

**CS684 - IT Security Policies and Procedures**  
**Instructor Joseph Burgoyne**

---

**Course Description**

**MET CS 684**

**IT Security Policies and Procedures**

This course enables IT professionals to implement security policies to support organizational goals. We discuss methodologies for identifying, quantifying, mitigating, and controlling security risks. Students learn to write IT risk management plans, standards, and procedures that identify alternate sites for processing mission-critical applications, and techniques to recover infrastructure, systems, networks, data, and user access.

The course also discusses disaster recovery; handling information security; protection of property, personnel and facilities; protection of sensitive and classified information; privacy issues; and hostile activities.




---

**Course Learning Objectives**

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
- 

**Course Outline**

- **Calendar Tool** - You can see many due dates in the Vista calendar tool . You may add your own events there as well. However, please be aware that you may not find all of the important dates for the course listed there. You will stay current by checking announcements, discussions, and emails in the course.
- **Readings** - Each module has both textbook readings and online lectures . Your professor may suggest additional readings during the running of the course.
- **Discussion** - There are threaded discussions  for each module. These discussions are moderated by your instructor. Postings for each discussion should be completed by the assigned due dates. There are also general discussions boards, which are not graded, for you to use to discuss any issues with your classmates. Please see the Discussion Module on the home page for more details.
- **Assignment** - There are assignments that are due throughout the course.

You may notice that the table of contents expands and contracts (+/- sign) and may conceal some pages. To avoid missing content pages, you are advised to use the next/previous page icons in the top right-corner of the learning modules.

### **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**

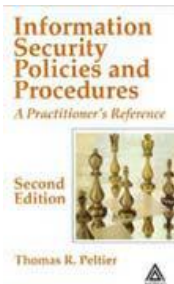
- Continuity and Disaster Recovery
- Preparing for I.T. Continuity
- Managing Disaster Recovery

### **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.

## Course Materials and Resources

### Required Course Books



Peltier, T. R. (2004). *Information security policies and procedures: A practitioner's reference* (2nd ed.). New York, NY/London: Auerbach Publications.  
ISBN-13: 978-0849319587



*Security Program and Policies: Principles and Practices, 2/E*  
Sari Greene  
ISBN-10: 0789751674 • ISBN-13: 9780789751676  
Published 03/19/2014

These textbooks can be purchased from [Barnes and Noble at Boston University](#).

### 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.

---

### Student/Class expectations

1. All work must be properly cited. Failure to cite work will result in a 0 and may be subject to additional disciplinary measures.
2. Assignments are due by 5:00 pm on the dates identified in the class syllabus.
  - In the event of some extraordinary event, students should notify the professor and request an extension of the deadline. If approved, a new date will be given to the student depending upon the circumstances.
  - Failure to pass assignments in on time will result in a loss of points. All grading is based on a 0 – 4.0 grading scale. For each day an assignment is late, the student will lose 1.0 from their total possible score. (ex. 1 day late – maximum score is a 3.0 or “B”)
3. Each student (D1) is expected to bring in a ‘current news’ article to class for discussion purposes.
4. EL students are expected to use the online discussion forums on a regular basis and to participate in class discussions while attending the 4 required class dates.
5. All students are expected to participate in classroom discussions.

## Study Guide

The following material is collected here for your convenience but the required readings, discussion particulars, and assignment particulars can be found within the modules, in the “Discussion” section of the course, and in the “Assignment” sections respectively.

### 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:** OL students are expected to use the on-line discussion forum

**Assignments:** Assignment 1 due – February 2, 2017 by 5:00 PM

### Module 2 Study Guide and Deliverables

**Readings:** *Greene: Chapter 2, pages 32 - 53*

Peltier: Primary: 47–80; Secondary: 199–241

**Discussions:** OL students are expected to use the on-line discussion forum

**Assignments:** Assignment 2 due – February 16, 2017 by 5:00 PM

### 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:** OL students are expected to use the on-line discussion forum

**Assignments:** Assignment 3 due - March 2, 2017 by 5:00 PM

### Module 4 Study Guide and Deliverables

**Readings:** *Greene: Chapter 11, pages 328 – 354*

Peltier: pages 341, 347–348, 350–358

**Discussions:** OL students are expected to use the on-line discussion forum

**Assignments:** Assignment 4 due - March 23, 2017 by 5:00 PM

### Module 5 Study Guide and Deliverables

**Readings:** *Greene: Chapter 12, pages 370 - 397*

**Discussions:** OL students are expected to use the on-line discussion forum

**Assignments:** Assignment 5 due April 6, 2017 by 5:00 PM

### Module 6 Study Guide and Deliverables

**Readings:** Peltier Page 34

**Discussions:** OL students are expected to use the on-line discussion forum

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

**Class Presentations:** Each student is required to present in class on a unique topic. Presentation details and topics will be available for students to choose. For those students in the EL class, presentations will be held on Thursday, April 27<sup>th</sup>. The D1 students will present on April 13<sup>th</sup> & 20<sup>th</sup>.

The grade for the course is determined by the following:

**Overall Grading Percentages**

**Grading Criteria**

Assessment Item(s)	% Final Grade
Assignments	40%
Class participation, online discussions & current events	30%
Final Class Presentation	30%
<b>Total Possible:</b>	<b>100%</b>

**Class Meetings, Lectures & Assignments**

*Lectures, Readings, and Assignments subject to change, and will be announced in class as needed.*

CS 684 D1/EL Spring 2017				
Class #1	19-Jan-17*	Module 1		
Class #2	26-Jan-17	Module 1		
Class #3	2-Feb-17	Module 2	Assignment 1 due (5:00 pm)	
Class #4	9-Feb-17	Module 2		
Class #5	16-Feb-17	Module 3	Assignment 2 due (5:00 pm)	
Class #6	23-Feb-17*	Module 3		
Class #7	2-Mar-17	Module 4	Assignment 3 due (5:00 pm)	
	9-Mar-17	Spring Recess		
Class #8	16-Mar-17	Module 4		
Class #9	23-Mar-17*	Module 5	Assignment 4 due (5:00 pm)	
Class #10	30-Mar-17	Module 5 & 6		
Class #11	6-Apr-17	D1 Final Presentations	Assignment 5 due (5:00 pm)	
Class #12	13-Apr-17		*Counts as the final	
Class #13	20-Apr-17	D1 Final Presentations	*Counts as the final	
Class #14	27-Apr-17*	EL Final Presentations	*Counts as the final	

*\*EL students required to attend these classes*

## Reference 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)