Toronto Metropolitan University

The Chang School of Continuing Education

TED ROGERS SCHOOL Information Technology Management

(C)ITM 820 – Information Systems Security and Privacy

COURSE OUTLINE FOR 2023-2024

Prerequisite(s): (C)ITM 301
Antirequisite(s): (C)CPS 633

Instructor Information

- **Instructor Name:** Dr. Farid Shirazi
- **Office Location:** TRS3-094
- **Office Hours:**
- **Phone:** (416) 979 – 5000, 557938.
- **Course Website:** my.torontomu.ca (for courses using D2L)
- **Email Address:** f2shiraz@torontomu.ca

Email Policy

Students are expected to monitor and retrieve messages and information sent through D2L and TMU email on a frequent and consistent basis. In accordance with the Policy on TMU Student E-mail Accounts (Policy 157), Toronto Metropolitan University (TMU) requires that any electronic communication by students to TMU faculty or staff be sent from their official university email account. Communications sent from other accounts may be disregarded.

Course Description

This course considers the technical, operational, and managerial issues of computer and network security in an operational environment. Industry best-practices relating to computer security including schemes for breaking security, and techniques for detecting and preventing security violations are the core focus of this course. This course will also explore the principles of data privacy, threats to privacy, international and national policy, particularly related to privacy-enhancing technologies as they apply to the management of information systems and e-Business.

Course Details

Teaching Methods

If you are registered in an in-person or a virtual classroom, instruction will take place at scheduled hours, following the approach outlined in D2L Brightspace. If you are

registered in a Chang School Distance Education course, please follow the schedule, course outline and learning modules as outlined in D2L Brightspace.

Course Materials

Title: Computer Security: Principles and Practice, 5th Edition
Author: William Stallings and Lawrie Brown
Publisher: Pearson
ISBN-13: 978-013-8091712

Suggested/Recommended Textbook
Title: Cloud Computing, Automating the Virtualized Data Center
Authors: Venkata Josyula, Malcom Orr & Greg Page
Publisher: Cisco Press
ISBN: 978- 1285448367

Title: Principles of Information Security (7th Edition)
Authors: Michael E. Whitman, Herbert J. Mattord
Publisher: Course Technology
ISBN: 9780357710777

Course Objectives and Learning Outcomes

This course provides students with a detailed review of the industry-accepted methods for securing computer applications and computer networks. The course will provide an awareness of the risks and threats to computer operations and communications and an overview of the different types of security techniques. The course will address issues and challenges associated with implementing the appropriate level of security to meet the needs of the organization.

Upon completion of the course, students should be able to:

1. Explain the fundamental principles of Information Technology Security and Privacy, and Data Protection.
2. Explain the concepts of threat, evaluation of assets, information assets, physical, operational, and information security, and how they are related.
3. Describe the need for the careful design of a secure organizational information infrastructure
4. Describe risk analysis and risk management in the context of business.
5. Describe both technical and administrative mitigation approaches.
6. Explain the need for a comprehensive security model and its implications for the security manager.
7. Demonstrate knowledge of security technologies.
8. Demonstrate knowledge of basic cryptography, its implementation considerations, and key management.
9. Demonstrate knowledge of designing and guiding the development of an organization's security policy.
10. Demonstrate knowledge of determining appropriate strategies to assure confidentiality, integrity, and availability of information.

11. Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.
12. Describe privacy issues associated with storing and distributing digital data.
13. Explain Privacy-by-Design (PbD) framework.

Plagiarism Detection

Turnitin

Turnitin.com is a plagiarism prevention and detection service to which TMU subscribes. It is a tool to assist instructors in determining the similarity between students' work and the work of other students who have submitted papers to the site (at any university), internet sources, and a wide range of books, journals and other publications. While it does not contain all possible sources, it gives instructors some assurance that students' work is their own. No decisions are made by the service; it generates an "originality report," which instructors must evaluate to judge if something is plagiarized.

Students agree by taking this course that their written work will be subject to submission for textual similarity review to Turnitin.com. Instructors can opt to have student's papers included in the Turnitin.com database or not. Use of the Turnitin.com service is subject to the terms-of-use agreement posted on the Turnitin.com website. Students who do not want their work submitted to this plagiarism detection service must, by the end of the second week of class, consult with their instructor to make alternate arrangements.

Even when an instructor has not indicated that a plagiarism detection service will be used, or when a student has opted out of the plagiarism detection service, if the instructor has reason to suspect that an individual piece of work has been plagiarized, the instructor is permitted to submit that work in a non-identifying way to any plagiarism detection service.

Evaluation, Assessment and Feedback

Teaching Methods:

- Regular lectures, prescribed weekly readings, problem based assignments, and topic and case study discussions are the main teaching activities that occur in this course.

- Since a major component of this course is problem-based learning, the five individual assignments provide practice and progressive skill-building that ensure that each student can master the course content.

- Teamwork activities allow the students to apply the analytical techniques that were introduced in class and practiced in the problem sets. In addition, by working in small teams the students develop interaction and individual and group presentation skills.

- The instructor will establish an active learning environment by engaging the students in a Socratic exchange of relevant questions and ideas. Students should expect a frequent and substantive interaction between the instructor and students and among students in every class.

Those students that actively participate in the learning process will gradually assume ownership of the knowledge contained in the course materials. In addition to ownership of the course content, the students will master a set of skills that they can use to develop communications networks.

The grade for this course is composed of the mark received for each of the following components:

Evaluation Component	Percentage of Final Grade
Four Assignments (5% each)	20%
Group Project	10%
Midterm Examination	30%
Final Examination	40%
Final Grade	100%
Note: Students must achieve a course grade of at least 50% to pass this course. At least 20% of student's grade based on individual work will be returned to students prior to the last date to drop a course in good academic standing.	

Topics and Course Schedule

Week	Topics & Learning Outcomes	Readings	Activities & Due Dates
1	Security Concepts: Introduction, Framework ● Explain what assets we need to protect. ● Explain how those assets are threatened. ● Explain the best options to counter those threats. ● Explain the concept of security assurance and evaluation	Ch. 1 Lecture Notes	

Week	Topics & Learning Outcomes	Readings	Activities & Due Dates
2	Cryptographic Tools: Symmetric Encryption, Public Key Encryption, Hash Functions, Digital Signatures ● Describe various types of algorithms and their application. ● Explain the basics of encryption ● Describe modern cryptography methods ● Describe message authentication methods	Ch. 2 Lecture Notes	
3	User Authentication: Password, Token and Biometric Authentication; Access Control: Access Control and Access Management ● Describe the four general means of authenticating a user's identity ● Explain passwords authentication methods ● Describe token-based user authentication ● Explain - access controls & user authentication ● Distinguish among subjects, objects, and access rights	Ch. 3 & 4	Assignment 1
4	Database and security attacks: Database Access Control, SQL Injection Attacks; Data protection in Cloud ● Discuss the unique need for database security ● Describe SQL injection attacks ● Compare different approaches of database security ● Discuss key concepts of cloud security	Ch. 5 Lecture Notes	
5	Malicious Software: Viruses, Worms, SPAM, Trojans, Bots, Phishing, Spyware, Rootkits ● Describe three broad malware uses to propagate ● Discuss the basic operations of viruses, worms, Trojan horses, and logic bombs ● Discuss the different threats posed by bots, spams, spyware, and rootkits ● Discuss the backdoor vulnerabilities of systems	Ch. 6 Lecture Notes	Assignment 2
6	Security Attacks: Denial of Service Attacks, Man-in-the-middle Attack, Spoofing, Sniffing	Ch. 7 Lecture	Intro. to Group Project

Week	Topics & Learning Outcomes	Readings	Activities & Due Dates
	• Explain the basic concepts of DoS & DDoS attacks • Describe flooding attacks • Explain man-in-the-middle attacks • Explain spoofing and sniffing, and their negative impacts on business	Notes	
7	**Midterm Examination** Firewall, Intrusion Detection and Prevention Systems • Explain snort architecture • Explain the purpose of honeypots • Describe different types of honeypots and sandboxes • Explain the role of firewalls, proxies, and NAT in a network	Ch. 8 & 9 Lecture Notes	
8	Operating System Security: System Security, Linux/UNIX and Windows Security ; Privacy Enhancing Technologies • Explain the features of Windows and Linux\Unix security • Discuss virtualization and hypervisor management • Explain security vs. privacy • Describe Privacy by Design (PbD) framework • Explain the concept of privacy acts such as EU directives, PIPEDA, and ISO standards	Ch. 12 & 19 Lecture Notes	Assignment 3
9	Cloud and IoT Security IT Security Management and Risk Assessment; • Explain Cloud deployments & Security • Explain data protection in Cloud • Explain the role of IoT in business • Explain IoT Security Framework • Explain organizational security policy • Explain Risk assessment • Analyze and evaluate risks	Ch. 13 & 14 Lecture Notes	
10	Wireless Network Security; • Explain components of 802.11 standards and WLAN	Ch. 24 Lecture Notes	Assignment 4

Week	Topics & Learning Outcomes	Readings	Activities & Due Dates
	• Explain WEP and WPA authentication methods • Describe advanced features of 802.11i technology		
11	Security Controls, Plans and Procedure Security Auditing, Legal and Ethical Aspects • Explain ISO IT security standards • Discuss organizational IT security policy • Discuss IT security plans • Identify security threats and security risk assessments • Describe the process of security compliance, audits, and trails	Ch.15 & 18	
12	Symmetric Encryption and Message Confidentiality Physical and Infrastructure Security: Prevention, Mitigation, Recovery • Describe the general model for the symmetric encryption process. • Describe block encryption algorithms: DES, 3DES, and AES. • Describe stream cipher RC4. • Examine the application of symmetric algorithms to achieve confidentiality. • Discuss measures for physical disaster and recovery plans • Discuss physical and logical security integration • Describe benefits of security awareness, training, and education	Ch. 16 & 20 Lecture Notes	Group Project

University Policies

You are reminded that you are required to adhere to all relevant university policies found in their online course shell in D2L and/or on the Senate website. Please refer to the Course Outline Appendix for more detail.

Important Resources Available at Toronto Metropolitan University

- The Library provides research workshops and individual assistance. If the University is open, there is a Research Help desk on the second floor of the library, or students can use the Library's virtual research help service to speak with a librarian.

- The Academic Integrity Office provides education and support for the administration of Policy 60: Academic Integrity.

- Student Life and Learning Support offers group-based and individual help with writing, math, study skills, and transition support, as well as resources and checklists to support students as online learners.

- You can submit an Academic Consideration Request when an extenuating circumstance has occurred that has significantly impacted your ability to fulfill an academic requirement. You may always visit the Senate website and select the blue radio button on the top right hand side entitled: Academic Consideration Request (ACR) to submit this request.

  For Extenuating Circumstances, Policy 167: Academic Consideration allows for a once per semester ACR request without supporting documentation if the absence is less than 3 days in duration and is not for a final exam/final assessment. Absences more than 3 days in duration and those that involve a final exam/final assessment, require documentation. Students must notify their instructor once a request for academic consideration is submitted. See Senate Policy 167: Academic Consideration.

- If taking a remote course, familiarize yourself with the tools you will need to use for remote learning. The Remote Learning Guide for students includes guides to completing quizzes or exams in D2L Brightspace, with or without Respondus LockDown Browser and Monitor, using D2L Brightspace, joining online meetings or lectures, and collaborating with the Google Suite.

- Information on Copyright for Faculty and students.

Accessibility

- We are committed to making this course accessible to students with disabilities. Students should contact the instructor if they discover an accessibility barrier with any course materials or technologies.

- As outlined in Policy 159: Academic Accommodation of Students with Disabilities, students are required to proactively consult with AAS, the faculty/instructor, Department or Faculty, as soon as feasible, including prior to enrolling in a course or program, on any concerns they may have about their ability to meet the essential academic requirements of a course/program.

Academic Accommodation Support

Academic Accommodation Support (AAS) is the university's disability services office. AAS works directly with incoming and returning students looking for help with their academic accommodations. AAS works with any student who requires academic accommodation regardless of program or course load.

- Learn more about Academic Accommodation Support.

- Learn how to register with AAS.

Academic Accommodations (for students with disabilities) and Academic Consideration (for students faced with extenuating circumstances that can include short-term health issues) are governed by two different university policies. Learn more about Academic Accommodations versus Academic Consideration and how to access each.

Wellbeing Support

At Toronto Metropolitan University, we recognize that things can come up throughout the term that may interfere with a student's ability to succeed in their coursework. These circumstances are outside of one's control and can have a serious impact on physical and mental well-being. Seeking help can be a challenge, especially in those times of crisis.

If you are experiencing a mental health crisis, please call 911 and go to the nearest hospital emergency room. You can also access these outside resources at anytime:

- **Distress Line:** 24/7 line for if you are in crisis, feeling suicidal or in need of emotional support (phone: 416–408–4357)
- **Good2Talk:** 24/7-hour line for postsecondary students (phone: 1-866-925-5454)
- **Keep.meSAFE:** 24/7 access to confidential support through counsellors via My SSP app or 1-844-451-9700

If non-crisis support is needed, you can access these campus resources:

- **Centre for Student Development and Counselling:** 416-979-5195 or email csdc@torontomu.ca
- **Consent Comes First – Office of Sexual Violence Support and Education:** 416-919-5000 ext 3596 or email osvse@torontomu.ca
- **Medical Centre:** call (416) 979-5070 to book an appointment

We encourage all Toronto Metropolitan University community members to access available resources to ensure support is reachable. You can find more resources available through the Toronto Metropolitan University Mental Health and Wellbeing website.