber security" track in the graduate program in Professional Security Studies to include:

- a. SEC 655: Topics in Computer Security
- b. SEC 660: Security and Privacy of Information & Information Systems
- c. SEC 665: Information Security Strategy and Policy Development