CS684 A1 IT Security Policies and Procedures

Learn from Anywhere Course Format, Offered Simultaneously On Campus and Remote

Instructor: Pamela Campbell

Contact Information

Office Location: Virtual Office

Office Hours: Thurs 5 - 6 pm Wednesday EDT via Zoom; other times as arranged

Office Phone: 978-884-1157

Wednesdays: 6:00 - 8:45 PM

The First Class will take place on September 2, 2020

DATES: Sept 2, 9, 16, 23, 30, Oct 7, 14, 21, 28, Nov 4, 11, 18 – NO CLASS NOV 25, Dec 2

Classroom: Zoom classroom, on Blackboard website; SHA 210

E-Mail: pdc@bu.edu Pamela Campbell

Materials will be delivered using the 'Blackboard Learn' web site for this course which can be accessed at http://learn.bu.edu

Fall 2020 COVID-19 Policies

Classroom Rotations: [*for courses with rooms that cannot accommodate the all students wanting to meet in-person*] Classrooms on campus have new capacities that follow guidelines issued by state and local health and government authorities related to COVID-19 and physical distancing. Before the beginning of the class, and throughout the semester, I will be reaching out to students who have indicated that they want to attend the classroom in-person. Our classroom hold [] students, and therefore we will have [two] rotations of students that come to class on campus alternate weeks. You will be asked to attend remotely on the week that you have rotated out the classroom.

Compliance: All students returning to campus will be required, through a digital agreement, to commit to a set of Health Commitments and Expectations including face coverings, symptom attestation, testing, contact tracing, quarantine, and isolation. The agreement makes clear that compliance is a condition of being a member of our on-campus community.

You have a critical role to play in minimizing transmission of COVID-19 within the University community, so the University is requiring that you make your own health and safety commitments. Additionally, if you will be attending this class in person, you will be asked to show your Healthway badge on your mobile device to the instructor in the classroom prior to starting class, and wear your face mask over your mouth and nose at all times. If you do not comply with these rules you will be asked to leave the classroom. If you refuse to leave the class, the instructor will inform the class that they will not proceed with instruction until you leave the room. If you still refuse to leave the room, the instructor will dismiss the class and will contact the academic Dean's office for follow up.

Boston University is committed to offering the best learning environment for you, but to succeed, we need your help. We all must be responsible and respectful. If you do not want to follow these guidelines, you must participate in class remotely, so that you do not put your classmates or others at undue risk. We are counting on all members of our community to be courteous and collegial, whether they are with classmates and colleagues on campus, in the classroom, or engaging with us remotely, as we work together this fall semester

Biography

Pamela Campbell is a lecturer at Boston University. She has been working and teaching in the area of Project Management, Education, and software development for 20 years in organizations such as MITRE, Synetics, and BEA Systems, Inc. She holds a Masters degree from Bentley College in Computer Information Systems and has designed and implemented systems that include large databases.

One of her most rewarding assignments was to manage the project to upgrade the Amver system (amver.com). Amver, sponsored by the United States Coast Guard, is a unique, computer-based, and voluntary global ship reporting system used worldwide by search and rescue authorities to arrange for assistance to persons in distress at sea. Ms. Campbell has been teaching for Boston University for more than 15 years.

In addition to her lecturing, she is a consultant to Bridging Distances, for which she provides training services to software, healthcare, and engineering firms.

IT Security Policies and Procedures

Course description

This course enables IT professional leaders to identify emerging security risks and implement highly secure networks to support organizational goals. Discussion of methodologies for identifying, quantifying, mitigating and controlling risks. Students implement a comprehensive IT risk management plans (RMP) that identify alternate sites for processing mission-critical applications, and techniques to recover infrastructure, systems, networks, data and user access. The course also discusses related topics such as: disaster recovery, handling information security; protection of property, personnel and facilities; protection of sensitive and classified information, privacy issues, and criminal terrorist and hostile activities.

All students should be sure to obtain a free Boston University computer account and email address as these are necessary both for essential electronics communications with students and to use the web sites for this and other courses at Boston University. Students are expected to check the 'Blackboard Learn' site for announcements and assignment changes, and to read their email **which will be addressed to their bu.edu email address**. Note that you can arrange for your bu.edu email to be forwarded to a different preferred email address (e.g. your work or personal email address such as a yahoo or Gmail account (and you can do this via the university web site).

Revisions to this syllabus, schedule changes, new readings and assignments, and so forth, will be posted on the 'Blackboard Learn' web site as the course goes along, where you can download them. Additional materials will be posted to the site as needed, and as they become relevant.

Learning Goals and Objectives and Outcomes

Upon successful completion of this course, you will understand:

- The common Information Systems Security models
- Security characteristics, threats and responses
- Security measures from Technology, Policy and Practice, and Education, Training, and Awareness dimensions
- Risk Management—identification, quantification, response, and control
- Disaster Recovery procedures and countermeasures for the business enterprise

Further, upon successful completion of this course, you will be able to:

1. Demonstrate knowledge of IT security policy terms and techniques such as:
    a. Information Security Policy Lifecycle
    b. Policies vs. Standards vs. Procedures vs. Guidelines
    c. Identifying vulnerabilities
    d. Regulations, laws, and governance
    e. Asset identification and asset recovery
    f. The role of NIST and ISO
    g. Human Resource Security
    h. The Secure Facility Layered Defense Model
    i. Network Segmentation
    j. The GLBA, HIPAA, and the PCI framework

2. Understand advanced topics in the domain on IT Security Policy
    a. Threats to enterprise security, both common and specialized
    b. Confidentiality, Integrity and Availability
    c. Security policy tiers
    d. Classifying security assets

e. Business Continuity Threat Assessment
f. Identifying and quantifying risks and developing risk response plans
g. Disaster Recovery and Response Plans
h. Security in software and application development
i. Operational Change Control
j. Identifying and classifying incidents and breach notification

3. Apply IT Security Policy concepts through assignments
   a. Preventing or mitigating security damage
   b. Codifying security policies and procedures
   c. Identification of standards application
   d. Assessing security issues
   e. Develop security policies and procedures

4. Students will develop good documentation/technical writing skills, and through discussion and the final presentation, build communication skills, particularly virtual communication skills.

Note: (If you plan to become a certified Project Management Professional this comment applies to you.) This course counts to PMP educational requirements and the project produced counts towards experience.

See the Individual Assignment documents posted on Blackboard for Detailed Homework and Reading Assignments.

Course Outline

- **Readings** - Each module has textbook readings. There are additional materials online. Your professor may suggest additional readings during the running of the course.
- **Discussion** – Discussions will be conducted in class. Reading will be assigned in advance. The Discussion tab will also hold the slides shown in class.
- **Assignment** - There are assignments that are due throughout the course. – Look in Assignments on the website for detailed instructions.

Module 1: Introduction and Threats to the I.T. Environment

- Threats to enterprise security
- Overview of enterprise I.T. threat responses
- Common enterprise security issues
- Specialized enterprise security issues
- ***(Laws and Regulations)***

Module 2: Security Policies

- Policies vs. standards vs. procedures
- Policies in detail

- Security policy tiers

Module 3: Security Standards and Procedures

- Security Standards
- Procedures for security
- Classifying assets
- ***(Regulatory requirements)***

Module 4: Operational Security Management

- Managing operational security
- Introduction to Business Continuity
- ***(Technology changes and its impact on business)***

Module 5: Business Continuity and Disaster Recovery

- Continuity and Disaster Recovery
- Preparing for I.T. Continuity
- Managing Disaster Recovery

Module 6: Managing Security Risk in System Development and Integration

- Security in system development and integration
- Using Quality to assess security risk in system development
- Review course material and prepare for final class presentations.

Class Schedule

Class sessions are 6:00 – 8:45 PM

Students are expected to attend on Zoom, using video. Each student is expected to bring a current news item on security issues to each class for discussion purposes.

Class Presentations: Each student is required to present in class on a unique topic in lieu of a final exam. Presentation details and topics will be available for students to choose.

LECTURE SCHEDULE: This is a ‘provisional’ schedule and is subject to change as the course progresses and evolves.

See the Assignments document posted on Blackboard for Detailed Homework and Reading Assignments.

1. Sep 2 – **Module 1 Study Guide and Deliverables**

- **Readings:** *Greene*: Chapter 1, pages 2 - 21; *Peltier*: pages 187–188, 250–263, 287–296, and pages 367–370
- **Discussions:**
- **Assignments: Assignment 1 due - Sept 23 by 5:00 PM**

2. Sep 9 - **Module 1 Continued**

- **Assignments: Assignment 1 due - Sept 23 by 5:00 PM**

3. Sep 16 – **Module 2 Study Guide and Deliverables**

- **Readings:** *Greene*: Chapter 2, pages 32 - 53 *Peltier*: Primary: 47–80; Secondary: 199–241
- **Discussions:**
- **Assignments: Assignment 2 due - Oct 7 by 5:00 PM**

4. Sep 23 – **Module 2 Continued**

- **Assignments: Assignment 2 due - Oct 7 by 5:00 PM**

5. Sep 30 –– **Module 3 Study Guide and Deliverables**

- **Readings:** *Greene*: Chapter 5, pages 124 - 144 *Peltier* p 243–245 and 256–262 Peltier p 85–88 and 95–101
- **Discussions:**
- **Assignments: Assignment 3 due - Oct 21 by 5:00 PM**

6. Oct 7 **Module 3 Continued**

- **Assignments: Assignment 3 due - Oct 21 by 5:00 PM**

7. Oct 14 – **Module 4 Study Guide and Deliverables**

- **Readings**: *Greene*: Chapter 11, pages 328 – 354 *Peltier*: pages 341, 347–348, 350–358
- **Discussions:**
- **Assignments: Assignment 4 due Nov 4 by 5:00 PM**

8. Oct 21 – **Module 4 Continued**

- **Assignments: Assignment 4 due Nov 4 by 5:00 PM**.

9. Oct 28 **- Module 5 Study Guide and Deliverables**

- **Readings**: *Greene*: Chapter 12, pages 370 - 397
- **Discussions**:
- **Assignments: Assignment 5 due Nov 18 by 5:00 PM**

10. Nov 4 – **Module 5 Continued**

- **Assignments: Assignment 5 due Nov 18 by 5:00 PM**

11. Nov 11 – **Module 6 Study Guide and Deliverables**

- **Readings:** *Peltier* Page 34
- **Discussions:**
- **Assignments: Draft Presentation Due**

12. Nov 18 – **Module 6 Continued**

- **Assignments: No assignment – prepare for class presentations**

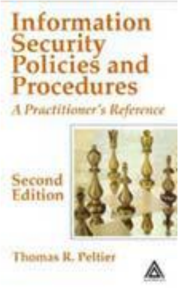
Nov 25 – NO CLASS – Thanksgiving Break

13. Dec 2 –**Presentations (counts as final)**

- Final Project Report hardcopy due
- Lessons Learned Paper Due
- Presentation in class

14. Dec 9 –**Presentations (if needed, counts as final)**

Course Resources


Information Security Policies and Procedures
A Practitioner's Reference
Second Edition
Thomas R. Peltier

Pelitier, T. R (2004) Information Security Policies and Procedures: A practitioner's reference (2nd edition) New York, NY/London: Auerback Publications

ISBN: 9780849319587

Greene, S. S. (2014) Security Program and Policies: Principles and Practices (2nd edition) Pearson

ISBN: 9780789751676

Optional Text: (recommended for those planning a career in security)

Erbschloe, M. (2003) Guide to Disaster Recovery. Boston: Thompson Course Technology

ISBN: 9780619131227

Grading Structure

All students will be expected to demonstrate knowledge of IT Security Policies and Procedures and relevant techniques. To obtain an exceptional grade you have to exceed expectations in your projects and weekly assignments.

Accommodation of Special Needs

In accordance with University policy, we make every effort to accommodate unique and special needs of students with respect to speech, hearing, vision, seating, or other disabilities. Please notify Disability Support Services as soon as possible of requested accommodations.

Grading Structure, Distribution and Grading Criteria

The course consists of homework assignments, participation in discussions, and a final (individual) presentation, weighted as follows:

Assignments: **40%**

Participation and Discussions: **30%**

Students are expected to attend class, using video, and to participate in discussions and exercises

Final Presentation (counts as final exam): **30%**

The Final Presentation includes providing a **draft**, with the **final deliverable a set of slides and bibliography**. Topics are available online under Discussions in the Final Presentation document– students will select one topic – no repeats.

There is a Rubric (grading criteria) posted online that describes the specifics of grading for all assignments, showing what is required to achieve a high grade.

Lessons Learned Document: Each student is also required to submit a **Lessons Learned** document, approximately 250 words in length, that describes some of the most important points that the student learned during the course. This should not just a recitation of the contents of the course, but rather a brief read-out on what the course has taught you. You may wish to discuss how you plan to apply the course material you have learned to your professional or even your private life. This is also an opportunity to reflect on how this course contributes to the value of the academic degree that you are seeking. The only “wrong” way to do this assignment is to NOT do it.

Expectations

Homework are expected to be submitted at the deadline via Blackboard.

This is a graduate course and since almost all of you are experienced you are expected to produce a quality materials.

Students are expected to attend all classes. If you will be absent, notify your professor as soon as you know you will miss class. More than one absence may impact your grade, especially as participation is a large portion of the grade.

Final Presentation: Researching your topic for your presentation. (Guidelines for the presentation and suggested topics are available on Blackboard.)

The Internet has led to a false sense of what research is all about. Those new to research tend to think that it means spending an afternoon surfing the Internet and then cutting and pasting from material available. Wikipedia is a fine first step, but is not to be quoted as a research-quality source. Your references should be high-quality journals, not sales materials or personal blogs.

Keep in mind the Internet is:

1. Not quality oriented.
2. The Internet has both good stuff and bad stuff, but does not know the difference.
3. I expect to see materials from a wide variety of sources, attributed as to source. Avoid using sales materials for your bibliography.

Deliverables on this Final Presentation: draft (see schedule for due date); hardcopy of presentation slides in Notes format at time of presentation; hardcopy bibliography.

Deadline Expectations

Due dates must be respected for assignments. It is unfair to other students to allow extensions for some. Issues that interfere with coursework such as work travel, home demands and vacations can all be anticipated. These pressures face everyone and are not sufficient reason for extensions to be offered. Extensions can only be granted under truly extenuating circumstances. Contact your instructor as soon as you think you will miss a deadline.

Security Reference links:

http://www.securitystrategy101.com

This site provides the basic of InfoSec as well as useful links

https://www.fireeye.com/current-threats/threat-intelligence-reports.html

Cyber Threat Intelligence Reports

http://www.ponemon.org/
Ponemon Institute conducts independent research on privacy, data protection and information security policy.

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/index.html
U.S. Department of Health & Human Services - enforcement data.

http://www.isaca.org/
The Information Systems and Control Association and Foundation. The guidelines and framework for the Control Objectives for Information Technology (COBIT) can be downloaded from this website

http://www.isc2.org/
The International Information Systems Security Certification Consortium.

http://www.cert.org
The website of the Computer Emergency Response Team at Carnegie Mellon University, USA.

http://www.attrition.org/
A web site for the collection, dissemination and distribution of information about computer security.

http://cve.mitre.org/
A web site with a database of standardized names for Common Vulnerabilities and Exposures in information systems.

http://www.htcn.org/
The High Tech Crimes Network – a somewhat complex home page leads into valuable information, training and testing facilities, conferences and technology issues.

http://www.csoonline.com/
CSO provides news, analysis and research on a broad range of security and risk management topics.

https://www.ic3.gov/default.aspx
Federal Bureau of Investigation – Internet Crime Complaint Center (IC3)

Grading Standards

Grade inflation is not in the best interests of BU students or the reputation of the institution. I have a responsibility to differentiate the performance of my students, and to reward with high grades only those who do exceptionally well. A Grade of 'A' or 'A minus' will be limited only to those students truly distinguishing themselves in the course. The Academic Policy Committee of Metropolitan College recommends the following guidelines for distinguishing grades.

A, A-	20%
B+, B, B-	80%
Other	As merited

While there are strict policies for grades at MET, I do NOT impose a grading curve.

You can expect to be challenged in this course, and excellent, high-quality work will be rewarded with an 'A'. If everyone submits high quality work, then everyone will get an 'A'. An 'A' grade requires high quality excellence in all aspects of the course: homework, class discussions, final project and exams.

Timely Presentation of Materials Due

All assignments (papers, homework, etc.) have due dates. These are the LAST DATES that stated material is due. I maintain the right to refuse, or downgrade, any materials presented after due dates. **This is not a subject for discussion**.

Organize your time and efforts- to turn in the work before the due date. To be absolutely clear, this means that the final paper will be accepted anytime up to that date but not after. Set a time schedule that has the work for the paper built around your personal needs and schedule a “hand in time” well before the last minute. This way, should some unforeseen problem arise, the timely presentation of your paper and its usefulness to the project is not in jeopardy.

If, for any reason, you are unable to meet any assignment deadline, contact me immediately, and preferably in advance. All assignments must be completed to receive full credit for the course.

6. Academic Conduct Policy

The academic conduct policy is summarized below. Cheating and plagiarism will not be tolerated in any Metropolitan College course. They will result in no credit for the assignment or examination and may lead to disciplinary actions. Please take the time to review the Student Academic Conduct Code:

For the full text of the academic conduct code, please go to:
http://www.bu.edu/met/metropolitan_college_people/student/resources/conduct/code.html

Academy Conduct Policy

For the full text of the academic conduct code, please go to http://www.bu.edu/met/metropolitan_college_people/student/resources/conduct/code.html

A Definition of Plagiarism

"The academic counterpart of the bank embezzler and of the manufacturer who mislabels products is the plagiarist: the student or scholar who leads readers to believe that what they are reading is the original work of the writer when it is not. If it could be assumed that the distinction between plagiarism and honest use of sources is perfectly clear in everyone's mind, there would be no need for the explanation that follows; merely the warning with which this definition concludes would be enough. But it is apparent that sometimes people of goodwill draw the suspicion of guilt upon themselves (and, indeed, are guilty) simply because they are not aware of the illegitimacy of certain kinds of "borrowing" and of the procedures for correct identification of materials other than those gained through independent research and reflection."

"The spectrum is a wide one. At one end there is a word-for-word copying of another's writing without enclosing the copied passage in quotation marks and identifying it in a footnote, both of which are necessary. (This includes, of course, the copying of all or any part of another student's paper.) It hardly seems possible that anyone of college age or more could do that without clear intent to deceive. At the other end there is the almost casual slipping in of a particularly apt term which one has come across in reading and which so aptly expresses one's opinion that one is tempted to make it personal property.

Between these poles there are degrees and degrees, but they may be roughly placed in two groups. Close to outright and blatant deceit-but more the result, perhaps, of laziness than of bad intent-is the patching together of random jottings made in the course of reading, generally without careful identification of their source, and then woven into the text, so that the result is a mosaic of other people's ideas and words, the writer's sole contribution being the cement to hold the pieces together. Indicative of more effort and, for that reason, somewhat closer to honest, though still dishonest, is the paraphrase, and abbreviated (and often skillfully prepared) restatement of someone else's analysis or conclusion, without acknowledgment that another person's text has been the basis for the recapitulation."

{The two paragraphs above are from H. Martin and R. Ohmann, The Logic and Rhetoric of Exposition, Revised Edition. Copyright 1963, Holt, Rinehart & Wins