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 CS695

Enterprise Cyber Security

The goal of this course is to prepare students to perform security related tasks and contribute to organizational security related activities. Formal and technical aspects of information, computer and network security are presented and explained along with examples of real world systems, thereby enabling the student to relate theoretical approaches and both procedural and technical control implementations to meet the security requirements of enterprises.

The course provides an in-depth presentation of security issues in computer systems, networks, and applications. The concept of information security governance is presented and discussed. The basic concepts of security services, and the role played by encryption and hash algorithms are discussed along with issues and approaches for key management. Formal security models are explained and illustrated on operating system security aspects, more specifically memory protection, access control and authentication, file system security, backup and recovery management, intrusion and virus protection mechanisms. Application level security focuses on language level security and various security policies; conventional and public keys encryption, authentication, message digest and digital signatures. Internet and intranet topics include security in IP, routers, proxy servers, both packet filtering firewall and application-level gateway firewalls, Web servers, file and mail servers. Discussion of remote access issues, such as dial-up servers, modems, VPN gateways and clients are included.

Prerequisites

Knowledge of information technology fundamentals (computer hardware, operating systems, applications and networking) is required. Successful completion of MET CS625, CS535, or permission of the instructor is also required.

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

Upon successful completion of this course you will be able to:

- Understand and be able to discuss the general concepts of information security governance and the importance of balancing the use of security policy, processes, technology and operations to mitigate organizational security risks.
- Develop detailed security requirements based on market/business needs, threat profiles, security policy obligations and asset vulnerabilities/exposure.
- Perform asset assessments, determine probable threats and risks that drive solution architectural alternatives, trade-off studies, modeling and design issues.
- Prepare service/product security architectures and designs that sufficiently comply with enterprise security requirements thereby minimizing risks to acceptable cost levels.
- Plan operational security procedures, ensure operations security activities comply with policy, along with conducting periodic security reviews and audits.
- Support product/service development, integration and procurement activities ensuring that selected components, when deployed, will comply with the organizational detailed security requirements.

Course Outline

- **Calendar Tool**—You can see many due dates in the 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. Your study guide will provide the details of most of your readings and deliverables.
- **Readings**—Each module may have both textbook readings and online lectures. The details are in the study guide and on the first page of each module. 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.
- **Assessments/Quizzes**—Quizzes are also listed in the course calendar and accessed from the Assessments menu.

- **Labs**—Students will be required to complete a number of lab exercises as part of selected assignments. These lab exercises must be submitted as separate Word documents at the same time as the assignments.

Module 1

- **Lecture 1**—Branches of security, Defining security by function, The Common Body of Knowledge (CBK) Security Domains, An example of security failures, Why every employee has a role in achieving information security, Introduction to security related terminology.

- **Lecture 2**—What is Systems Engineering: Stating the Problem, Investigate Alternatives and Model the System, Integrate, Launch the system, Assess performance, Re-evaluate, Process Variations. Process Management: ISO 9000 Processes and Procedures, Capability Maturity Model (CMM). Organization Environments: Regulations/Legislation, Technology Evolution, Customers demands and expectations, Legal Liability, Competition, Terrorism or Cyber crime. Business/Organizational Types: Commercial enterprises, Residential, Governmental, Non-Governmental Organizations (NGOs), National Critical Infrastructure

Module 2

- **Lecture 3**—Role of Cryptography in Information Security, Application of Services, Human Authentication and the concept of Factors, Cryptography, Cryptanalysis and Key Management.

- **Lecture 4**—Cryptographic Authentication, Authentication Systems: Kerberos Based Authentication, Public Key Infrastructures and human authentication.

Module 3

- **Lecture 5**—Security policy development, security process management (governance) and associated standards, Security Policies, Risk management spanning assets, attack analysis and risk mitigation, Security requirements analysis and decomposition. Access control concepts, Security modeling and security related standards.

- **Lecture 6**—Traditional networking architectures, Types of networks (LANs, MANs, WANs), Network protocols, Data Link Layer complexity, The Insecurity of ARP, IP and the network Layer, Transport Protocols and protocol vulnerabilities and protocol internal security mechanisms

Module 4

- **Lecture 7**—Next generation networking concepts and related security mechanisms.

- **Lecture 8**—Generic security Related Hardware: Processor States and Status, Memory Addressing, Registers and Architectures, Interruption of Processor Activity, Operating Systems (OSs), The Security Kernel and Rings of protection, Memory and Address Protection, Fences, Relocation, Base/Bound Registers, Segmentation, Paging

Module 5

- **Lecture 9**—Unix Type OS Security Capabilities. Solaris Security Capabilities and RBOC, Real-Time OS Security Capabilities, Microsoft Windows Security Capabilities. Applications software development security, malicious software (malware) and countermeasures.
- **Lecture 10**—Layer 2 Network Security mechanisms (802.1q, 802.1x, 802.1i), Layer 3 Network Security mechanisms (IPsec, Firewalls, Intrusion Protection).

Module 6

- **Lecture 11**—Layer 4 Network Security mechanisms (TLS, SSL, DTLS, SSH), Application Layer Network Security mechanisms (Email, XML, SAML/IdM, VoIP & SBCs), Application Framework Security mechanisms (CORBA, DCE, Java.NET).
- **Lecture 12**—Security of Network Services (DNS, NTP, Active Directory), Penetration Testing, Network and Security management. NGOSS and eTOM.
- **Lecture 13**—Operational Security Compliance. Systems implementation, procurement and decommissioning.

Module 7 - Prepare for and take the final exam

You will prepare for and take the proctored final exam.

The course will remain open two weeks after the final exam, so that you can continue discussions and ask any questions about database technology, your grades or the course. This is also a time when we enter into a dialog where we endeavor to learn from you how we can modify the course so that it better meets your needs.

Instructor

Charles Pak, Ph.D.

Computer Science
Department
Metropolitan College
Boston University
808 Commonwealth Ave, 2nd floor
Boston, MA 02215

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.

Course Materials

Required Book

Jacobs, S. (2016). ***Engineering information security: The application of systems engineering concepts to achieve information assurance*** **- Second Edition.**
Wiley-IEEE Press.

ISBN-13: 978-1119101604
ISBN-10: 1119101603

This book covers the subject area of information security from an engineering perspective.

Physical copies of the textbook by Jacobs are sold at Barnes and Noble at Boston University, though an electronic version is available for free through the BU Library. Students can find the book at this link: http://ieeexplore.ieee.org/servlet/opac?bknumber=7362912. After logging in using your BU credentials,

To access the eBook:

1. Go to bu.edu/library and search the title of the book “Engineering Information Security” in the general search box.
2. The first result should be the one you’re looking for. Click it, then identify the 2015 edition and click “online access available.”
3. On the screen that opens, click “Sign in,” then enter your BU user name and password. Once this is done, it should return you to that same page you were on previously.

4. Click the IEEE Xplore link, and it should open the page you're looking for, with each of the chapters now unlocked.
5. After logging in, you can navigate the chapters by using the table of contents at the bottom of the page.

Books and References for Further Study

The following books are not required for this course. However you will find each to be valuable resources to anyone involved in the Information Security area.

The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2nd edition, R.L. Krutz, and R. D. Vines, Wiley, 2004. ISBN: 0471413569
The above book is very useful should you decide to sit for the CISSP examination to prepare you for the style and level of detail of questions in the six hour exam.

Firewalls and Internet Security, Repelling the Wily Hacker, William R. Cheswick, and Steven M. Bellovin, Addison-Wesley, 1994
The above book is a classic for its very detailed treatment for statefull firewalls and DMZs and is still relevant today.

Practical UNIX & Internet Security, 2nd Edition, ,Simson Garfinkel and Gene Spafford: O'Reilly, 1996
The above book is a classic for its very detailed treatment of general networking security and hardening of unix typs operating systems and is still relevant today.

Hacking Expose Network Security Secrets & Solutions, 2nd Edition, Joel Scambray, Stuart McClure, and George Kurtz, McGraw-Hill, 2001
The above book provides an interesting look into those involved in malware and some of the techniques used for breaching targeted systems.

Security Engineering; A Guide to Building Dependable Distributed Systems, Ross Anderson, Wiley, 2001
The above book is an interesting collection of discussions on security engineering and associated challenges.

Computer Related Risks, Peter G. Neumann, Addison-Wesley, 1995
The above book is one of the definitive texts on the basic concepts of what constitutes risks, especially information security risks.

Applied Cryptography, Bruce Schneier, 2nd Edition, Wiley & Sons, 1996
The above book is an excellent source for details on most any encryption algorithm you are likely to encounter. Most any version, starting with the 2nd edition, will be invaluable.

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 is displayed here

Download

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.

Journals & conferences/proceedings in Information Security

- Computer Security Update
- European Conference on Information Warfare and Security
- IEEE Transactions on Dependable and Secure Computing
- Information Security Journal
- Information Security Management Principles
- Inside Cybersecurity
- International Conference on Information Warfare and Security
- International Journal of Computer Science and Information Security
- International Journal of Information Security
- Journal of Information Privacy & Security
- SC Magazine

Portals

- ACM Digital Library
- Proceedings of the IEEE

Additional links for searching

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 http://www.bu.edu/library/research/collections to access eBooks and eJournals directly.

If you have questions about library resources, go to http://www.bu.edu/library/help/ask-a-librarian to email the library or use the live-chat feature.

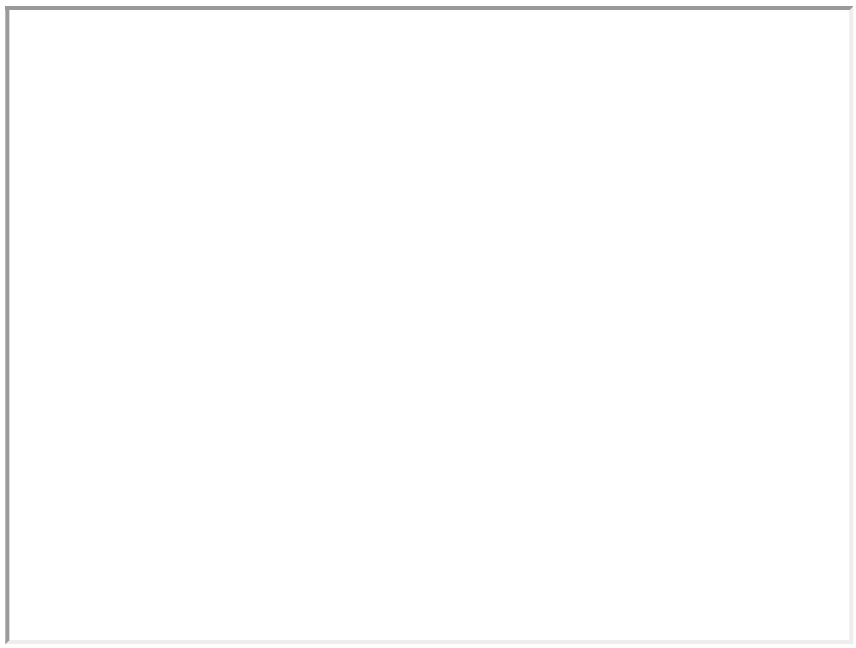
To locate course eReserves, go to http://www.bu.edu/library/services/reserves.

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

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

Module 1 Study Guide and Deliverables

Readings:	*Engineering Information Security*: Chapter 1 What is Security, Chapter 2 Systems Engineering "Systems Engineering Fundamentals," Defense Acquisition University Press, 2001, chapters 1 through 13 (SEFGuide01-01.pdf) Students are not expected to read this document in detail, students are expected to become familiar with what the document covers so they become aware of the document's value and possible applicability in their professional activities.
Assignments:	Assignment 1 and Lab 1 due Tuesday, January 23 at 6:00 AM ET
Assessments:	Quiz 1 due Tuesday, January 23 at 6:00 AM ET
Discussions:	Module 1 Discussion posts due Tuesday, January 23 at 6:00 AM ET. Any posts after the due time will not be included in the grading process.
Live Classroom:	Thursday, January 18, at 8:00 PM ET

Module 2 Study Guide and Deliverables

Readings:	*Engineering Information Security*: Chapter 3 Foundation Concepts, Chapter 4 Authentication of Subjects Security Architecture for Open Systems Interconnection for CCITT Applications (ITU-TRecommendationX0800-91.pdf) Students are not expected to read this document in detail, students are

	expected to become familiar with what the document covers so they become aware of the document's value and possible applicability in their professional activities.
Assignments:	Assignment 2 and Lab 2 due Tuesday, January 30 at 6:00 AM ET
Assessments:	Quiz 2 due Tuesday, January 30 at 6:00 AM ET
Discussions:	Module 2 Discussion posts due Tuesday, January 30 at 6:00 AM ET. Any posts after the due time will not be included in the grading process.
Live Classroom:	Thursday, January 25, at 8:00 PM ET

Module 3 Study Guide and Deliverables

Readings:	*Engineering Information Security*: Chapter 5 Security Systems Engineering, Chapter 6 Traditional Network Concepts DoD Trusted Computer System Evaluation Criteria, sections 1.0 through 8.0 (5200.28-STDTheOrangeBook.pdf) Proposed NIST Standard for Role-Based Access Control, sections 1 through 6 (rbacSTD-ACMProposedRBACStandard.pdf) Students are not expected to read these two documents in detail, students are expected to become aware of the documents' value and possible applicability in their professional activities.
Assignments:	Assignment 3 and Lab 3 due Tuesday,

	February 6 at 6:00 AM ET
Assessments:	Quiz 3 due Tuesday, February 6 at 6:00 AM ET
Discussions:	Module 3 Discussion posts Tuesday, February 6 at 6:00 AM ET. Any posts after the due time will not be included in the grading process.
Live Classroom:	Thursday, February 1, at 8:00 PM ET

Module 4 Study Guide and Deliverables

Readings:	*Engineering Information Security*: Chapter 7 Next Generation Networks, Chapter 8 General Computer Security Architecture
Assignments:	Assignment 4 and Lab 4 due Tuesday, February 13 at 6:00 AM ET
Assessments:	Quiz 4 dueTuesday, February 13 at 6:00 AM ET
Discussions:	Module 4 Discussion posts dueTuesday, February 13 at 6:00 AM ET. Any posts after the due time will not be included in the grading process.
Live Classroom:	Thursday, February 8, at 8:00 PM ET

Module 5 Study Guide and Deliverables

Readings:	*Engineering Information Security*: Chapter 9 Computer Software Security, Chapter 10 Security Systems Design – Designing Network Security
Assignments:	Assignment 5 and Lab 5 due Tuesday,

	February 20 at 6:00 AM ET
Assessments:	Quiz 5 due Tuesday, February 20 at 6:00 AM ET
Discussions:	Module 5 Discussion posts due Tuesday, February 20 at 6:00 AM ET. Any posts after the due time will not be included in the grading process.
Live Classroom:	Thursday, February 15, at 8:00 PM ET

Module 6 Study Guide and Deliverables

Readings:	*Engineering Information Security*: Chapter 11 Transport & Application Security Design and Use, Chapter 12 Securing Management and Managing Security
Assignments:	Assignment 6 due Tuesday, February 27 at 6:00 AM ET
Assessments:	Quiz 6 due Tuesday, February 27 at 6:00 AM ET
Discussions:	Module 6 Discussion posts due Tuesday, February 27 at 6:00 AM ET. Any posts after the due time will not be included in the grading process.
Live Classroom:	Thursday, February 22, at 8:00 PM ET

Final Exam Details

The Final Exam is a proctored exam available from **Wednesday, February 28 at 6:00 AM ET to Saturday, March 3 at 11:59 PM ET**. The Computer Science department requires that all final exams be proctored.

You will be responsible for setting up your own appointment with an approved proctoring option. Further information about the testing centers will be forthcoming from the exam coordinator.

The exam will only be accessible during the final exam period. You can access it from the Assessments section of the course. Your proctor will enter the password to start the exam.

You will receive a technical support hotline number before the start of the exam. Please bring this number with you to the exam.

Course Grading Information

It is important for each student to participate on a regular basis and complete all aspects of this course. This course is designed to include a major portion of learning by interacting (asynchronously) with the other students in the class, and the grade is therefore dependent on this activity. Course quizzes are cumulative in what they cover. This means that a quiz may include questions on material from prior modules.

Grading Structure and Distribution

The following tables depict how final grades will be calculated. Only exceptions necessary to maintain academic standards will be allowed.

Overall Grading Percentages	
Homework Assignments	25
Quizzes	20
Lab exercises	10
Discussion thread participation	10
Proctored final exam	35

Grading Scale	
A	94 ≤
A-	90 ≤ and < 94
B+	87 ≤ and < 90
B	84 ≤ and < 87

B-	80 ≤ and < 84
C+	77 ≤ and < 80
C	74 ≤ and < 77
C-	70 ≤ and < 74
F	≤ 70

Homework Assignments and Lab Exercises

- Both homework assignments and lab exercises: are mandatory, must be completed and submitted in a timely manner, and are required to be submitted via Online Campus for this course;
- For each day after the submission date a homework assignment or lab exercise is due will result in a penalty of 3 points;
- Homework assignments or lab exercises passed in that are over 5 days late will receive a grade of zero (0);
- All homework assignments or lab exercises are identified within the Online campus Study Guide.
- File names for assignment documents should be:

  CS695-HW<number>-<student last name>.doc

  An example assignment document file name is:

  CS695-HW5-Jacobs.doc

- File names for lab exercise documents should be:

  CS695-LAB<number>-<student last name>.doc

  An example lab exercise document file name is:

  CS695-LAB5-Jacobs.doc

- Student work submissions must be no more than 4 pages in length, be , single spaced**,** use 12 point Times Roman type font and 1” margins on all sides.
- Include your name and assignment number in the header and a page number in the footer of you assignment submission document.
- Title cover pages are not required.
- Assignment submission documents MUST be in Word format with the file extension .doc, rather than .docx.
- Quoted material and citations must follow the American Psychological Association (APA) format with a reference section at the end of a student's submitted work. Please refer to the http://www.apastyle.org/ web site for guidance on following the APA style guide.
- Wikipedia is a useful starting point for finding information about a subject BUT NOT an acceptable direct reference source. One should only reference or quote from primary (source) documents.

Delays

In the case of serious or emergency situations, or if, for any reason, you are unable to meet any assignment deadline, contact your instructor.

Discussion Grading Rubric

Graded discussion periods are held Day 1 of each module until 6:00 AM ET on Day 1 of the following module. You're certainly welcome to continue a discussion past the grading period, but that additional posted material will not affect your discussion grade. The discussion grading rubric below is the guide we use to evaluate your discussion contributions.

Discussion Grading Rubric					
Criteria	51–60	61–70	71–80	81–90	91–100
Participation	Very limited participation	Participation generally lacks frequency or relevance	Reasonably useful relevant participation during the discussion period	Frequently relevant and consistent participation throughout the discussion period	Continually relevant and consistent participation throughout the discussion period
Community	Mostly indifferent to discussion	Little effort to keep discussions going or provide help	Reasonable effort to respond thoughtfully, provide help, and/or keep discussions going	Often responds thoughtfully in a way frequently keeps discussions going and provides help	Continually responds thoughtfully in a way that consistently keeps discussions going and provides help
Content	No useful, on-topic, or interesting information, ideas or analysis	Hardly any useful, on-topic, or interesting information, ideas or analysis	Reasonably useful, on-topic, and interesting information, ideas and/or analysis	Frequently useful, on-topic, and interesting information, ideas and analysis	Exceptionally useful, on-topic, and interesting information, ideas and analysis
Reflection and Synthesis			No significant effort to clarify, summarize or synthesize topics	Contributes to group's effort to clarify, summarize or synthesize	Leads group's effort to clarify, summarize or synthesize topics raised in discussions

			raised in discussions	topics raised in discussions	

Academic Conduct Policy

Please visit Metropolitan College's website for the full text of the department's *Academic Conduct Code*.

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 paragraphs above are from H. Martin and R. Ohmann, *The Logic and Rhetoric of Exposition, Revised Edition.* Copyright 1963, Holt, Rinehart and Winston.

Academic Conduct Code

I. **Philosophy of Discipline**

The objective of Boston University in enforcing academic rules is to promote a community atmosphere in which learning can best take place. Such an atmosphere can be maintained only so long as every student believes that his or her academic competence is being judged fairly and that he or she will not be put at a disadvantage because of someone else's dishonesty. Penalties should be carefully determined so as to be no more and no less than required to maintain the desired atmosphere. In defining violations of this code, the intent is to protect the integrity of the educational process.

II. **Academic Misconduct**

Academic misconduct is conduct by which a student misrepresents his or her academic accomplishments, or impedes other students' opportunities of being judged fairly for their academic work. Knowingly allowing others to represent your work as their own is as serious an offense as submitting another's work as your own.

III. **Violations of this Code**

Violations of this code comprise attempts to be dishonest or deceptive in the performance of academic work in or out of the classroom, alterations of academic records, alterations of official data on paper or electronic resumes, or unauthorized collaboration with another student or students. Violations include, but are not limited to:

A. **Cheating on examination**. Any attempt by a student to alter his or her performance on an examination in violation of that examination's stated or commonly understood ground rules.
B. **Plagiarism.** Representing the work of another as one's own. Plagiarism includes but is not limited to the following: copying the answers of another student on an examination, copying or restating the work or ideas of another person or persons in any oral or written work (printed or electronic) without citing the appropriate source, and collaborating with someone else in an academic endeavor without acknowledging his or her contribution. Plagiarism can consist of acts of commission-appropriating the words or ideas of another-or omission failing to acknowledge/document/credit the source or creator of words or ideas (see below for a detailed definition of plagiarism). It also includes colluding with someone else in an academic endeavor without acknowledging his or her contribution, using audio or video footage that comes from another source (including work done by another student) without permission and acknowledgement of that source.
C. **Misrepresentation or falsification of data** presented for surveys, experiments, reports, etc., which includes but is not limited to: citing authors that do not exist; citing interviews that never took place, or field work that was not completed.
D. **Theft of an examination**. Stealing or otherwise discovering and/or making known to others the contents of an examination that has not yet been administered.
E. **Unauthorized communication during examinations**. Any unauthorized communication may be considered prima facie evidence of cheating.
F. **Knowingly allowing another student to represent your work as his or her own**. This includes providing a copy of your paper or laboratory report to another student without the explicit permission of the instructor(s).
G. **Forgery, alteration, or knowing misuse of graded examinations, quizzes, grade lists, or official records of documents**, including but not limited to transcripts from any institution, letters of

recommendation, degree certificates, examinations, quizzes, or other work after submission.

H. **Theft or destruction of examinations or papers** after submission.

I. **Submitting the same work in more than one course** without the consent of instructors.

J. **Altering or destroying another student's work or records**, altering records of any kind, removing materials from libraries or offices without consent, or in any way interfering with the work of others so as to impede their academic performance.

K. **Violation of the rules governing teamwork**. Unless the instructor of a course otherwise specifically provides instructions to the contrary, the following rules apply to teamwork: 1. No team member shall intentionally restrict or inhibit another team member's access to team meetings, team work-in-progress, or other team activities without the express authorization of the instructor. 2. All team members shall be held responsible for the content of all teamwork submitted for evaluation as if each team member had individually submitted the entire work product of their team as their own work.

L. **Failure to sit in a specifically assigned seat during examinations.**

M. **Conduct in a professional field assignment that violates the policies and regulations of the host school or agency.**

N. **Conduct in violation of public law occurring outside the University that directly affects the academic and professional status of the student, after civil authorities have imposed sanctions.**

O. **Attempting improperly to influence the award of any credit, grade, or honor.**

P. **Intentionally making false statements to the Academic Conduct Committee or intentionally presenting false information to the Committee.**

Q. **Failure to comply with the sanctions imposed under the authority of this code.**

Important Message on Final Exams

Dear Boston University Computer Science Online Student,

As part of our ongoing efforts to maintain the high academic standard of all Boston University programs, including our online MSCIS degree program, the Computer Science Department at Boston University's Metropolitan College requires that each of the online courses includes a proctored final examination.

By requiring proctored finals, we are ensuring the excellence and fairness of our program. The final exam is administered online, and the access will be available at the exam sites.

Specific information regarding final-exam scheduling will be provided approximately two weeks into the course. This early notification is being given so that you will have enough time to plan for where you will take the final exam.

I know that you recognize the value of your Boston University degree and that you will support the efforts of the University to maintain the highest standards in our online degree program.

Thank you very much for your support with this important issue.

Regards,

Professor Lou Chitkushev, Ph.D.

Associate Dean for Academic Affairs

Boston University Metropolitan College

Who's Who: Roles and Responsibilities

You will meet many BU people in this course and program. Some of these people you will meet online, and some you will communicate with by email and telephone. There are many people behind the scenes, too, including instructional designers, faculty who assist with course preparation, and video and animation specialists.

People in Your Online Course in Addition to Your Fellow Students

Your Facilitator. Our classes are divided into small groups, and each group has its own facilitator. We carefully select and train our facilitators for their expertise in the subject matter and their excellence in teaching. Your facilitator is responsible for stimulating discussions in pedagogically useful areas, for answering your questions, and for grading homework assignments, discussions, term projects, and any manually graded quiz or final-exam questions. If you ask your facilitator a question by email, you should get a response within 24 hours, and usually faster. If you need a question answered urgently, post your question to one of the urgent help topics, where everyone can see it and answer it.

Your Professor. The professor for your course has primary responsibility for the course. If you have any questions that your facilitator doesn't answer quickly and to your satisfaction, then send your professor an email in the course, with a cc to your facilitator so that your facilitator is aware of your question and your professor's response.

Your Senior Faculty and Student Support Administrator, Jennifer Sullivan. Jen is here to ensure you have a positive online experience. You will receive emails and announcements from Jen throughout the semester. Jen represents Boston University's university services and works for the Office of Distance Education. She prepares students for milestones such as course launch, final exams, and course evaluations. She is a resource to both students and faculty. For example, Jen can direct your university questions and concerns to the appropriate party. She also handles general questions regarding Online Campus functionality for students, faculty, and facilitators, but she does not provide tech support. She is enrolled in all classes and can be contacted within the course through Online Campus email as it is running. You can also contact her by external email at jensul@bu.edu or call toll free at 1-888-524-2200.

People Not in Your Online Course

Although you will not normally encounter the following people in your online course, they are central to the program. You may receive emails or phone calls from them, and you should feel free to contact them.

Your Computer Science Department Online Program Coordinator, Peter Mirza. Peter administers the academic aspects of the program, including admissions and registration. You can ask him questions about the program, registration, course offerings, graduation, or any other program-related topic. He can be reached at metcsol@bu.edu or (617) 353-2566.

Your Computer Science Department Program Manager, Kim Richards. Kim is responsible for administering most aspects of the Computer Science Department. You can reach Kim at kimrich@bu.edu or (617) 353-2566.

Andrew Gorlin, Academic Advisor. Reviews requests for transfer credits and waivers. Advises students on which courses to take to meet their career goals .You can reach Andrew at asgorlin@bu.edu, or (617)-353-2566.

Professor Anatoly Temkin, Computer Science Department Chairman. You can reach Professor Temkin at temkin@bu.edu or at 617-353-2566.

Professor Lou T. Chitkushev, Associate Dean for Academic Affairs, Metropolitan College. Dr. Chitkushev is responsible for the academic programs of Metropolitan College. Contact Professor Chitkushev with any issues that you feel have not been addressed adequately. The customary issue-escalation sequence after your course facilitator and course faculty is Professor Temkin, and then Professor Chitkushev.

Professor Tanya Zlateva, Metropolitan College Dean Dr. Zlateva is responsible for the quality of all the academic programs at Boston University Metropolitan College.

Disability Services

In accordance with University policy, every effort will be made to accommodate unique and special needs of students with respect to speech, hearing, vision, or other disabilities. Any student who feels he or she may need an accommodation for a documented disability should contact the Office of Disability Services at (617) 353-3658 or at access@bu.edu for review and approval of accommodation requests.

Netiquette

The Office of Distance Education has produced a netiquette guide to help you understand the potential impact of your communication style.

Before posting to any discussion forum, sending email, or participating in any course or public area, please consider the following:

Ask Yourself…

- How would I say this in a face-to-face classroom or if writing for a newspaper, public blog, or wiki?
- How would I feel if I were the reader?
- How might my comment impact others?
- Am I being respectful?
- Is this the appropriate area or forum to post what I have to say?

Writing

When you are writing, please follow these rules:

- **Stay polite and positive in your communications**. You can and should disagree and participate in discussions with vigor; however, when able, be constructive with your comments.
- **Proofread your comments before you post them.** Remember that your comments are permanent.
- **Pay attention to your tone.** Without the benefit of facial expressions and body language your intended tone or the meaning of the message can be misconstrued.
- **Be thoughtful and remember that classmates' experience levels may vary.** You may want to include background information that is not obvious to all readers.
- **Stay on message.** When adding to existing messages, try to maintain the theme of the comments previously posted. If you want to change the topic, simply start another thread rather than disrupt the current conversation.
- **When appropriate, cite sources.** When referencing the work or opinions of others, make sure to use correct citations.

Reading

When you are reading your peers' communication, consider the following:

- **Respect people's privacy.** Don't assume that information shared with you is public; your peers may not want personal information shared. Please check with them before sharing their information.
- **Be forgiving of other students' and instructors' mistakes.** There are many reasons for typos and misinterpretations. Be gracious and forgive other's mistakes or privately point them out politely.
- **If a comment upsets or offends you, reread it and/or take some time before responding.**

Important Note

Don't hesitate to let your instructor or your faculty and student support administrator know if you feel others are inappropriately commenting in any forum.

All Boston University students are required to follow academic and behavioral conduct codes. Failure to comply with these conduct codes may result in disciplinary action.

Registration Information and Important Dates

View the drop dates for your course.

Withdraw or drop your course.

- If you are dropping down to zero credits for a semester, please contact your college or academic department.
- **Nonparticipation in your online course does not constitute a withdrawal from the class.**
- If you are unable to drop yourself on student link please contact your college or academic department.

Technical Support

Experiencing issues with BU websites or Blackboard?

It may be a system-wide problem. Check the BU Information Services & Technology (IS&T) news page for announcements.

Boston University technical support is available via email (ithelp@bu.edu), the support form, and phone (888-243-4596). Please note that the IT Help Center has multiple locations. All locations can be reached through the previously mentioned methods. For IT Help Center hours of operation please visit their contact page. For other times, you may still submit a support request via email, phone, or the support form, but your question won't receive a response until the following day. If you aren't calling, it is highly recommended that you submit your support request via the technical-support form as this provides the IS&T Help Center with the best information in order to resolve your issue as quickly as possible.

Examples of issues you might want to request support for include the following:

- Problems viewing or listening to sound or video files
- Problems accessing internal messages
- Problems viewing or posting comments
- Problems attaching or uploading files for assignments or discussions
- Problems accessing or submitting an assessment

To ensure the fastest possible response, please fill out the online form using the link below:

IT Help Center Support
888-243-4596 or 617-353-4357 or Web
Check your open tickets using BU's ticketing system.

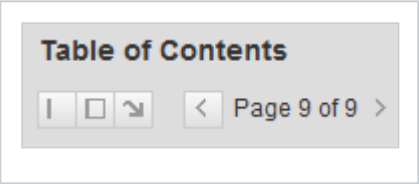
Navigating Courses

For best results when navigating courses, it is recommended that you use the Mozilla Firefox browser.

The Table of Contents may contain folders. These folders open and close (+ and − signs) and may conceal some pages. To avoid missing content pages, you are advised to use the next- and previous-page buttons (and icons) in the top-right corner of the learning content.

Please also familiarize yourself with the navigation tools, as shown below; these allow you to show and hide both the Course Menu and the Table of Contents on the left. This will be helpful for freeing up screen space when moving through the weekly lecture materials.

Navigation tools for the Table of Contents are shown in the image below:



Clicking on the space between the Course Menu and the Table of Contents allows you to show or hide the Course Menu on the left:

Web Resources/Browser Plug-Ins

To view certain media elements in this course, you will need to have several browser plug-in applications installed on your computer. See the Course Resources page in the syllabus of each individual course for other specific software requirements.

- Check your computer's compatibility by reviewing Blackboard's System Requirements
- Check your browser settings with Blackboard's Connection Test
- Download most recent version of Adobe Flash Player
- Download most recent version of Adobe Acrobat Reader

How to Clear Your Browser Cache

The IT Help Center recommends that you periodically clear your browser cache to ensure that you are viewing the most current content, particularly after course or system updates.

This page is also found within the "How to…" section of the online documentation, which contains a list of some of the most common tasks in Blackboard Learn.

Boston University Metropolitan College