SUNY INSTITUTE OF TECHNOLOGY
MARCY CAMPUS
P.O.BOX 3050
UTICA, NEW YORK 13504-3050
SCHOOL OF INFORMATION SYSTEMS & ENGINEERING TECHNOLOGY
SPRING 2012

NCS 330 - INFORMATION ASSURANCE POLICIES, ETHICS AND DISASTER RECOVERY

INSTRUCTOR: Dave Climek

OFFICE ROOM & TELEPHONE: DONOVAN 1215**,** 315-792-7284

EMAIL: climekd@sunyit.edu

OFFICE HOURS: Monday and Tuesday, 4PM-6PM and appointments by request

REQUIRED TEXTS:
(TAYLOR) FISMA Certification and Accreditation, by Laura Taylor, Syngress Publishing, 2007, ISBN-10: 1597491160 | ISBN-13: 978-1597491167

(GREENE) Security Policies and Procedures; Principles and Practices, by Sari Stern Greene, Pearson Prentice Hall, 2006 ISBN-10: 0131866915 ISBN-13: 978-0131866911

(800-100) NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2006, AVAILABLE ONLINE:
http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

SM-1 Federal Records Act
SM-2 Federal Managers Financial Integrity Act of 1982
SM-3 Federal Property and Administration Service Act
SM-4 USA Patriot Act
SM-5 GPEA
SM-6 Paperwork Reduction Act
SM-7 National Archives and Records Act
SM-8 Computer Fraud and Abuse Act, P.L. 99- 474, 18 U.S. Code 1030
SM-9 Freedom of Information Act
SM-10Electronic Freedom of Information Act
SM-11 Public Law 107-347, E-Government Act 0f 2002, Title III, Federal Information Security Management Act (FISMA), 17 Dec 02
SM-12 Privacy Act

RECOMMENDED READING: The student should have access to the Internet and World Wide Web. There are also several magazines and journals that may be used as sources of material for this course. You will be required to keep abreast of current events in this field. Reading and written assignments will be required utilizing the aforementioned reference sources.

COURSE OVERVIEW: This course teaches the student how to develop Information Systems security policies for small and large organizations with specific regard to components such as email, web servers, web browsers, firewalls, personal applications, passwords, etc. The need for and development of Disaster Recovery plans and procedures are also covered. This course builds upon the foundations of Information Assurance presented in NCS 320 Information Assurance Fundamentals. This course provides further background and skills for those individuals who seek skills in the areas of Network and Data Security.

COURSE OBJECTIVES: Upon completion of the course, the student will have a sound understanding of the areas of Information Systems (IS) where policy development and implementation may aid in reducing the effects of attack and carelessness. The student will also be prepared to develop and implement Information System Disaster Recovery Plans and Procedures to avoid loss and reconstitute business operations quickly after an Information System attack or other disaster. The student will be aware of the certification and accreditation practice as it relates to US Government requirements. Skills essential to future employment including: reading; research; technical writing; and presentation before an audience will be stressed.

SPECIFIC COURSE OBJECTIVES: At the end of this course, the successful student will:

1. Describe the security concerns of information system networks
2. Understand that security is provided by hardware, software, procedures, and education/training
3. Describe how policy, procedures, and standards are developed and used to enhance security
4. Understand the Certification and Accreditation process used by the US government
5. Describe processes involved in incident handling
6. Describe processes involved in disaster preparation and operations recovery
7. Become familiar with ethics and laws associated with information system networks

METHOD OF INSTRUCTION: This course will be conducted in a lecture/discussion format. Assigned reading, visual aids, supplementary reading (handouts) and independent research may also be used. If time and opportunity permits, guest lecturers and/or field trips will be included.

COURSE ETHICS: Student collaboration on reading assignments, studying for exams and finding homework sources is acceptable and encouraged. Students are expected to do their own original work on any Exams, Homework Assignments, Research Papers and Presentations. Mere cut and paste of material from the Internet for homework assignments, research papers or presentations will result in a zero (0) for that grade. Assignments will be checked via plagiarism detection software packages available to SUNYIT. Plagiarism will not be tolerated.

COURSE GRADING COMPONENTS:

Assessments (1, 2, 3), (100 pts each)	= 60%
Homework Assignments (10), (100 pts each)	= 10%
Term Paper (1), (100 pts)	= 20%
Attendance	= 10%
Total 100 points	= 100 %

Attendance will be taken for every class. Homework assignments are due the day listed below. Assignments that are turned in later than 10 days past the assigned due date will not be accepted.

COURSE OUTLINE

(Tentative - May be revised as school calendar and class meetings dictate. Students will be advised of changes)

Week 1: Communications and Connectivity
comm gear, TCP/IP, wireless, OPSEC/TEMPEST/EMSEC, Interconnecting Systems
800-100: 6

Week 2: Vulnerabilities & Threats
Natural disasters, accidents, human issues, thefts, attacks , vulnerability assessment, threat assessment
TAYLOR: 17

Week 3: Countermeasures
Technical: access control & privilege, authorization, email, information classification & marking, PKI, auto sec tools, backups, configuration management, downgrade & sanitization, DAC/MAC, biometrics, Sep of duties, Job Rotation, Need-to-know, inventory risk assessment
TAYLOR: 6, 14, 17, 18
GREENE: 8, 9, 10, 15
800-100: 10, 14

Week 4: Education, Training and Awareness, Acquisition, Life Cycle Mgmt
Education, Training, cert tools, contracting for services, facilities, sys sec plan
TAYLOR: 9, 19
GREENE: 3, 8, 10
800-100: 3, 4, 8, 12

Week 5: ASSESSMENT #1

Week 6: Procedural Countermeasures I
Policies, procedures and standards, Policy format, contents, essentials
TAYLOR: 10
GREENE: 1, 2, 4

Week 7: Procedural Countermeasures II

Asset classification, access control, authorization, acceptable use, personnel, Email, SW, encryption, physical & environmental, comm & ops mgmt, etc.
GREENE: 5, 6, 7, 8, 9, 10, 11

Week 8: Certification I
Why?, definition, types, responsibilities, gov requirements
TAYLOR: 1, 2, 3, 4, 7
800-100: 2, 5, 8, 11

Week 9: Certification II
Recert, waivers, SSAA, test & evaluation, package contents
TAYLOR: 3, 5, 12
800-100: 7

Week 10: ASSESSMENT #2

Week 11: Incident Handling
definitions, roles, responsibilities, forensics, checklists, policies, ops management
TAYLOR: 11
GREENE: 6, 8
800-100: 13

Week 12: Disaster Recovery/Business Continuity/Continuity of Ops
Disasters, roles & responsibilities, preparing, responding, recovering, develop, test, and maintain plan
TAYLOR: 14, 15
GREENE: 11
800-100: 9

Week 13: Ethics and Laws
Ethics, Fraud, waste and abuse, banking, healthcare, business, copyright, due care, due diligence, privacy, various laws
TAYLOR: 13, 19
GREENE: 12, 13, 14
SM 1-12

Week 14: ASSESSMENT #3

HOMEWORK ASSIGNMENTS

1. Submit homework in the form of short, double-spaced, typewritten pages, of uniform margins, with correct grammar, spelling and syntax.
2. Use textbooks, professional journals, newspapers, magazines, WWW and Internet.
3. Each homework assignment will be done according to the format discussed in class.

4. Homework assignments should be handed in the date that they are due. 10 points will be lost for each day late unless prior arrangement is made with instructor. Assignments that are turned in later than 10 days past the assigned due date will not be accepted.
5. You MUST use the following Format (separate page each)
Title Page (see below for format)
Item I (What was the assignment?, What was I asked to do?)
Item II (What did I do?, What were the results? What the homework asked you to do.)
Item III (What did I learn? What information assurance principles did I learn?)
List of References - POINTS WILL BE LOST FOR FAILURE TO FOLLOW FORMAT.
6. This should be a summarization of what you were asked to do or what you found out (CUT AND PASTE WILL RESULT IN POINT LOSS).
7. You must document the source(s) used for the homework.

(Sample Title Page Format)

NCS 330

Information Assurance Policies, Ethics and Disaster Recovery

Homework Assignment #1

Date Due

Student Name

PAPERS

1. Get research topic approved no later than Week 6. Suggested areas of research will be provided by Week 3.
2. Research and describe your chosen area using a number of sources, including textbooks, magazine articles, the World Wide Web, Internet, etc.
3. A double-spaced paper, consisting of 3500- 4500 ORIGINAL words is due by Week 11. 10 points will be lost for each day late unless prior arrangement is made with instructor. Assignments that are turned in later than 10 days past the assigned due date will not be accepted.
4. You MUST use the following format for the paper:
Title Page
Introduction
Information Sections (may be 1 to 5 or more)
Summary
List of References (You must document the sources used for the paper). POINTS WILL BE LOST FOR FAILURE TO FOLLOW FORMAT.

(Sample Title Page Format)

NCS 330

Information Assurance Policies, Ethics and Disaster Recovery

Paper Topic Title

Date Due

Student Name

This course is also offered under the articulation agreement between Binghamton University and SUNYIT. It is available to qualified students at Binghamton University via the distance learning system Enginet.
