

**COLLEGE OF PROFESSIONAL STUDIES**  
*Professional Security Studies Department-Undergraduate*  
**SECU 322**

1. **Abbreviated Course Title:** COMPUTER SECURITY II
2. **Full Course Title:** Computer Security II - Intermediate
3. **Credits:** Three (3) undergraduate degree credits, 45 contact hours with additional study/activities expected outside the classroom.
4. **Catalog Description:** This intermediate course focuses on the importance of information security (INFOSEC) and the impact technology has in the field of security. Specific areas of coverage include: Operational Security (OPSEC), policy, roles and responsibilities, cryptography, transmission security, and components of the National Training Standard for Information Systems Security – (NSTISS). Components include: national policy, threats, countermeasures, and risk management among others.
5. **Course Prerequisites:** SECU 222 – Computer Security I or permission of instructor.
6. **Rationale:** Students typically enter this course with a basic level of computer security knowledge. Everyone is expected to continually self-reflect on the ways computers and associated technology can improve professional security practice. The foci of the course are to review or learn the fundamentals of computer security, create a knowledge base, and maximize day-to-day applications for the professional security field. By design, this course will develop the following three thinking skills:
  - o knowledge
  - o comprehension
  - o application, using the terminology, hands-on, and references provided throughout this course.

Students are expected to attain the apprentice-level of proficiency with the use of computer security.

7. **Student Learning Outcomes and Course Goals:** Students who successfully complete this course will be able to...
  - A. DESCRIBE critical characteristics of information.
  - B. DISCUSS the states of information.
  - C. EXPLAIN security measures to protect information.
  - D. IDENTIFY threats to and vulnerabilities of systems.
  - E. LIST the major legal issues of computer security.
  - F. OUTLINE potential countermeasures and risk management.
  - G. DISCOVER the concept of life cycle management.
  - H. EXPLAIN the facets of NSTISS.
  - I. GENERALIZE specific professional aspect of computer security to larger cross-career applications.
  - J. ARTICULATE emerging computer security trends.

- K. DEVELOP a personalized webliography through the use of a self-reflective journal from personal learning obtained in this course.
- L. DETERMINE which resources are best.
- M. REFLECT on the impact of computer security.

**8. Instructional Procedures:**

- Hands-on computer use (encourages student engagement)
- Lecture (minimal – designed to invoke thought and reflection)
- Group discussion and interaction
- Individual assignments/projects
- Student presentations of their computer security webliography

**9. Course Content:**

| UNIT | TOPIC  | SUBTOPICS   | OUTCOMES      |
|------|--|---|---------------|
| 1    | Operations Security (OPSEC)                  | INFOSEC and OPSEC Interdependency; Process; Surveys and Planning; Unclassified Indicators                 | A, K, L, M    |
| 2    | Information Security                         | Application Dependent Guidance; Policy; Roles and Responsibilities  | B, K, L, M    |
| 3    | Computer Security Procedures                 | Access Control; Audit; Identification and Authentication  | B, C, K, L, M |
| 4    | Cryptography                                 | Encryption; Key Management; Strength  | B, C, K, L, M |
| 5    | Security Principles                          | Emanations; Physical; Personnel; Administrative; Transmission   | B, C, K, L, M |
| 6    | National Policy and Guidance                 | AIS; Communications; Employee Accountability; Protection of Information                                   | B, C, K, L, M |
| 7    | Threats and Vulnerabilities of Systems       | Definition of Terms; Major Threat Categories; Threat Impact Areas   | D, K, L, M    |
| 8    | Mid-term Examination                         |   | A through D   |
| 9    | Legal Issues                                 | Criminal Prosecution; Evidence Collection/Preservation; Fraud, Waste and Abuse; Investigative Authorities | E, K, L, M    |
| 10   | Countermeasures and Risk Management Concepts | Assessments; Cover and Deception; Education, Training and Awareness; HUMINT; Monitoring;                  | F, K, L, M    |

|           |   |  |                      |
|-----------|---|--|----------------------|
|           |   | Technical Surveillance;<br>Consequences; Cost/Benefit;<br>Cost-Effective Controls;<br>Monitoring   |                      |
| <b>11</b> | Life Cycle Management                       | Demonstration and<br>Validation; Development;<br>Implementation; Operations<br>and Maintenance;<br>Requirements Definition;<br>Certification and<br>Accreditation                              | <b>G, K, L, M</b>    |
| <b>12</b> | Concepts of Trust and<br>Modes of Operation | Assurance; Mechanisms;<br>Policy; Compartmented /<br>Partitioned; Dedicated;<br>Multilevel; System- High   | <b>H, K, L, M</b>    |
| <b>13</b> | Roles of Organizational<br>Personnel        | Audit Office; COMSEC<br>Custodian; End Users;<br>INFOSEC Officer; OPSEC<br>Managers; Program<br>Managers; Senior<br>Management; System<br>Manager/Staff;<br>Telecommunications<br>Office/Staff | <b>H, I, K, L, M</b> |
| <b>14</b> | NSTISS in Action                            | Application of Cryptographic<br>Systems; Data/File Backups;<br>Multiple Protections;<br>Reporting Violations;<br>Transmission<br>Countermeasures   | <b>J, K, L, M</b>    |
| <b>15</b> | Final Examination                           |  | <b>A through J</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 – this is a College of Professional Studies offering/free elective.

**11. Graduate Course Status:** Not applicable – undergraduate level course.

**12. Programmatic/Departmental Outcomes:**

Programmatic: This course fulfills the mission of the College of Professional Studies to provide students with the knowledge, skills and abilities in the professions to:

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

Departmental: The development of this free elective allows all Professional Security Studies majors to meet the elective requirements while maintaining a direct connection to the field. The Department is committed to this *scholar-practitioner* approach. This course is part of a deliberate three-course sequence needed for computer security professionals.

**13. Degree Requirements:** This course is a free elective.

**14. Specialized Accreditation, Certification, and Licensure:** This course in conjunction with SECU 222 and 422 has been mapped against the *National Security Agency's (NSA)* certification requirements for *National Training Standard for Information Systems Security (INFOSEC) for Professionals – NSTISS 4011*. Certain aspects of this permanent course approval request are designed to comply with the *NSA* standards, i.e. course names, proficiency levels, universal references and increasing content (covering 256 elements), over the entire three course sequence. Levels are aligned with the course levels, e.g. SECU 222 - Basic = “novice,” SECU 322 - Intermediate = “apprentice,” and SECU 422 - Advanced = “proficient.” In other words, upon successful completion of the appropriate courses/student learning outcomes, our students would be rated at these levels within the field of Information Security (INFOSEC).

In addition to internal University evaluation, these courses have been externally reviewed by National level Information Assurance subject matter experts and determined to meet the *NSTISS 4011* standard. *New Jersey City University* received National recognition from the *NSA* along with certification for these three courses on June 5, 2007.

**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.**

Students will be continuously assessed throughout the semester with regular detailed and prompt feedback in keeping with modern assessment concepts. 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        | -Personal observations of in-class computer use<br>-Class discussions of assigned readings<br>-Presentation of group responses to issues discussed in each class |
| Exams                      | -Written essay examinations for mid-term and final examination   |
| Oral Presentations         | -Individual presentation of one selected intermediate-level computer security topic  |
| Webliography               | -Individual creation of a list of 15 computer security resources available on the Internet   |

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

| ASSESSMENT/EVALUATION TOOL | % OF TOTAL GRADE | OUTCOMES    |
|----------------------------|------------------|-------------|
| Class Participation        | 20 %             | A through J |
| Midterm Exam               | 20 %             | A through D |
| Oral Presentation          | 10 %             | E through J |
| Final Exam                 | 30 %             | A through J |
| Self-Reflection Journal    | 10 %             | A through M |
| Webliography               | 10 %             | A through J |

**16. References (APA format):**

**a. Required Text(s):**

Pfleeger, C. P. & Pfleeger, S. L. (2006). *Security in computing (4<sup>th</sup> Ed.)*. Upper Saddle River, NJ : Prentice Hall, 2006.

Department of Commerce, National Institute of Standards and Technology. (1995) *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook*. Available on-line at:

<http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>

Washington, DC: author.

**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:** (See the following:)

- \*Anderson, R. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken, NJ: John Wiley and Sons, Inc.
- \*Biery, K. & Hager, D. (2001). *The Risks of Mobile Communications*. New Jersey City University, NJ, Proquest Web site:  
<http://proquest.umi.com/pqdweb?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.
- 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.
- Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases*. Hoboken, NJ : John Wiley & Sons.
- Easttom, C. (2006). *Computer Security Fundamentals*. Upper Saddle River, N.J.: Pearson Prentice Hall.
- Fuller, F. & Larson, B. (2005). *Computers: Understanding Technology. Introductory (2<sup>nd</sup> ed.)*. St. Paul, Minn.: EMC/Paradigm.
- \*Gollmann, D. (2006). *Computer Security (2<sup>nd</sup> ed.)*. Hoboken, NJ: John Wiley and Sons, Inc.
- Gralla, P. (2006). *How personal & Internet security works*. Indianapolis, Ind.: Que/Sams; London : Pearson Education [distributor].
- Hamilton, P. (1972). *Computer security*. Philadelphia, PA: Auerbach Publishers.  
 (Reference is added to demonstrate this subject is not as new as many students may believe; the text is available from the Library of Congress).
- Internet Security Systems, Inc. (2000). *Microsoft Windows 2000 Security Technical Reference*. Redmond, WA: Microsoft Press.

- \*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.
- \*LaMacchia, B. et al. (2002). *.NET Framework Security*. New York: Addison Wesley Longman, Inc.
- LeVeque, V. (2006). *Information Security: A strategic approach*. Hoboken, N.J.: Wiley
- \*National Institute of Standards and Technology. (2005). *Special Publication 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. Washington, DC: author.
- National Security Agency. (1994) *National Training Standard for Information Systems Security (INFOSEC) for Professionals – NSTISS 4011*. Washington, D.C.: author.
- \*Neumann, P. (1995). *Computer-Related Risks*. Cartersville, MA: Addison-Wesley.
- Newman, M. (2007). *You have mail: True stories of Cyberspies*. New York: Franklin Watts.
- \*Panko, R. R. (2004) *Corporate Computer and Network Security*. Upper Saddle River, NJ: Prentice Hall.
- \*Russell, D. & Gangemi, Sr., G. (1991). *Computer Security Basics*. Sebastopol, UK: O'Reilly and Associates.
- Salomon, D. (2006). *Foundations of Computer Security*. London : Springer.
- Schifreen, R. (2006). *Defeating the hacker: A non-technical guide to Computer Security*. Hoboken, NJ : Wiley.
- \*Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. Hoboken, NJ: John Wiley and Sons. Inc.
- Walker, A. (2006). *Absolute Beginner's Guide to Security, Spam, Spyware and Viruses*. Indianapolis, Ind.: Que.
- Whitman, M. & Mattord, H. (2005). *Principles of Information Security (2nd ed.)*. Boston, Mass.: Thomson Course Technology.
- Zwicky, E. et al. (2000). *Building Internet Firewalls, 2nd Edition*. Sebastopol, UK:

O'Reilly & Associates.

***NSA References –Government Reference Format***

- [CHR90]Interview with Agent Jim Christy, Chief, Air Force Office of Special Investigations, Computer Crime Division, 26 March 1990.
- [DOD85]*Department of Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, Department of Defense, Washington, DC, December 1985.
- [DOJ88]*Basic Considerations in Investigating and Proving Computer-Related Federal Crimes*, U.S. Department of Justice, Justice Management Division, Washington, DC, November 1988.
- [HIG89]Higgins, John C., “Information Security as a Topic in Undergraduate Education of Computer Scientists,” *Proceedings of the 12th National Computer Security Conference*, November 1989.
- [MAC89]Maconachy, W.V., “Computer Security Education, Training, and Awareness: Turning a Philosophical Orientation into Practical Reality,” *Proceedings of the 12<sup>th</sup> National Computer Security Conference*, November 1989.
- \*[OTA87]U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310, Washington, DC, U.S. Government Printing Office, October 1987.
- \*[PFL89]Pfleeger, Charles P., *Security in Computing*, Prentice-Hall, 1989.

**Note** - \* = holdings physically present in the *Congressman Frank J. Guarini Library*. Other resources are available through inter-library loan(s). All resources have been validated and available at the U.S. Library of Congress at: <http://www.loc.gov>

**c. Relevant Periodical Sources:**

*Computer Fraud & Security* (2002 – Present)  
*Computer Security Update* (1999 – Present)  
*Information Systems Security* (1995 – Present)  
*Journal of Computer Security* (1996 – Present)  
*Security Dialogue* (2001 – Present)

All of the above journals/periodicals can be accessed through the EBSCO Academic Search Premier:  
<http://www.njcu.edu/guarini/clicktracker/click.asp?id=128&ky=>  
 (Requires GothicNet ID)

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

American Society for Industrial Security, International: [www.asisonline.org](http://www.asisonline.org)  
Computer Security Organizations: [www.sans.org](http://www.sans.org)  
Federal Bureau of Investigation: [www.fbi.gov](http://www.fbi.gov)  
Improving CyberSecurity Research in the United States:  
[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: [www.nsa.gov](http://www.nsa.gov)  
Society of Competitive Intelligence Professionals: [www.scip.org](http://www.scip.org)  
Department's Webpage: [www.njcu.edu/professionalsecurity](http://www.njcu.edu/professionalsecurity)

**17. Enrollment and Scheduling:** This course will be routinely offered (each regular semester – Fall and Spring, along with selected Summer sessions each year) with a minimum of 10 students and a maximum of 25\* per class.

\* - some computer labs only have 22 stations and that would be the maximum if assigned less than 25 computers.

**18. Resources:**

- a. Supplies & Materials: A computer lab that allows each student to individually have hands-on activity throughout the course. Other items that would assist with delivery are 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: No additional space required.

**19. Budget:** The department's current budget covers all costs.