

Course	SECR 5080 – Information Systems Security
Term	Spring 2 2007
Instructor	David E. Fowler, CISSP-ISSMP (O) 703-604-1489 ext 104 (C) 703-628-6321 Email: davidfowler72@webster.edu
Catalog Description	Students examine the management of information security and data-processing facilities, including thefts of data, unauthorized uses of information technology, computer viruses, and methods of protecting information, with an emphasis on networked computers. The course covers information technology laws, issues of privacy, and security planning.
Prerequisites	Must be capable of graduate work. Should have attended SECR 5000 and/or have experience in security management or have cleared attendance in advance with the instructor.
Course Level Learning Outcomes	<p>After completing this course, students should be able to explain and analyze:</p> <ol style="list-style-type: none"> 1. Concepts of confidentiality, integrity, and availability as applied to Information Systems Security 2. Security management policies, practices, and technologies to cost effectively reduce risk 3. Technical controls such as access, authentication, cryptography, and devices used to achieve secure system environments. 4. Managerial roles and controls used in securing the Information Systems environment. 5. Disaster planning and disaster recover models. 6. Laws and issues of privacy. <p>In addition, students will understand and explain:</p> <ol style="list-style-type: none"> 7. Important terminology, facts, concepts, principles, and theories used in the field of Business and Organizational Security Management. These will consist of the mandatory topics taught in the pre-requisite, advanced core courses, and integrative capstone course. 8. Important terminology, facts, concepts, principles and theories in the field of Business and Organizational Security Management to analyze simple to moderately complex factual security situations. 9. How to creatively construct and implement moderately complex Business and Organizational Security Management solutions to real organizational problems using frameworks procedures, and methods derived from the individual security discipline of Information Systems Security. 10. How to assess the effectiveness of their solutions by quantitatively or qualitatively measuring their results against theory-based criteria and standards of performance. 11. Utilize themselves as scholar-practitioners, capable of creatively synthesizing intellectual explanation of security models with methodological competencies and experience-based perceptual skills and judgment.

<p>Materials</p>	<p>For purchase: The CERT Guide to System and Network Security Practices, Julia H. Allen, Boston, Addison-Wesley, 2001, ISBN 0-201-73723-X.</p> <p>Supplemental Available on line:</p> <p>FIPS and NIST standards, available at http://csrc.nist.gov/publications/nistpubs/</p> <p>Information Security Handbook: A Guide for Managers, Pauline Bowen, Joan Hash, Mark Wilson, Nadya Bartol, Gina Jamaldinian, U. S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, June 2006, NIST Special Publication 800-100 Initial Public Draft. www.csrc.nist.gov.</p>
<p>Grading</p>	<p>Course Grades Your course grade will be based on your scores on your examinations, paper, presentation, and your contributions to the class discussions. These different components will be weighted as follows:</p> <p>Class Participation (10%):</p> <ul style="list-style-type: none"> • Students will be evaluated on their positive contribution to the overall class learning experience. At minimum, students are expected to: • Attend every session in its entirety • Ask questions and constructively contribute to topics being discussed during class, as appropriate • Avoid disruptive behavior (i.e. cell phones off, maintain constructive and courteous interaction with instructor and fellow students) <p>Research Paper (30%) Each student will be required to write and present an original paper addressing an information security topic of interest and value to a specified organization. Grading for this category is decomposed into the following milestones due on the corresponding class sessions.</p> <p>Class 4 – Selected Topic and Thesis Statement (5%) Class 8 – Final Research Paper 25%)</p> <p>System Security Planning (30%) Students will develop the basic elements of System Security Planning. The deliverables will be based on an accessible General Support System or Major Application. Grading for this category is decomposed into the following milestones due on the corresponding class sessions.</p> <p>Class 3 – Information System Description/Security Categorization (5%) Class 5 – System Security Control Selection (10%) Class 8 – Security Assessment Report (15%)</p> <p>Final Exam (30%) During the final session, students will provide a response to essay questions.</p>

Activities	<p>The Course Level Learning Outcomes will be covered as follows:</p> <ul style="list-style-type: none"> • Outcomes 1-4, and 7 -11 are covered throughout the course using lectures and group discussions, as well as multiple case studies and a number of practical exercises. • Outcomes 5 and 6 are covered in weeks 1 and 8 using lectures and group discussion. <p><u>Research Paper Project</u> Research paper project should follow Turabian, 6th edition. Good technical writing is concise, is void of colloquialisms, is absolutely nonsexist, and is generally written in the third-person. Pay particular attention to the way you use headings and sub-headings to clarify the organization of your paper. Your paper should be in the range of ten pages (excluding references, tables, and appendixes). See Turabian Form and Style manual for additional guidance on format. Students will make a presentation of the Research Paper Project in class. The presentation is part of the overall Research Paper Project grade.</p> <p>Example of Research Paper Project Sections (parts of the paper)</p> <ul style="list-style-type: none"> -Title Page -Table of Contents -List of Figures (Optional) -List of Tables (Optional) -Abstract (one page maximum) -Introduction -Multiple Sections on the Topic -Conclusion -Reference <p><u>Class Presentation</u> Students are expected to complete a research paper on a topic dealing with Security Administration and Management. They are also expected to prepare a 10 minute class presentation, supported by electronic projection (Microsoft® PowerPoint®) that highlights the student's research.</p> <p><u>Final Exams</u> Each exam will be given in class. The final during week nine class.</p>
Policy Statements: University Policies	<p>University policies are provided in the current course catalog and course schedules. They are also available on the university website. This class is governed by the university's published policies.</p>
Course Policies	<ul style="list-style-type: none"> • Late deliverables will be assessed a 10% penalty for each week or portion of a week overdue. • Deliverables should be provided in hard copy; pages attached by staples only. The final C&A package pages may be attached by alternate means. • Additional details will be provided at the first class meeting.
Weekly	<p>Week One: Introduction and Course overview.</p>

<p>Schedule</p>	<p>Allen, through Ch. 1, The CERT Guide ... Bowen, through Ch. 2, Information Security Handbook Review information available at two government Web sites, the National Infrastructure Protection Center (http://www.nipc.gov), and the Federal Computer Incident Response Center (http://www.fedcirc.gov) Reading: chapters one and two Assignments and Activities: Discuss text, syllabus, assignments, quizzes, and requirements to include system security plan and research project.</p> <p>Week Two: Security Management NIST SP 800-18 NIST SP 800-30 NIST SP 800-64 Swanson, Ch. 3, Plan Development Allen, Ch. 2, Securing Network Servers and User Workstations Assignments and Activities: Discussion: How the topic covered this week is integrated into policy by management.</p> <p>Week Three: Security Architecture and Models Allen, Ch. 2, Securing Network Servers and User Workstations Allen, Ch. 3, Securing Public Web Servers Swanson, through Ch. 2, Systems Analysis Bowen, Ch. 6, Information Security Handbook Assignments and Activities Discussion: How the topic covered this week is integrated into policy by management</p> <p>Week Four: Network Security Allen, Ch. 3, Securing Public Web Servers Allen, Ch. 4, Deploying Firewalls Swanson, Ch. 3, Plan Development Bowen, Ch. 8, Information Security Handbook Reading: chapters five and six Assignments and Activities Discussion: How the topic covered this week is integrated into policy by management</p> <p>Week Five: Cryptography and Public Key Infrastructure NIST SP 800-21 Student Presentations on Research Projects Research Proposal and Paper Outline Due Allen, Ch. 5, Intrusion Detection and Response</p>
------------------------	--

	<p>Swanson, Ch. 4, Management Controls</p> <p>Assignments and Activities Discussion: How the topic covered this week is integrated into policy by management</p> <p>Week Six: Malicious Code & Intrusion Detection Research Proposal and Paper Outline Due Allen, Ch. 5, Intrusion Detection and Response Allen, Ch. 6, Detecting Signs of Intrusion NIST SP 800-31 “Intrusion Detection Systems” Assignments and Activities Discussion: How the topic covered this week is integrated into policy by management</p> <p>Week Seven: Contingency Planning and Physical Security Allen, Ch. 7, Responding to Intrusions Swanson, Ch. 6, Technical Controls Common Criteria, pp. 8-11, Security Functionality and Assurance Assignments and Activities Discussion: How the topic covered this week is integrated into policy by management</p> <p>Week Eight: Physical Security Law, Investigation, and Ethics NIST SP 800-55 NIST SP 800-65 NIST SP 800-66 Assignments and Activities Discussion: How the topic covered this week is integrated into policy by management Start student presentations (in class)</p> <p>Week Nine: Student Presentations on Research Findings Paper Due Final Exam Reading: All previously assigned Course Wrap up</p>
Additional Information	None

Copyright © 2005 – 2006, School of Business & Technology, Webster University. All rights reserved.