

(C)ITM 820 – Information Systems Security and Privacy

COURSE OUTLINE FOR 2026-2027

Semester, Section
Classroom, Class Time

Prerequisite(s): ITM 301

Antirequisites: CPS 633

Faculty/Contract Lecturer Information

- **Faculty/Contract Lecturer Name:**
- **Office Location:**
- **Office Hours:**
- **Phone:** (416) 979 – 5000, ext.
- **Course Website:** my.torontomu.ca (for courses using D2L)
- **Email Address:** youremail@torontomu.ca

Mode of Course Delivery: In person

[Academic Program Advising Contacts](#)

Chair/Director for this Course: Sameh Al Natour

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.

Note: All assessments in this course, regardless of its delivery format, will be held in-person on campus. This applies to in-person, virtual, and online courses, including sections/courses delivered through the Chang School.

Course Materials

Textbook and Other Learning Materials:

Lecture:

Title: Computer Security: Principles and Practice, 5th Edition

Author(s): William Stallings and Lawrie Brown

Publisher: Pearson

Paperback ISBN-10: 0134794109

Paperback ISBN-13: 9780134794105

eTextbook on Pearson+: 9780138091712

Price: eText: \$59.94; Paperback: \$84.99

Course 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.

Academic Integrity

Academic integrity is integral to your learning, the credibility of your degree or certification, and the integrity of the university as a whole. [Senate Policy 60: Academic Integrity](#) defines academic misconduct, provides a non-exhaustive list of examples of behaviours that may be considered as academic misconduct, and explains how academic misconduct concerns are evaluated and decided. The entirety of the policy applies in this course. As well, please note that submitting work created in whole or in part by artificial intelligence tools unless expressly permitted by the faculty/contract lecturer, is considered a violation of Policy 60.

Generative AI Course Policy, and Plagiarism Detection

Generative AI Course Policy

Use of Generative AI (e.g. ChatGPT, Grammarly, Perplexity, DeepL Translator) to develop or assist with any ideas or material submitted for coursework is expressly prohibited in this course. Use of Generative AI in this manner will be considered a breach of Policy 60.

Turnitin or another originality detection software

Turnitin is a plagiarism prevention and detection service to which TMU subscribes. It is a tool to assist faculty/contract lecturers 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 faculty/contract lecturers some assurance that students' work is their own. No decisions are made by the service; it generates an "originality report," which faculty/contract lecturers 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. Instructors can opt to have student's papers included in the Turnitin database or not. Use of the Turnitin service is subject to the terms-of-use agreement posted on the Turnitin 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 faculty/contract lecturer to make alternate arrangements. Students who choose not to have their papers screened for textual similarity review by turnitin may be required to submit additional work with their research essay. For example:

- an annotated bibliography of each source used in your paper; and/or
- the first few pages of each cited source used in your paper

Even when an faculty/contract lecturer 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 faculty/contract lecturer has reason to suspect that an individual piece of work has been plagiarized, the faculty/contract lecturer is permitted to submit that work in a non-identifying way to any plagiarism detection service.

Copyright

The course materials provided to you are copyrighted, and may not be shared without my express written permission. Do not share these materials (e.g. course outline, lecture slides, assignment instructions) with others and do not post them on the internet during the course, or at any time after. If you do so, Policy 60 will apply.

Academic Integrity Resources

To learn more about Policy 60 and how to avoid academic misconduct, please review and take advantage of these resources:

- Policy 60: Academic Integrity: www.torontomu.ca/senate/policies/academic-integrity-policy-60/
- Academic Integrity Office website: www.torontomu.ca/academicintegrity
- “Academic Integrity in Space” game: <https://games.de.torontomu.ca/aio/#/>
- “Academic Integrity in Cyberspace!” game: <https://www.torontomu.ca/aic/#/>
- Student Life and Learning Support: www.torontomu.ca/student-life-and-learning/learning-support

If you are a student registered with Academic Accommodation Support (AAS):

Please inform your faculty/contract lecturer if you have test accommodation needs that include the use of assistive technology (including text-to-speech, dictation, or literacy software). Some software may require additional configurations by the faculty/contract lecturer, so it is important you inform them in advance and leverage the sample quiz to ensure the tools are compatible with the Brightspace Quiz in LockDown Browser.

However, not all Assistive Technology tools approved by AAS work well with Respondus' software; if your experience of the sample quiz does not function as expected, please notify your faculty/contract lecturer and/or Accommodation Facilitator.

Topics and Course Schedule

Week	Topic	Readings
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	Stallings & Brown: Chapter 1 & Lecture notes
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	Stallings & Brown: Chapter 2 & Lecture notes
3	User Authentication and Access Control - 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	Stallings & Brown: Chapters 3, 4 & Lecture notes
4	Database and Data Center Security - Discuss the unique need for database security - Describe SQL injection attacks - Compare different approaches of database security - Discuss key concepts of data center security	Stallings & Brown: Chapter 5 & Lecture notes
5	Malicious Software - Explain types of Malicious Software - Discuss the basic operations of viruses, worms, Trojan horses, and logic bombs - Discuss the different threats posed by bots, spam, spyware, rootkits, and Advanced Persistent Threat - Discuss the backdoor vulnerabilities of systems	Stallings & Brown: Chapter 6 & Lecture notes
6	Denial-of-Service Attacks - Explain the basic concepts of DoS and DDoS attacks - Describe flooding attacks - Application-Based Bandwidth Attacks - Explain Reflector and Amplifier Attacks - Discuss defenses Against Denial-of-Service Attacks	Stallings & Brown: Chapter 7 & Lecture notes
7	Midterm Examination Firewall, Intrusion Detection and Prevention Systems - Explain snort architecture - Explain the purpose of honeypots	Stallings & Brown: Chapters 8, 9 & Lecture notes

	- Describe different types of honeypots and sandboxes - Explain the role of firewalls, proxies, and NAT in a network	
8	Operating System Security and 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	Stallings & Brown: Chapters 12, 19 & Lecture notes
9	Wireless Network Security - Explain components of 802.11 standards and WLAN - Explain WEP and WPA authentication methods - Describe advanced features of 802.11i technology	Stallings & Brown: Chapter 24 & Lecture notes
10	IT Security Management and Risk Assessment; Security Controls, Plans and Procedure - Explain ISO IT security standards - Discuss organizational IT security policy - Discuss IT security plans - Identify security threats and security risk assessments	Stallings & Brown: Chapters 14, 15 & Lecture notes
11	Symmetric Encryption and Message Confidentiality - 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.	Stallings & Brown: Chapter 20 & Lecture notes
12	Physical and Infrastructure Security; Security Auditing - Discuss measures for physical disaster and recovery plans - Discuss physical and logical security integration - Describe benefits of security awareness, training, and education - Describe the process of security compliance, audits, and trails	Stallings & Brown: Chapters 16, 18 & Lecture notes

Evaluation

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

Evaluation Component	Due Date	Percentage of Final Grade	Anticipated Return Date
Assignments	Weeks 2, 4, 6, & 8	20%	Week 4, 6, 8, 10
Group Project	Week 11	10%	Week 13
Midterm Exam	Week 7	30%	Week 9
Final Exam	TBA	40%	TBD
Final Grade		100%	
Note: Students must achieve a course grade of at least 50% to pass this course. At least 20% of the grade based on individual work will be returned to students prior to the last date to drop a course in good academic standing. For Fall 2026 this must be before Friday, November 20, 2026 and for Winter 2027 before Friday, April 2, 2027.			

University Policies

Students must be reminded that they are required to adhere to all relevant university policies found in their online course shell in D2L and/or on [the Senate website](#).

Important Resources Available at Toronto Metropolitan University

- **Addressing Academic Concerns:** Students are expected to address any questions or concerns through open and timely communication with the course faculty/contract lecturer, as soon as they arise. If a concern cannot be resolved through this initial communication or if additional support is required, students are encouraged to reach out to their program advisor or the chair/director of the teaching department for further guidance. These individuals can help provide clarity, facilitate next steps, and ensure that matters are reviewed in a fair and appropriate manner.
- [The University Libraries](#) provide research [workshops](#) and individual consultation appointments. There is a drop-in Research Help desk on the second floor of the library, and students can use the [Library's virtual research help service](#) to speak with a librarian, or [book an appointment](#) to meet in person or online.
- [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, always require documentation. Students must notify their faculty/contract lecturer once a request for academic consideration is submitted. See Senate [Policy 167: Academic Consideration](#).

Longer absences are not addressed through Policy 167 and should be discussed with your Chair/Director/Program to be advised on next steps.

- [FAQs Academic Considerations and Appeals](#)
- Information on Copyright:
 - [Copyright FAQs for Faculty/Contract Lecturers](#)
 - [Copyright FAQs for Students](#)
- Information on Academic Integrity:
 - [Academic Integrity for Faculty/Contract Lecturers](#)
 - [Academic Integrity for Students](#)

Accessibility

- At Toronto Metropolitan University, we are committed to ensuring that all courses are accessible to everyone and to removing barriers that may prevent some individuals from enrolling in courses.
- All technologies and tools used in this course are accessible.
- Students who discover an accessibility barrier with any of the course materials or technologies should contact their faculty/contract lecturer.
- As outlined in [Policy 159: Academic Accommodation of Students with Disabilities](#), students are required to proactively consult with AAS, the faculty/contract lecturer, 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 accessibility services office, supporting students with disabilities. AAS works with students, faculty, and staff to create inclusive learning environments, reduce barriers, and promote accessibility across the university.

If you have (or suspect you may have) a disability, AAS can provide consultation, guide you through registration, develop accommodation plans where appropriate, and connect you with supports and services. For information about eligibility, documentation requirements, registration, deadlines, and available services, visit [AAS](#).

Academic Accommodations (for students with disabilities) and Academic Consideration (for short-term extenuating circumstances) are governed by **different university policies**. [Learn more about each process](#) and how to access support. Students registered with AAS may request academic consideration (related or unrelated to their

disability) if they experience extenuating circumstances that impact their ability to meet their shorter term academic obligations. This includes short term physical or mental health issues that are sudden/acute (e.g, the flu), unexpected illness or injury, hospitalization or treatment, and significant aggravation of a pre-existing condition. Please see [Policy 167: Academic Consideration](#) for more information and details.

Please note that there is no accommodation for missing/rescheduling or reweighting of tests - this is considered an alternate arrangement. Any student who misses a test/exam will be directed to submit an ACR to explore if possible alternate arrangements under [Policy 167: Academic Consideration](#) can apply.

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)
- **[GuardMe Student Support Program \(GMSSP\)](#):** 24/7 access to confidential support through counsellors via the [Student Support 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's Wellbeing Central](#) website.