COURSE OUTLINE: CSD227 - COMPUTER SECURITY

Prepared: D. Kachur
Approved: Corey Meunier, Chair, Technology and Skilled Trades

Course Code: Title	CSD227: COMPUTER SECURITY, PRIVACY, AND ETHICS
Program Number: Name	2095: COMPUTER PROGRAMMING
Department:	COMPUTER STUDIES
Academic Year:	2023-2024
Course Description:	This course focuses on high-level computer, network and cloud security and privacy concepts. The learner will apply hands-on skills in establishing then implementing security policies to protect systems and data from internal and external threats. The topics of cyber-security, ransomware, social engineering and phishing will be explored in detail. Cryptography, encryption and hashing methods along with firewall defence, will be applied in various scenarios, then tested for resiliency. Packet Analysis tools will be used by the learner to extract data flowing through systems and across networks.
Total Credits:	4
Hours/Week:	4
Total Hours:	56
Prerequisites:	CSD123, CSD213
Corequisites:	There are no co-requisites for this course.
Vocational Learning Outcomes (VLO's) addressed in this course: **Please refer to program web page for a complete listing of program outcomes where applicable.**	**2095 - COMPUTER PROGRAMMING** VLO 2 Contribute to the diagnostics, troubleshooting, documenting and monitoring of technical problems using appropriate methodologies and tools. VLO 3 Implement and maintain secure computing environments. VLO 8 Adhere to ethical, legal, and regulatory requirements and/or principles in the development and management of computing solutions and systems. VLO 13 Contribute to the integration of network communications into software solutions by adhering to protocol standards.
Essential Employability Skills (EES) addressed in this course:	EES 1 Communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience. EES 2 Respond to written, spoken, or visual messages in a manner that ensures effective communication. EES 4 Apply a systematic approach to solve problems. EES 5 Use a variety of thinking skills to anticipate and solve problems. EES 6 Locate, select, organize, and document information using appropriate technology and information systems. EES 7 Analyze, evaluate, and apply relevant information from a variety of sources. EES 8 Show respect for the diverse opinions, values, belief systems, and contributions of others.

	EES 9 Interact with others in groups or teams that contribute to effective working relationships and the achievement of goals. EES 10 Manage the use of time and other resources to complete projects. EES 11 Take responsibility for ones own actions, decisions, and consequences.
Course Evaluation:	Passing Grade: 50%, D A minimum program GPA of 2.0 or higher where program specific standards exist is required for graduation.
Other Course Evaluation & Assessment Requirements:	A+ = 90-100% A = 80-89% B = 70-79% C = 60-69% D = 50-59% F < 50% Students are expected to be present to write all tests in class, unless otherwise specified. If a student is unable to write a test due to illness or a legitimate emergency, that student must contact the professor prior to class and provide reasoning. Should the student fail to contact the professor, the student shall receive a grade of zero on the test. If a student is not present 10 minutes after the test begins, the student will be considered absent and will not be given the privilege of writing the test. Students exhibiting academic dishonesty during a test will receive an automatic zero. Please refer to the College Academic Dishonesty Policy for further information. In order to qualify to write a missed test, the student shall have: a.) attended at least 75% of the classes to-date. b.) provide the professor an acceptable explanation for his/her absence. c.) be granted permission by the professor. NOTE: The missed test that has met the above criteria will be an end-of-semester test. Labs / assignments are due on the due-date indicated by the professor. Notice by the professor will be written on the labs / assignments and verbally announced in the class. Labs and assignments that are deemed late will have the following penalty: 1 day late - 10% reduction, 2 days late, 20% reduction, 3 days late, 30% reduction. After 3 days, no late assignments and labs will be accepted. It is the responsibility of the student who has missed a class to contact the professor immediately to obtain the lab / assignment. Students are responsible for doing their own work. Labs / assignments that are handed in and are deemed identical or near identical in content may constitute academic dishonesty and result in a zero grade. Students are expected to be present to write in-classroom quizzes. There are no make-up options for missed in-class quizzes. Students have the right to learn in an environment that is distraction-free, therefore, everyone is expected to arrive on-time in class. Should lectures become distracted due to students walking in late, the professor may deny entry until the 1st break period, which is 50 minutes into the class or until that component of the lecture is complete. The total overall average of test scores combined must be 50% or higher in order to qualify to pass this course. In addition, combined tests, Labs / Assignments total grade must be 50% or higher.

Course Outcomes and Learning Objectives:

Course Outcome 1	Learning Objectives for Course Outcome 1
1. Computer / Network / Cloud Security	1.1 Identify components that make up Cyber Security 1.2 Define and research attack types including Phishing, Ransomware and Social Engineering 1.3 Identify and discuss issues faced in today`s world of computer security 1.4 Examine the roles of those in the security industry that defend networks and devices 1.5 Research and analyze recent and current cyber security threats 1.6 Analyze techniques used to attack and defend computers 1.7 Discuss why software patches must be up-to-date to secure the network 1.8 Identify potential weaknesses in open-source software 1.9 Review the most common techniques used to break computer security 1.10 Review common passwords and password generation 1.11 Research cyber security job / career opportunities
Course Outcome 2	**Learning Objectives for Course Outcome 2**
2. Corporate Security Policy	2.1 Identify the importance of having a corporate security policy 2.2 Discuss components that should be included in a corporate security policy 2.3 Identify why user education is so important with relevance to understanding the policy 2.4 Create a detailed security policy to address the needs of a corporation 2.5 Recognize the importance of keeping the policy up-to-date with current trends / threats 2.6 Discuss where the future of security might be heading and potential new threat types
Course Outcome 3	**Learning Objectives for Course Outcome 3**
3. Firewalls	3.1 Explain how firewalls work and what they do 3.2 Contrast both software and hardware firewalls 3.3 Create, then apply, software firewall rules 3.4 Test your firewall from a client device 3.5 Discuss firewall network policies 3.6 Monitor firewall activity and logs
Course Outcome 4	**Learning Objectives for Course Outcome 4**
4. Cryptography	4.1 Describe and explain cryptography 4.2 Differentiate between encryption and hashing 4.3 Discuss public keys and the difference between symmetric and asymmetric encryption 4.4 Examine different encryption techniques and compare 4.5 Examine different hashing techniques and compare 4.6 Apply encryption and hashing knowledge to real applications 4.7 Understand how hashing tables work and their applications
Course Outcome 5	**Learning Objectives for Course Outcome 5**

5. Risk	5.1 Identify threats, vulnerabilities, and risk 5.2 Understand threat monitoring, vulnerability assessment, and risk management 5.3 Create risk matrices and describe risk with computer applications 5.4 Understand disaster recovery and business continuity 5.5 Explore then explain Cyber-Security Insurance
Course Outcome 6	**Learning Objectives for Course Outcome 6**
6. Privacy	6.1 Understand the difference between privacy and anonymity 6.2 Explain the difference between staying secure, staying private, and staying anonymous 6.3 Understand biometrics and how it is used and calculated for computer security 6.4 Understand access control 6.5 Explain how logging can help with security but also increase privacy concerns 6.6 Review real world privacy breaches and their impact on the world around us 6.7 Review real world Terms of Service and agreements which are signed by billions of people 6.8 Explain PIPEDA and its role in Canadian technology 6.9 Explain anti-spam legislation and the effect it has on the role of web developers
Course Outcome 7	**Learning Objectives for Course Outcome 7**
7. Ethics	7.1 Understand what a white hat, black hat, and grey hat hacker is and the difference 7.2 Explain how ethical decisions are made all the time with computer programming 7.3 Examine real world ethical dilemmas with computer security 7.4 Identify methods to collect information and understand how to collect just enough 7.5 Explore and discuss the topic of the dark web and the effect on ethics

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Assignments and Labs	40%
Test 1	30%
Test 2	30%

Date: May 31, 2023

Addendum: Please refer to the course outline addendum on the Learning Management System for further information.