GLIS 629 Information Security (3 credits)

1. Course Description

- Introduction to information security. Topics include basic concepts of confidentiality, integrity, and availability; security threats; access control; cryptography (encryption, decryption, passwords and digital signature); malware (viruses, trojan horses, worms, botnets, etc.); operating systems security; network security; cloud security; security policies and practices; risk assessments; privacy threats and protection techniques; cybercrime and cyber forensics.
- Prerequisite: GLIS 617 – Information System Design

2. Learning Outcomes

By the end of the course, students will be able to:

- explain the fundamental concepts of information security: confidentiality, integrity, and availability (CIA)
- identify the major physical and cyber security threats faced by organizations today
- understand the technical aspects of access control, encryption and decryption, and digital signatures.
- classify different types of malware and describe their basic mechanisms
- explain the purpose of some commonly used security techniques, including firewalls, anti-virus software, vulnerability analysis tools, etc.,
- perform threat and risk assessments
- assess and develop security policies for an organization
- understand the fundamental principles of cyber forensics

3. Lecture Notes, Textbook and Articles

- Lecture notes: Powerpoint slides provided by the instructor.
- Santos M., Greene S. Developing Cybersecurity Programs and Policies, Third Edition. Pearson IT Certification, 2018. Available on the Safari Books Online platform through McGill's Catalogue.
- Sandhu, Ravi S., and Samarati, Pierangela. "Authentication, Access Control, and Intrusion Detection." Web. 1996.
- CERT-UK "An introduction to Malware." Web. 2014.
- National Institute of Standards and Technology Special Publications 800-30, Revision 1, "Guide for Conducting Risk Assessments." September 2012.
- Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC press. 2001. ISBN: 0-8493-8523-7. A free copy is available here http://cacr.uwaterloo.ca/hac/

4. Evaluation (tentative)

1. Short assignments & presentations: 30%
2. Mid-term exam: 40%
3. Final project: 30%

5. Tentative Time Table

Date	Week	Class Content	Readings
Jan. 7	1	• Course information • Confidentiality, Integrity, and Availability (CIA) • Threats, Vulnerabilities and Controls • Common security threats	
14	2	• Handoff assignment 1 • Access control	
21	3	• Encryption and decryption • Digital signatures • Public key certificates	
28	4	• Operating system security	
Feb. 4	5	• Malware and anti-virus software • Common security protection techniques: Hardening, Firewalls, etc.	
11	6	• Handoff assignment 2 • Network & cloud security	
18	7	• Security policies and practices	
25	8	• Mid-term exam	
Mar. 4	**Study Break**		
Mar. 11	9	• Privacy • PCI compliance	
18	10	• Risk assessments	
25	11	• Handoff assignment 3 • Review session	
Apr. 1	12	• Cybercrime and cyber forensics • Final project due	

6. McGill Policy Statements

- McGill University values academic integrity. Therefore, all students must understand the meaning and consequences of cheating, plagiarism and other academic offences under the Code of Student Conduct and Disciplinary Procedures. See http://www.mcgill.ca/students/srr/honest for more information.
- In accord with McGill University's Charter of Students' Rights, students in this course have the right to submit in English or in French any written work that is to be graded.
- Instructor generated course materials (e.g., handouts, notes, summaries, exam questions, etc.) are protected by law and may not be copied or distributed in any form or in any medium without explicit permission of the instructor. Note that infringements of copyright can be subject to follow up by the University under the Code of Student Conduct and Disciplinary Procedures.
- If you have a disability, please contact the instructor to arrange a time to discuss your situation. You may also consider contacting the Office for Students with Disabilities at 514-398-6009 before discussing with the instructor.
- Mobile computing and communications devices are permitted in class insofar as their use does not disrupt the teaching and learning process.
- End-of-course evaluations are one of the ways that McGill works towards maintaining and improving the quality of courses and the student's learning experience. You will be notified by e-mail when the evaluations are available on Mercury, the online course evaluation system. Please note that a minimum number of responses must be received for results to be available to students.
- McGill has policies on sustainability, paper use and other initiatives to promote a culture of sustainability at McGill. (See the Office of Sustainability.)
- In the event of extraordinary circumstances beyond the University's control, the content and/or evaluation scheme in this course is subject to change.

7. Student's Responsibilities

- Students are expected to read the assigned materials and to actively participate in class discussions.