Syllabus

This is a single, concatenated file, suitable for printing or saving as a PDF for offline viewing. Please note that some animations or images may not work.

Course Description

This module is also available as a concatenated page, suitable for printing or saving as a PDF for offline viewing.

MET CS684

IT Security Policies and Procedures

This course enables IT professionals to manage cybersecurity and privacy programs across industries. Students will be introduced to cybersecurity & privacy policy frameworks, governance, standards, and strategy. We will review and discuss methodologies for identifying, quantifying, mitigating, and controlling risks. Risk management fundamentals and assessment processes will be reviewed in depth to understand risk tolerance is critical when building a cybersecurity and privacy program that supports business goals and strategies.

Asset classification and the importance of protecting Intellectual Property (IP) will prepare students to understand and identify protection mechanisms needed to defend against malicious actors, including industry competitors and nation states. Incident Response programs will cover preparation and responses necessary to triage incidents and respond quickly to limit damage from malicious actors.

This course covers many important topics that students need to understand in order to effectively manage a successful cybersecurity and privacy program.

Technical Notes

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.

This course requires you to access files such as Word documents, PDFs, and/or media files. These files may open in your browser or be downloaded as files, depending on the settings of your browser.

Course Learning Objectives

After successfully completing the course, you will be able to explain the following:

- The elements needed to effectively manage a cybersecurity and privacy program.
- Risk management—identification, quantification, response, and control.
- The importance of policy and governance within the cybersecurity and privacy program.
- Asset classification and the value of Intellectual Property.
- Security measures from Technology, Policy, and Practice; and Education, Training, and Awareness dimensions.
- Incident Response process and the importance of postmortem reviews.
- Why cybersecurity and privacy require alignment with business strategy and goals.

Instructor

Charles Pak, Ph.D.

Computer Science Department

Metropolitan College

Boston University

Email: cpak4@bu.edu

Charles Pak earned his Ph.D. in Information Security from Nova Southeastern University, an M.S. in Network Security from Capitol Technology University, and a B.S. in Electrical Engineering from Penn State University. He has taught Information Systems (IS) courses for over 25 years as an IS practitioner and professor. He has managed U.S. Federal Government data centers for over 20 years, including personnel. He has designed, tested, implemented, and maintained many of these enterprise network sites (largest in the world) that encompasses distributed sites across the U.S. as well as the international sites. He has managed state-of-the art systems for military and federal government missions for which he was deployed.

His research topics include Cyber Security, Critical Infrastructure Protection (CIP), PKI, Cyber Counter Terrorism, and Risk Assessment & Management. He has published several research papers in Information Security. As a practitioner, he holds several industry certifications: CISM, CRISC, CISSP, ITIL, SSCP, MCSE, MCT, and CCNA.

Recent Publications:

- Pak, C. (2011). Near Real-time Risk Assessment Using Hidden Markov Models. Nova Southeastern University, ProQuest Dissertations and Theses,ISBN:9781124992945.
- Pak, C. & Cannady, J. (2010). Risk Forecast Using Hidden Markov Models. Research in Information Technology (RIT), ACM, SIGITE, 7(2), 4-15.
- Pak, C. & Cannady, J. (2009). Asset Priority Risk Assessment Using Hidden Markov Models. Proceedings of the 10th ACM SIGITE, Fairfax, Virginia, 2009, 65-73.
- Pak, C. (2008). The near real time statistical asset priority driven (nrtsapd) risk assessment. Proceedings of the 9th ACM SIGITE, Cincinnati, Ohio, 2008, 105-112.

Areas of Expertise, Research Interests

Cybersecurity, Critical Infrastructure Protection (CIP), PKI, Cyber Counter Terrorism, and Risk Assessment & Management, Authentication Technologies, SCADA, Defense Cyber Protection

Work Experience as a Cybersecurity Solution Expert

Dr. Pak is an industry practitioner working for the DoD Cybersecurity Protection, and a scholar delivering a 35-years of hands-on practice and theory to our students. He delivers cybersecurity industry solutions to warfighters to defend the nation’s cybersecurity, cyber warfare, cyberterrorism, cybercriminals, critical protection. He is an industry proven mentor who has done 35 years of engineering, IT, cybersecurity for the government clients. Students look for a mentor who has a deep industry and scholarly background and provide them guidance on how to tackle real problems. With real-world based lab assignments, research papers, reading lecture materials and live lectures, students build their talent to tackle real cybersecurity challenges.

MET Teaching Highlights

Dr. Pak teaches CS695, 690, 625, 674, 682, 684. Our students are most interested in the CS695’s real-world hands-on lab project assignments as these assignments are directly applicable to their work place.

Course Contributor

Joseph Burgoyne

Computer Science Department
Metropolitan College
Boston University
1010 Commonwealth Ave
Boston, MA 02215

Office Hours: By Appointment
Office Phone: (978) 758-7665
Email: josephb@bu.edu

Joe Burgoyne is the Senior Director of Cybersecurity at GE Healthcare; he is responsible for vulnerability and patch management, as well as policies and programs for medical devices and solutions. Working with healthcare industry leaders, government, and regulatory organizations, including AAMI, MITA, HSCC, FDA, MITRE, and CISA, Joe contributes to industry best practices and standards as a subject matter expert.

With over 23 years of security experience, Joe has built a successful career by collaborating with business stakeholders, building trust, establishing security programs, and applying practical solutions to reduce risks to an acceptable level.

In previous roles, Joe has been responsible for information and physical security, privacy, and crisis management. Other specialties include eDiscovery, litigation support, criminal investigations, export control and compliance, ITAR, and workplace violence. Joe has worked closely with Federal, State, and local law enforcement throughout his career. While currently serving as an advisory board member, Joe was also a past director and President Emeritus for the InfraGard Boston Members Alliance, Inc., supporting public and private information sharing to protect the U.S. critical infrastructure sectors. Joe enjoys presenting and speaking within the enterprise and medical device cybersecurity community on cyber threats, trends, policy, and risk mitigation strategies. Since 2012, Joe has been working at Boston University as an adjunct professor, sharing his passion for security and helping

Course Outline

Module 1: Information

- Security & Privacy Introduction
- Introduction to Information Security & Privacy
- Cyber Threats & Actors
- Law & Ethics

Module 2: Policy Framework

- The Policy Framework
- Policy Elements & Hierarchy
- U.S. and International Standards Organizations

Module 3: Developing the Security Program

- Planning the Security Program
- The Written Information Security Program (WISP)

Module 4: Risk Management

- The Risk Assessment Process
- Assessing Risk Within the Organization

Module 5: Asset Management & Information Classification

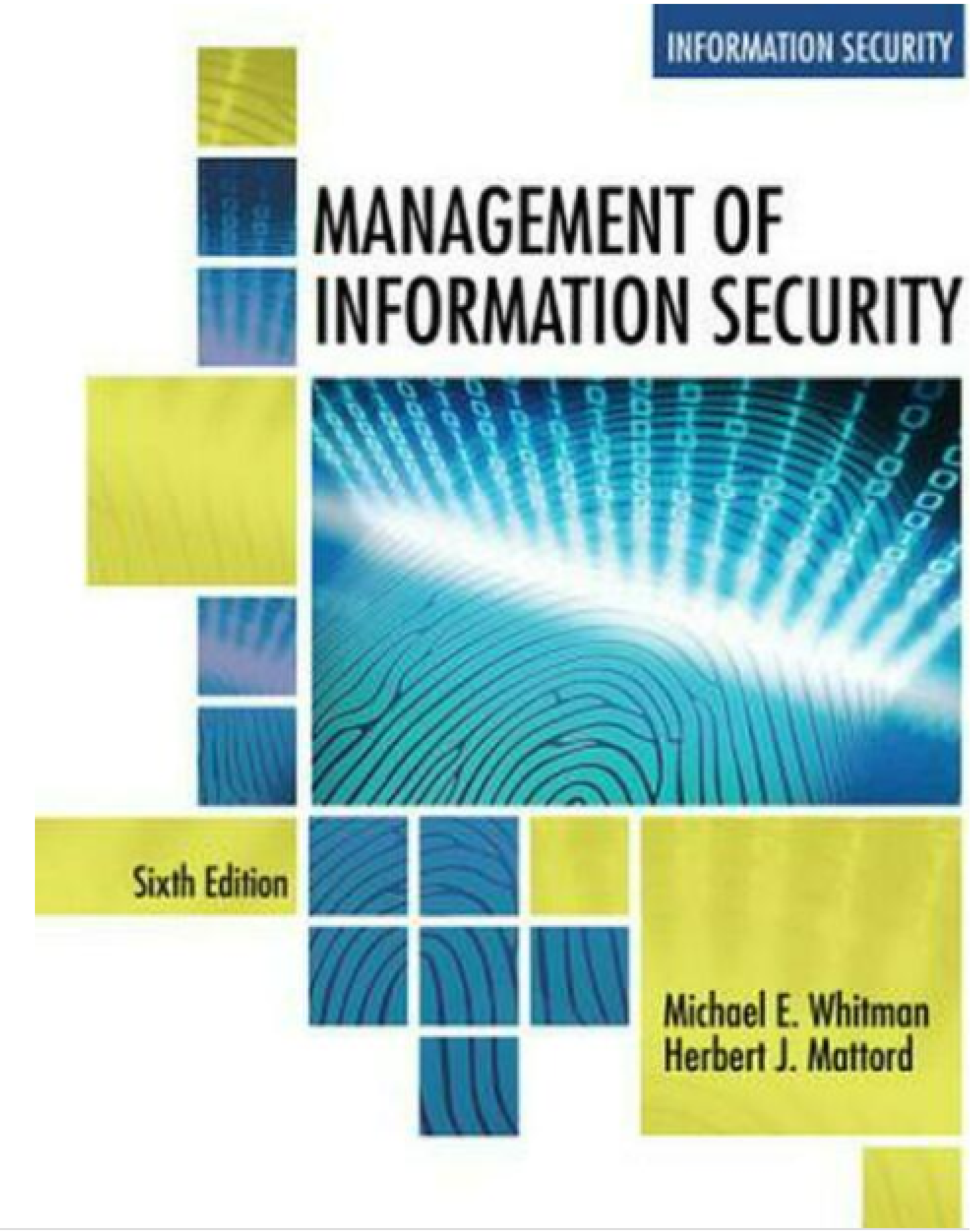
- Asset Classification
- Protected Personal Information
- Privacy Concerns and Considerations within Cloud Environments

Module 6: Incident Response & Disaster Recovery

- Incident Response Overview
- Disaster Recovery Planning

Materials

Required Books

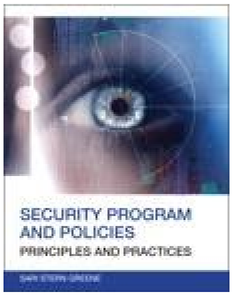


Michael E. Whitman, Herbert J. Mattord

Management of Information Security, 6th Edition (2019).

ISBN-10: 133740571X

ISBN-13: 9781337405713



Sari Greene

Security Program and Policies: Principles and Practices, 2nd Edition (2014).

ISBN-10: 0789751674

ISBN-13: 9780789751676

These books can be purchased from Barnes and Noble at Boston University.

Boston University Library Information

Boston University has created a set of videos to help orient you to the online resources at your disposal. An introduction to the series is below:

met_ode_library_14_sp1_00_intro video cannot be displayed here

All of the videos in the series are available on the Online Library Resources page, which is also accessible from the Campus Bookmarks section of your Online Campus Dashboard. Please feel free to make use of them.

As Boston University students, you have full access to the BU Library. From any computer, you can gain access to anything at the library that is electronically formatted. To connect to the library, use the link http://www.bu.edu/library. You may use the library's content whether you are connected through your online course or not, by confirming your status as a BU community member using your Kerberos password.

Once in the library system, you can use the links under “Resources” and “Collections” to find databases, eJournals, and eBooks, as well as search the library by subject. Some other useful links follow:

Go to Collections to access eBooks and eJournals directly.

If you have questions about library resources, go to Ask a Librarian: Help & FAQs to email the library or use the live-chat feature.

To locate course eReserves, go to Reserves.

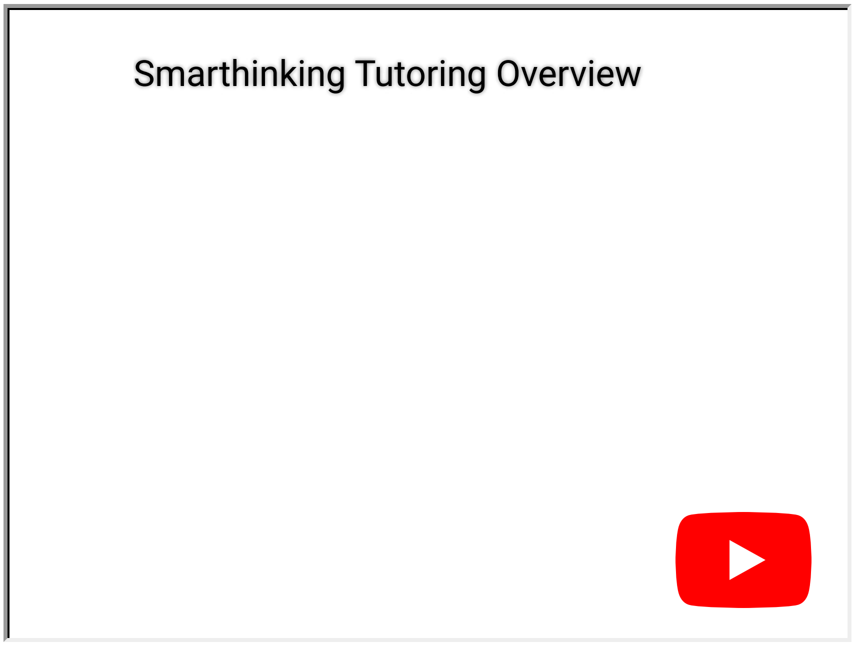
Please note that you are not to post attachments of the required or other readings in the water cooler or other areas of the course, as it is an infringement on copyright laws and department policy. All students have access to the library system and will need to develop research skills that include how to find articles through library systems and databases.

Free Tutoring Service

smarthinking

Free online tutoring with Smarthinking is available to BU online students for the duration of their courses. The tutors do not rewrite assignments, but instead teach students how to improve their skills in the following areas: writing, math, sciences, business, ESL, and Word/Excel/PowerPoint.

You can log in directly to Smarthinking from Online Campus by using the link in the left-hand navigation menu of your course.



YouTube

Please Note

Smarthinking may be used only for current Boston University online courses and career services. Use of this service for purposes other than current coursework or career services may result in deactivation of your Smarthinking account.

Study Guide

This course starts on a **Tuesday**. The modules in this course run from **Tuesday to Monday**.

Week 1 Study Guide and Deliverables

Topics:	• Information Security & Privacy introduction and overview • Cyberattacks – methods and actors • Understanding the changing threat landscape • Law & Ethics
Readings:	• Whitman/Mattord, pp. 1-55, 78-104
Discussions:	• Discussion 1 posts due **Tuesday, November 8 at 6:00 AM ET**

Assignments:

- Assignment 1 due **Tuesday, November 8 at 6:00 AM ET**

Live Classroom:

- **Tuesday, November 1 at 7:00 PM ET**

Week 2 Study Guide and Deliverables

Topics:

- The Policy Framework
- Policy Elements and Hierarchy
- U.S. and International Standards Organizations

Readings:

- Whitman/Mattord, pp. 169-214
- Greene, pp. 2-21, 32-53, 64-82

Recommended External Readings:

- NIST information security framework
- NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management
- American National Standards Institute, ANSI
- International Organization for Standardization, ISO

Discussions:

- Discussion 2 posts due **Tuesday, November 15 at 6:00 AM ET**

Assignments:

- Assignment 2 due **Tuesday, November 15 at 6:00 AM ET**

Live Classroom:

- **Tuesday, November 8 at 7:00 PM ET**

Week 3 Study Guide and Deliverables

Topics:

- Planning the Security Program
- The Written Information Security Program (WISP)

Readings:

- (Whitman/Mattord, pp. 123-164, 197-214)

Recommended External Readings:

- 201 CMR 17.00 COMPLIANCE CHECKLIST

Discussions:

- Discussion 3 posts due **Tuesday, November 22 at 6:00 AM ET**

Assignments:

- Assignment 3 due **Tuesday, November 22 at 6:00 AM ET**

Live Classroom:

- **Tuesday, November 15 at 7:00 PM ET**

Week 4 Study Guide and Deliverables

Topics:	• The Risk Assessment Process • Assessing Risk Within the Organization
Readings:	• Greene, pp. 105-112 • Whitman/Mattord, pp. 303-316, 365-406
Recommended External Reading:	• Cybersecurity
Discussions:	• Discussion 4 posts due **Tuesday, November 29 at 6:00 AM ET**
Assignments:	• Assignment 4 due **Tuesday, November 29 at 6:00 AM ET**
Live Classroom:	• **Tuesday, November 22 at 7:00 PM ET**

Week 5 Study Guide and Deliverables

Topics:	• Asset Classification • Protected Personal Information (PII) • Privacy Concerns and Considerations Within Cloud Environments
Readings:	• Greene, pp. 442-470 • Whitman/Mattord, pp. 381-393
Recommended External Readings:	• Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories • Specification for Asset Identification 1.1
Discussions:	• Discussion 5 posts due **Tuesday, December 6 at 6:00 AM ET**
Assignments:	• Assignment 5 due **Tuesday, December 6 at 6:00 AM ET**
Live Classroom:	• **Tuesday, November 29 at 7:00 PM ET**

Week 6 Study Guide and Deliverables

Topics:	• Incident Response Overview • Disaster Recovery Planning • Privacy Breach Notifications

- Incident Response Planning

Readings:

- Whitman/Mattord, pp. 497-562

Recommended External Readings:

- Cybersecurity
- Introduction to Information Security
- Incident Management
- Business Continuity Plan
- Crisis Communications Plan
- IT Disaster Recovery Plan
- CRR Supplemental Resource Guide

Discussions:

- Discussion 6 posts due **Tuesday, December 13 at 6:00 AM ET**

Assignments:

- Assignment 6 due **Tuesday, December 13 at 6:00 AM ET**

Course Evaluation:

Course Evaluation opens on **Tuesday, December 6, at 10:00 AM ET** and closes on **Tuesday, December 13 at 11:59 PM ET**.

Please complete the course evaluation. Your feedback is important to MET, as it helps us make improvements to the program and the course for future students.

Live Classroom:

- **Tuesday, December 6 at 7:00 PM ET**

Final Exam Details

The Final Exam is a proctored exam available from **Wednesday, December 14 at 6:00 AM ET to Saturday, December 17 at 11:59 PM ET**.

The Computer Science department requires that all final exams be administered using an online proctoring service called Examity that you will access via your course in Blackboard. Detailed instructions regarding your proctored exam will be forthcoming from the Assessment Administrator. You will be responsible for scheduling your own appointment within the defined exam window.

The Final Exam will be **open book/open notes** and is accessible only during the final exam period. You may bring notes and other materials to the exam.

You can take the exam only once. The exam features **essay questions**.

Final Exam Duration: **3 hours**. There is a clock in the upper right corner of the screen keeping time for the exam.

Course Grading Information

Please check the **Study Guide** in the syllabus for Live Classroom dates and specific due dates for assignments and assessments.

Grading Policy

All students will be expected to demonstrate knowledge of IT Security Policies and Procedures. To obtain an exceptional grade you have to exceed expectations in your assignments, discussions and proctored final exam.

Grading Structure and Distribution

The grade for the course is determined by the following:

Overall Grading Percentages	
Assignments	40%
Discussions	30%
Proctored Final Examination	30%
Total Possible	**100%**

The next table shows the minimum points for each letter grade, which is a slightly augmented form of the registrar's system. To get a B+ for the course, for example, your course points should be at least 3.3. The only exception is that to obtain an A for the course, a score of 3.85 or more is required.

The following grade structure (the university's, with two refinements) will be applied for your assignments:

Grading Scale		
Letter Grade	**100 pt. scale**	**4 pt. scale**
A	95-100	3.85 - 4.0
A-	90-94	3.7 – 3.84
B+	86-89	3.3 – 3.69
B	82-85	3.0 – 3.29

B-	78-81	2.7 – 2.99
C+	74-77	2.3 – 2.69
C	70-73	2.0 – 2.29
C-	67-69	1.7 – 1.99
D	60-66	1.0 – 1.69
F	0-59	0.0 – 0.99

Assignments

Your homework assignments are an integral part of the learning process. You will receive feedback from your facilitator for each assignment. Please review the assignment rubric.

Criteria	**C or lower**	**B- (2.7-2.99)**	**B (3.00-3.29)**	**B+ (3.30-3.69)**	**A- (3.7-3/84**	**A (3.85-4.00)**
Thoroughness & Coverage	Hardly covers any of the major relevant issues.	Covers some of the major relevant issues	Reasonable coverage of the major relevant areas.	Good coverage of the major relevant areas.	Thorough coverage of almost all of the major relevant areas.	Exceptionally thorough coverage of all major relevant issues.
Depth, Understanding, & Insight	Lack of understanding, or lack of insight into material.	Some understand of material.	Good overall understanding of material.	Very good overall understanding of material.	Very good overall understanding of material, with some real depth.	Excellent, deep understanding of material and its interrelationships.
Relevance & Significance	Focus is off topic or on insubstantial or secondary issues.	Some of the content is meaningful and on topic.	Most of the content is reasonably meaningful and on topic.	All content is reasonably meaningful and on-topic.	All content is meaningful and relevant to the case.	All content is exceptionally relevant and meaningful.

Criteria	C or lower	B- (2.7-2.99)	B (3.00-3.29)	B+ (3.30-3.69)	A- (3.7-3/84	A (3.85-4.00)
Persuasiveness & Clarity	Disorganized or hard to understand presentation.	Some parts of the presentation are disorganized or hard to understand.	Generally organized and clear.	Organized and persuasive presentation of ideas.	Very clear, organized, and persuasive presentation of ideas.	Exceptionally clear, organized, and persuasive presentation of ideas.
Creativity & Innovativeness	Little significant or reasonably backed creative or innovative points-of-view or ideas.	Few creative and innovative ideas or points-of-view that are reasonable and are backed by some analysis.	Good, and fairly creative ideas or points-of-view that are perceptive and are backed by good analysis.	Very good, creative, and innovative ideas or points-of-view that are perceptive.	Very good, creative, and innovative ideas or points-of-view that are perceptive and are backed by strong analysis.	Outstanding, creative, and innovative ideas or points-of-view that are perceptive and are backed by very strong analysis.
Utilization of Source Materials	No useful references, or weak references with incorrect details or applicability.	Some use of source material and/or some details or applicability is incorrect.	References indicate research.	Good references applied usefully.	References indicate strong research used well.	References indicate exceptional researched used persuasively.

Discussions

Graded Discussions - you will participate in discussions that will be graded using the A = 4.0, B = 3.0, etc. scale described above. Each week’s discussions are to concern only the online notes or the textbook readings. The post subject should be the relevant section, e.g, “5.9 **Real-Life Security Procedures”**

Graded discussion periods are held from Tuesday of each module until 6:00 AM ET on Tuesday of the following module. You are certainly welcome to continue a discussion past the grading period, but that additional posted material will not affect your discussion grade.

Relevance	This criterion is designed to keep you focused. It concerns the degree to which your postings are relevant to the week's material. Meaningful questions about material in the notes or the book may qualify also. (This should be an easy way for you to keep your discussion grade in reasonable territory.)
Degree of substance	This assesses the management or technical content of your posts, taken as a whole. This is most commonly achieved by putting the content of the notes or books in your own words or by giving examples that you have come across. Meaningful questions about material in the notes or the book may qualify also. Normally, interactive posts with no management or technical content will not count against you here (e.g., we encourage you to let a fellow student know that you found a post interesting or useful).
Usefulness of your week's contributions for the rest of your group	This evaluates how useful to your fellow students the totality of your comments and questions are in the context of each week's specified focus. "A" work will result from a significant set of comments and questions that are very useful to you and to the class. This criterion encourages you to be *participatory* (e.g., by responding to good questions or points posed by others). You should have an *even rate* of substantive postings throughout the week. (Contributions posted only at the end of the week are far less useful to your classmates.) If your posts are *long*, they are less likely to be read by others, and this *reduces their usefulness*. This is the only criterion affected by quantity. For example, if you make no posts, they can't be called useful.

Proctored Final Exam

There will be a proctored Final Exam in this course using a proctor service called Examity. Detailed instructions regarding your proctored exam will be forthcoming from the Assessment Administrator. You will be responsible for scheduling your own appointment.

Expectations

Many learning activities require sharing your assignments and opinions with your classmates. It is, therefore, very important that you, as well as your classmates, submit assignments on a timely basis. Due dates will be indicated for each assignment in the Assignments section of the course.

Delays

If, for any reason, you are unable to meet any assignment deadline, contact your Course Facilitator. All times mentioned in the course (unless otherwise specified) are in Eastern Time. All assignments must be completed and must be turned in by their due dates and due times. Extensions may be granted, though only under mitigating circumstances.