Syllabus

The following are all pages from this module linked as a single 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 CS674

Database Security

Prerequisite: MET CS 669 or proof of knowledge

The course provides a strong foundation in database security and auditing. This course utilizes Oracle scenarios and step-by-step examples. The following topics are covered: security, profiles, password policies, privileges and roles, Virtual Private Databases, and auditing. The course also covers a list of advanced topics, such as SQL injection. Database management security issues such as securing the DBMS, enforcing access controls, and related issues are also covered.

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 Objectives

At the completion of the course, you will fully understand how to implement database security on modern business databases by using practical scenarios and step-by-step examples. Hands-on projects using Oracle Database Management System are used to reinforce and showcase the topics presented.

By successfully completing this course, you will be able to:

- Describe the fundamentals of security, and how it relates to information systems.
- Identify assets in your organization and their values.
- Identify risks and vulnerabilities in operating systems from a database perspective.
- Explain good password policies and techniques to secure passwords in your organization.
- Implement administration policies for users.
- Use Oracle to create policies, profiles and roles.
- Compare the various database security models and their advantages or disadvantages.
- Implement a Virtual Private Database using views, roles, and application context.
- Summarize an overview of auditing fundamentals and create your own auditing model.
- Describe the purpose and use of data dictionaries, encryption, and SQL injection.
- Explore an interesting topic of your choice related to database security or related topic.

Course Outline

Module 1 – Information Security Fundamentals and the Types of Attacks

- Lecture 1 – Information Security Fundamentals
- Lecture 2 – Attackers and their Attacks
- Lecture 3 – Information Security Framework

Module 2 – Operating Systems and User Administration

- Lecture 4 – Operating Systems
- Lecture 5 – User Administration

Module 3 – Profiles, Passwords, Privileges and Roles

Due to a heavy workload in this third week, it is recommended that you get started on the assignments as early as possible (particularly the Research Paper Proposal).

- Lecture 6 – Authorization

- Lecture 7 – Database Applications Security

Module 4 - Virtual Private Database

- Lecture 8 – Virtual Private Database
- Lecture 9 – How the Virtual Private Database Works

Module 5 - Auditing

- Lecture 10 – Auditing

Module 6 - Advanced Topics (Data Dictionary, Encryption with Oracle, and SQL Injection)

- Lecture 11 – Data Dictionary
- Lecture 12 – Encryption with Oracle
- Lecture 13 – SQL Injection

Module 7 - Final Exam

- **Proctored Final Exam** – There will be a proctored final exam for this course.

Instructor: Shengzhi Zhang, Ph.D.

Assistant Professor
Computer Science Department
Metropolitan College
Boston University
Email: shengzhi@bu.edu

Dr. Shengzhi Zhang earned his PhD in Computer Science and Engineering from Penn State University in 2012. His research focuses on cybersecurity, including but not limited to Internet of Things (IoT) security, automobile security, mobile security, and operating system security, among others. He has most recently worked as an assistant professor in the Department of Computer Science at the Florida Institute of Technology. Prior to academia, Dr. Zhang conducted various research projects in Cisco, IBM, and Honeywell Aerospace labs. His existing partnerships, both nationally and internationally, include researchers from Ford Motor, IBM, GE, Indiana

University, Penn State, Kuwait University, and the Chinese Academy of Sciences. Dr. Zhang has published many papers and served as program committee members in top-tier security conferences and journals.

Course Resources

Required Book

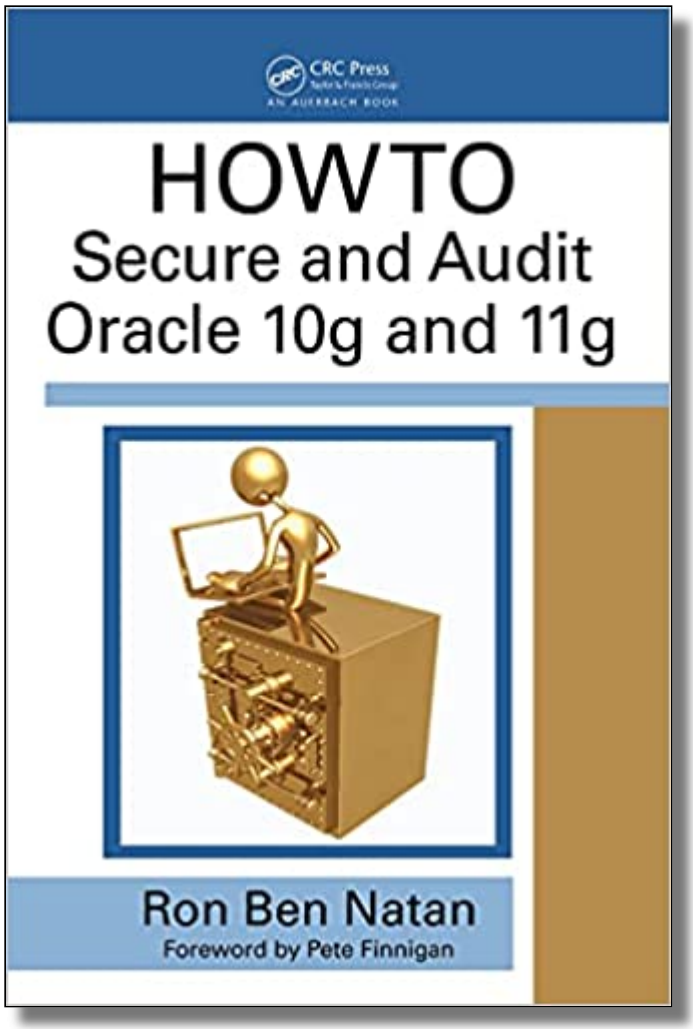
There is NO required textbook for this course.

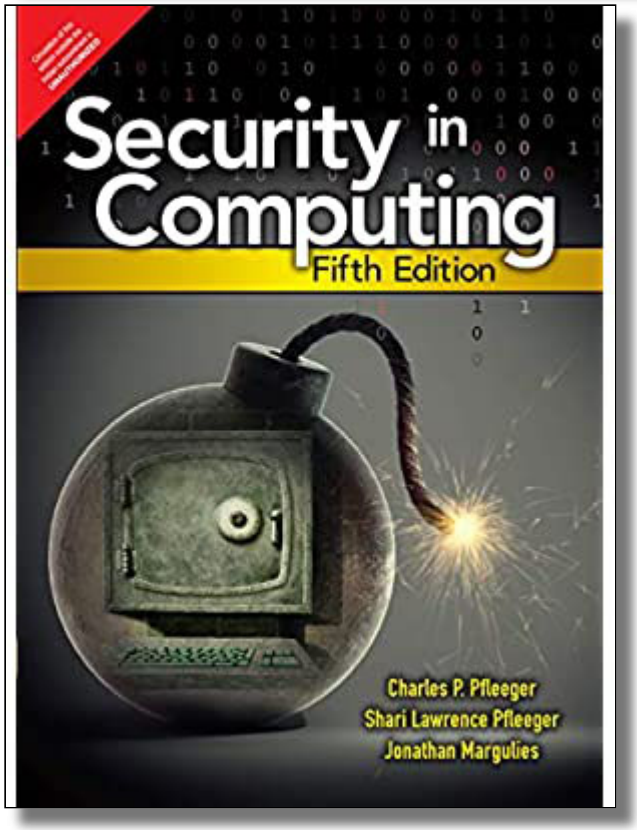
Recommended Book

Ben-Natan, R. (2009). ***HOWTO Secure and Audit Oracle 10g and 11g*****.**
Publisher: Auerbach Publications

ISBN-13: 978-1420084122
ISBN-10: 1420084127

This book can be purchased from Barnes & Noble at Boston University.





Pfleeger, C. P. & Pfleeger, S. L. (2018). *Security in Computing*.

Publisher: Pearson India

ISBN-13: 978-9352866533

ISBN-10: 9789352866533

This book can be purchased from Barnes & Noble at Boston University.

Tutorials and Handouts

Lab Assignment Instructions

Advanced SQL Injection In SQL Server Applications (available in Module 6, as well)

SQL Injection: Are your Web Applications Vulnerable? (available in Module 6, as well)

Oracle Error Codes Resource

Included for your convenience is a link of searching for standard Oracle database error messages, provided by Oracle.

There are more than 40,000 of these error codes, each with a code, cause, and what to do about it. For example:

ORA-12537: TNS:connection closed

Cause: "End of file" condition has been reached; partner has disconnected.

Action: None needed; this is an information message.

ORA-12538: TNS:no such protocol adapter

Cause: The protocol adapter requested (by way of the "(PROTOCOL=..)" keyword-value pair in a TNS address) is unknown. If the supplied address is typographically correct then the protocol adapter is not installed.

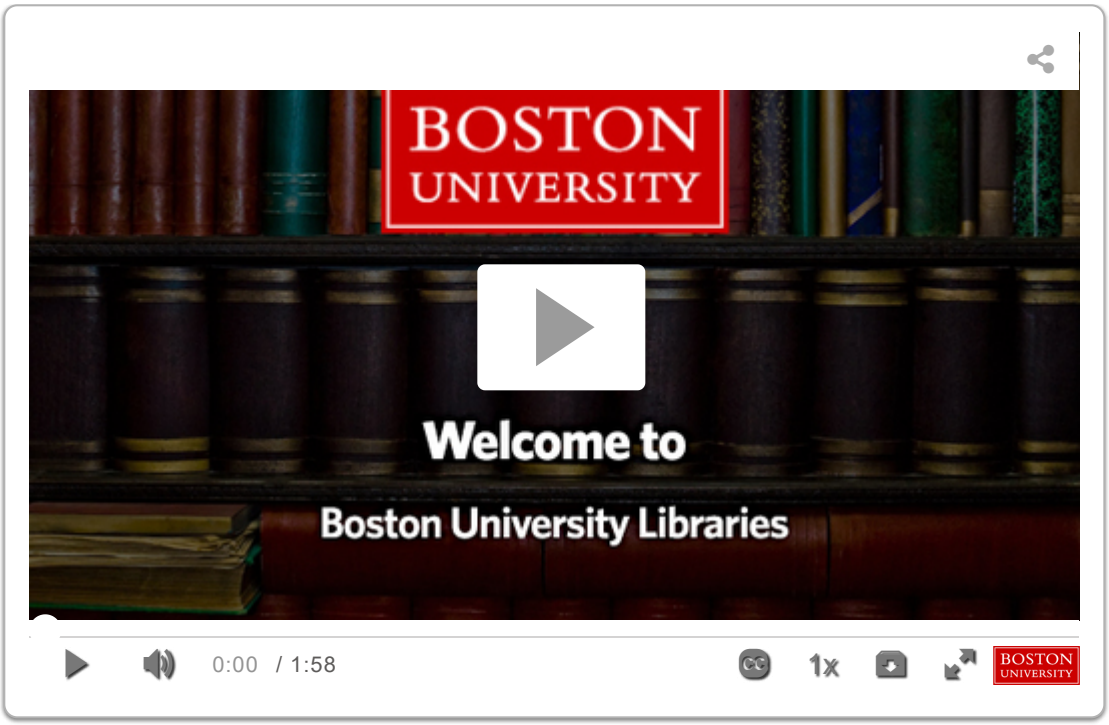
Action: Install the protocol adapter or correct typographical error, as appropriate. Note: if the supplied address was derived from resolving the service name, check the address in the appropriate file (TNSNAMES.ORA, LISTENER.ORA or SQLNET.ORA).

Glossary

For your convenience, there is a link to the glossary on each page. It is accessible by clicking the Glossary icon (G).

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:



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 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

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.

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:
- Online lectures 1–3
- Module 1 live classroom slides and recording (will be shared after the live classroom session)

Discussions: Discussion 1 postings end Tuesday, September 13 at 6:00 AM ET

Assignments: Assignment 1 due Tuesday, September 13 at 6:00 AM ET

Assessments: Quiz 1 due Tuesday, September 13 at 6:00 AM ET

Live Classroom:
- Module 1 – lecture: Wednesday, September 7 from 7:00 – 8:30 PM ET
- Module 1 – office hour: Saturday, September 10 from 8:00 – 9:00 PM ET

Module 2 Study Guide and Deliverables

Readings:
- Online lectures 4 and 5
- Module 2 live classroom slides and recording (will be shared after the live classroom session)

Discussions: Discussion 2 postings end Tuesday, September 20 at 6:00 AM ET

Assignments: Assignment 2 due Tuesday, September 20 at 6:00 AM ET

Assessments: Quiz 2 due Tuesday, September 20 at 6:00 AM ET

Live Classroom:
- Module 2 – lecture: Wednesday, September 14 from 7:00 – 8:30 PM ET
- Module 2 – office hour: Saturday, September 17 from 8:00 – 9:00 PM ETT

Module 3 Study Guide and Deliverables

Readings:
- Online lectures 6 and 7
- Module 3 live classroom slides and recording (will be shared after the live classroom session)

Discussions: *Open* Discussion

Assignments: Assignment 3 due Tuesday, September 27 at 6:00 AM ET

Assessments: Quiz 3 due Tuesday, September 27 at 6:00 AM ET

Live Classroom:
- Module 3 – lecture: Wednesday, September 21 from 7:00 – 8:30 PM ET
- Module 3 – office hour: Saturday, September 24 from 8:00 – 9:00 PM ET

Module 4 Study Guide and Deliverables

Readings:
- Online lectures 8 and 9

- Module 4 live classroom slides and recording (will be shared after the live classroom session)

Discussions: Discussion 4 postings end Tuesday, October 4 at 6:00 AM ET

Assignments: Assignment 4 due Tuesday, October 4 by 6:00 AM ET

Assessments: Quiz 4 due Tuesday, October 4 at 6:00 AM ET

Live Classroom:
- Module 4 – lecture: Wednesday, September 28 from 7:00 – 8:30 PM ET
- Module 4 – office hour: Saturday, October 1 from 8:00 – 9:00 PM ET

Module 5 Study Guide and Deliverables

Readings:
- Online lecture 10
- Module 5 live classroom slides and recording (will be shared after the live classroom session)

Discussions: Discussion 5 postings end Tuesday, October 11 at 6:00 AM ET

Assignments: Assignment 5 due Tuesday, October 11 by 6:00 AM ET

Assessments: Quiz 5 due Tuesday, October 11 at 6:00 AM ET

Live Classroom:
- Module 5 – lecture: Wednesday, October 5 from 7:00 – 8:30 PM ET
- Module 5 – office hour: Saturday, October 8 from 8:00 – 9:00 PM ET

Module 6 Study Guide and Deliverables

Readings:
- Online lectures 11–13
- Read the two PDF handouts on SQL Injections: *Advanced SQL Injection* *and* *SQL Injection: Are your Web Applications Vulnerable?*

Discussions: Discussion 6 postings end Tuesday, October 18 at 6:00 AM ET

Assignments:
- Research Paper due Tuesday, October 18 at 6:00 AM ET
- Assignment 6 due Tuesday, October 18 by 6:00 AM ET

Assessments: Quiz 6 due Tuesday, October 18 at 6:00 AM ET

Course Evaluation:
- Course Evaluation opens on Tuesday, October 11, at 10:00 AM ET and closes on Tuesday, October 18 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:	• Module 6 – lecture: Wednesday, October 12 from 7:00 – 8:30 PM ET • Course Wrap-up and Final Exam Review: Saturday, October 15 from 8:00 – 9:00 PM ET

Final Exam Details

The Final Exam is a proctored exam available from **Wednesday, October 19 at 6:00 AM ET to Saturday, October 22 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. In order to take the exam, you are required to have a working webcam and computer that meets Examity's system requirements. A detailed list of those requirements can be found on the How to Schedule page ("Proctored Final Exam Information" module at the course home page). Additional information 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 is open book and accessible only 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.

Final Exam Duration: three hours.

Student Research Presentations

The presentations linked below are samples from the classroom version of MET CS 674 and are meant to give you an idea of the scope of research topics. These are not all necessarily exceptional presentations (i.e., some are "B" grade). Also they were graded on a different rubric. Regardless, the presentations have a consistent theme – a research topic component and a "lab" component. Please note that on the bottom of most slides, narrative is documented. You have to view/print the slides in NOTES MASTER mode. In the online version of MET CS 674 you will be writing a research paper vs. creating a presentation.

- SQL Injection Attacks with SQL 2000
- AppDetective
- XMLWebSecurity (including Oracle)

- WebServices and DB Security
- Data Storage Security
- Web Application Security
- Disaster Recovery
- Access Control
- Rootkits
- Secure and Monitor Mobile Databases
- SQL Server Authentication Modes

Lab Assignment Instructions

Some assignments include hands-on lab exercises. Doing such labs helps to increase your understanding of the lecture material. Typically, we illustrate such concepts in a lab setting at Boston University. We are trying to replicate that approach in this course.

In your lab documents, you should include:

- Explanations of the work performed in the lab
- All SQL input and output used in the labs. You can use the SPOOL Command to save your Oracle code to a text file. This text file can then be pasted into the Word document
- Screen captures
- Websites - that you either used in completing the lab work or used as a resource
- Any other item that shows completion of the lab work
- Your submitted lab document should also include the following formatting at a minimum:
    - Your name
    - Lab title
    - Date
    - Table of contents
    - Clearly marked answers for each step in the labs
    - Page numbers in your document

An Example of Lab Submission

These submissions consist of a sentence or two describing the SQL query and a SPOOLed version of the code. For example:

I have created a new user called yourName, I used the following syntax:

```
SQL> CREATE USER yourName IDENTIFIED BY tiger01
     etc…
```

```
8 /
User created
```

Course Grading Structure

The course will be conducted by means of a sequence of lectures in text and graphic form. Each week will cover one or more core database security concepts and will have at least one lab component, along with a short quiz based on the topics covered that week. There is one major assignment: the Research Paper. Students will be able to demonstrate their understanding of the fundamentals of database security through these assignments. In the final module of the course there is a comprehensive final exam, and it is proctored.

Grading Policy

All students will be expected to demonstrate database security knowledge and techniques. To obtain an exceptional grade, you have to exceed expectations in your projects, quizzes, and assignments.

Grading Structure and Distribution

The grade for the course is determined by the following:

Overall Grading Percentages	
Quizzes	15
Labs/Assignment	20
Discussions/Participation	10
Research Paper	25
Final Examination	30

The following grades will be assigned for your assignments.

A	4.0

A-	3.7
B+	3.3
B	3.0
B-	2.7
C+	2.3
C	2.0
Fail	0

Grades will be curved to maintain academic standards at Boston University.

Assignments, Exams and Discussions

Participation

Graded Discussions – all discussions will be graded on a 100-point scale: Discussion Rubric

Assignments

Some assignments include hands-on labs. Instructions for submitting your lab work are available by clicking the following link: Lab Assignment Instructions.

Quizzes

There will be six 1-hour quizzes comprised of a combination of multiple-choice and true/false questions.

Research Paper

You are asked to research and provide a summary report on the latest security features of one of the database management systems, or a Database Security topic, as specified in the Research Paper Details.

Final Exam

There will be a proctored Final Exam in this course. The type and nature of questions in the final exam will be very similar to your quiz questions.

Expectations

Many learning activities require sharing your assignments and opinions with you classmates. For example, you may be given a set of criteria on the basis of which to evaluate other classmates' assignments, and asked to submit the results to your facilitator by a specified day of the week. It is, therefore, very important that you, as well as your classmates, submit your assignments on a timely basis. Timely submission by all will result in each of you being able to evaluate each other's assignments.

Delays

If, for any reason, you are unable to meet any assignment deadline, contact your Course Facilitator. All assignments must be completed. Extensions may be granted under mitigating circumstances.

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	Little effort to keep discussions	Reasonable effort to respond	Often responds thoughtfully in a way that	Continually responds thoughtfully in a

	to discussion	going or provide help	thoughtfully, provide help, and/or keep discussions going	frequently keeps discussions going and provides help	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 raised in discussions			Contributes to group's effort to clarify, summarize or synthesize topics raised in discussions	Leads group's effort to clarify, summarize or synthesize 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.

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

Boston University Metropolitan College