Carleton University

Office of the Vice-Provost
(Academic and Global Learning)

memorandum

DATE: January 23, 2026

TO: Senate

FROM: Dr. David J. Hornsby, Vice-Provost (Academic and Global Learning), and Chair, Senate Quality Assurance and Planning Committee

RE: BEng Systems Security Engineering
New Program Approval

SQAPC Motion

THAT SQAPC recommends to Senate the approval of the BEng in Systems Security Engineering program as presented, to commence in Fall 2027.

Senate Motion

THAT Senate approve the proposed BEng in Systems Security Engineering program as presented, to commence in Fall 2027.

Background

The proposed undergraduate program in Systems Security Engineering focuses on the analysis, evaluation and design of secure computer communications and distributed systems. It will be a four-year Bachelor of Engineering program, (or a five-year program with COOP). The key feature of the curriculum is the holistic approach to computer system security, by coupling threats to the network and system components/protocols. The advanced content and electives will include modern technologies such Software Defined Networks, cloud environments, or security applied to infrastructures.

Attachments

Self-Study with Appendices (Volume I)
Discussant Report
Site Visit Schedule
External Reviewer Biographies
External Reviewers' Report
Unit response to the External Reviewers' Report and Implementation plan
Dean's response to the External Reviewers' Report
Courseleaf Entries

Quality Assurance Framework and Carleton's Institutional Quality Assurance Process (IQAP)

Upon the above motion being passed by Senate, the required documentation will be submitted to the Ontario Universities' Council on Quality Assurance for approval. A submission to the Ministry for approval will follow. These approvals are required before the program can commence.

Carleton University

Office of the Vice-Provost and
Associate Vice-President (Academic)

Institutional Quality Assurance Process

Systems Security Engineering

New Program Approval Template

(Volume I)

October 2024

Approvals Table

This table will record that the brief has been approved by: 1) the program lead on behalf of the team; 2) the head of the academic unit or chair of the program committee (in the case of interdisciplinary programs not administered exclusively by one academic unit) on behalf of the unit or program committee; 3) the Faculty Dean(s).

Program Lead	**Date**
Jerome Talim, Assistant Professor, FED	November 26, 2024
Chair/Director	**Date**
Yvan Labiche, Chair, Dept. of Systems and Computer Engineering, FED	
Dean(s):	**Date**
Larry Kostiuk, Dean, FED	December 17, 2024

Committees Reviews and Approvals

Vice-Presidents' Academic Research Committee (executive summary)	
Provost's Budget Working Group (executive summary)	
Curriculum Committee	
Faculty Board	
Senate Committee on Curriculum, Admissions on Studies Policy	
Senate Quality Assurance and Planning Committee	
Senate	
Quality Council	

Contents

A. The Program

A.1. Program overview

The Department of Systems and Computer Engineering is proposing a new Bachelor of Engineering program in Systems Security Engineering. It will be a four-year Bachelor of Engineering program, (or a five-year program with COOP), with the main focus on the analysis, the evaluation and the design of secure computer communications and distributed systems.

In today's world, where most of the services rely on distributed systems and telecommunications services, there is a crucial need for secure computer systems and networks. The department currently offers three Engineering programs in Information Technology (IT):

(a) Computer Systems Engineering,
(b) Communications Engineering
(c) Software Engineering

These programs train future professionals to design and develop new technologies or services in their respective field, with a primary focus on the technical feasibility and development, while the security, in terms of cyber threats and cyber-attacks, is often considered at deployment or management. A global approach to cybersecurity must span over all components of the system: hardware, software and networking technologies, over the entire design and implement process. The goal of the proposed program is to prepare graduates for careers in secure computer networks solutions design or in distributed systems design.

1. The Department Academic Advising Board which comprises professionals from various IT fields, and from industries in the Ottawa areas and in Canada, unanimously recognized the need for experts in systems and networks security engineering.

2. The curriculum of the proposed program will rely on existing courses at introductory level as well as at advanced level and whose content is already part of accredited programs.
3. The department will consider online synchronous delivery of selected upper year courses. The development of the new courses introduced by the proposed program will consider the academic content and the feasibility of online delivery for the lecture and the laboratory/Problem analysis sessions. If successful, after few years, the experience will provide solid background and framework to extend the option to other courses offered by the department. The online synchronous delivery, combined with a well-designed courses schedule may be very attractive to potential students.
4. Many of the new courses in computer and network security rely on modern software tools, used by the industries to monitor, manage and analyze computer networked systems. The proposed program will integrate such software tools in the laboratory component and the project-based courses.

2) Goal of the new program

The purpose of the proposed program is to form future professionals who are knowledgeable in distributed systems (computer architecture and networking technologies) and who can evaluate existing system configuration or applications in order to identify threats and vulnerabilities that attackers can exploit. The technical content includes network protocols threats, secure design solutions, and analysis of various attacks targeting network and system components. The program will also provide practical approach to security, with government standards, legal aspects of cybersecurity, risks modelling and impact on users and institutions.

The key feature of the curriculum is the holistic approach to computer system security, by coupling threats to the network and system components/protocols. The advanced content and electives will include modern technologies such Software Defined Networks, cloud environments, or security applied to infrastructures.

3) Program Structure

The first-year curriculum of the proposed program is common to all Engineering programs. Students will be able to transfer to another program after the first year without missing any course or losing any completed credit.

The upper year courses are organized as follows

- 1.5 credits in in Software development
- 2.0 credits in Computer Systems Engineering, more specifically in computer architecture and operating systems
- 1.5 credits in Communication Engineering
- 1.5 credits in Systems Security
- 1.5 credits in Cybersecurity Standards, Ethics and Practice

The following Table summarizes the program content:

Year	Course Materials	Credits
1	Math / Science / Basic Science	2.5
	Engineering Core	2.0
	Software Engineering	0.5
	Engineering Profession (3 ECOR courses)	0.0
2	Math / Basic Science	1.5
	Electrical Engineering	0.5
	Software Engineering	1.0
	Computer Systems Engineering	1.0
	Cybersecurity Standards, Ethics and Practice	0.5
	Systems and Computer Engineering Core Course	0.5
3	Computer Systems Engineering	1.0
	Communications Engineering	1.0
	Systems Security	1.0
	Engineering Core	1.0
	CCDP	0.5
	Complementary Studies	0.5
4	Communications Engineering	0.5
	Systems Security	0.5
	Cybersecurity Standards, Ethics and Practice	1.0
	Capstone Project	1.0
	Engineering Elective	2.0
	Engineering Core	0.5
	Complementary Studies	0.5
	Total	21.0

The program will introduce 7 new core courses in systems security and cybersecurity standards, ethics and practice. The department will also introduce new courses as electives which will present more advanced topics in autonomous vehicles, Internet of Things, cryptography, security applied to infrastructures (Hydro, Air traffic, Traffic systems, Telecom, healthcare). Those will also be relevant to the other IT programs.

The three following Tables provide the sequence of courses, with and without the cooperative education option):

First year			
1.	**a) 4.5 credits in**		4.5
	CHEM 1101 [0.5]	Chemistry for Engineering Students	
	ECOR 1031 [0.5]	Programming and Data Management	
	ECOR 1032 [0.5]	Circuits and Mechatronics	
	ECOR 1033 [0.5]	Statics	
	ECOR 1034 [0.5]	Dynamics	
	MATH 1004 [0.5]	Calculus for Engineering or Physics	

	MATH 1104 [0.5]	Linear Algebra for Engineering or Science	
	PHYS 1004 [0.5]	Introductory Electromagnetism and Wave Motion	
	SYSC 1006 [0.5]	Imperative Programming	
	b) The introduction to Engineering Disciplines requirement must be met through the successful competition of		
	ECOR 1055 [0.0]	Introduction to Engineering Disciplines I	
	ECOR 1056 [0.0]	Introduction to Engineering Disciplines II	
	ECOR 1057 [0.0]	Engineering Profession	
2.	**0.5 credit in** Science Electives		0.5
Second year			
3.	**a) 4.0 credits in**		4.5
	COMP 1805 [0.5]	Discrete Structures I	
	~~COMP 2804 [0.5] Discrete Structures II~~		
	MATH 1005 [0.5]	Differential Equations and Infinite Series for Engineering or Physics	
	SYSC 2010 [0.5] or SYSC 2004 [0.5]	Programming Project or Object-Oriented Software Development	
	SYSC 2100 [0.5]	Algorithms and Data Structures	
	SYSC 2310 [0.5]	Introduction to Digital Systems	
	SYSC 2320 [0.5]	Introduction to Computer Organization and Architecture	
	SYSC 2510 [0.5]	Probability, Statistics and Random Processes for Engineers	
	~~SYSC 2xxx~~ SYSC 2821	~~Computer Network and Security Foundations~~ Introduction to cybersecurity	
	b) Successful Completion of:		
	ECOR 2995 [0.0]	Engineering Portfolio	
4.	**0.5 credit in** Complementary Studies Electives		0.5
5.0	**0.5 credit in Science Elective**		
Third year			
6.	**5.0 credits in**:		4.5
	CCDP 2100 [0.5]	Communication Skills for Engineering Students	
	ECOR 2050 [0.5]	Design and Analysis of Engineering Experiments	
	ECOR 3800 [0.5]	Engineering Economics	
	SYSC 3310 [0.5]	Introduction to Real-Time Systems	
	SYSC 3512 [0.5]	Computer Communications	
	~~SYSC 3522 [0.5]~~ SYSC 4416 [0.5]	~~Communications Software Laboratory~~ Artificial Intelligence in Engineering	

	~~SYSC 3xxx [0.5]~~ SYSC 3821 [0.5]	~~Physical Layer, principles and Security~~ Data Security and Cryptography	
	~~SYSC 3xxx [0.5]~~ SYSC 3821 [0.5]	~~Computer Networks Security~~ Network Security I	
	SYSC 3523 [0.5]	Introduction to distributed applications	
	SYSC 4001 [0.5]	Operating Systems	
~~**6.**~~	~~**0.5 credit in** Science Electives~~		~~0.5~~
Fourth year			
7.	**2.5 credits in**:		2.5
	ECOR 4995 [0.5]	Professional Practice	
	~~SYSC 4xxx [0.5]~~ SYSC 4831 [0.5]	~~Computer Systems Security~~ Software Security	
	~~SYSC 4xxx [0.5]~~ SYSC 4831 [0.5]	~~Secure Systems and Communications~~ Network Security II	
	~~SYSC 4xxx [0.5]~~ SYSC 4821 [0.5]	~~Advanced Network Security~~ Security in Emerging Technologies	
	~~SYSC 4xxx [0.5]~~ SYSC 4822 [0.5]	Network Security Development Project	
8.	**1.0 credit from**:		1.0
	SYSC 4907 [1.0]	Engineering Project	
	OR		
	ECOR 4997 [1.0]	Multidisciplinary Engineering Project	
9.	**2.0 credits from**:		2.0
	SYSC at the 3000 level or above (may include 1.0 credit in SYSC at the 5000 level)		
10.	**0.5 credit in** Complementary Studies Electives		0.5
Total Credits			21.0

Program schedule without cooperative education:

Year 1	Year 2	Year 3	Year 4
			[1.0 credit] SYSC 4907
[0.5 credit] MATH 1004 MATH 1104 CHEM 1101 PHYS 1004	[0.5 credit] MATH 1005 COMP 1895 ~~COMP 2804~~	[0.5 credit] CCDP 2100 ECOR 2050 ECOR 3800 SYSC 3512 [CNP]	[0.5 credit] ECOR 4995 SYSC 4822 [CNP - NSS] SYSC 4832 [NSS] SYSC 4821 [CSEP}

ECOR 1031 ECOR 1032 ECOR 1033 ECOR 1034 SYSC 1006 [SD] Basic Science Elective	SYSC 2010 or SYSC 2004 [SD] SYSC 2100 [SD] SYSC 2310 [CSA] SYSC 2320 [CSA] SYSC 2510 SYSC 2821 [CSEP} Complementary Studies Elective Science Elective	SYSC 3310 [CSA] SYSC 4001 [CSA] SYSC 3821 [NSS] SYSC 33822 [NSS] SYSC 33523 [SD] SYSC 4416 [SD]	SYSC 4831 [NSS} Engineering Elective Engineering Elective Engineering Elective Engineering Elective Complementary Studies Elective
[0.0 credit] ECOR 1055 ECOR 1056 ECOR 1057		[0.0 credit] ECOR 2995	
Notes: SD: Software Development CSA: Computer System and Architecture CNP: Computer Network Protocol NSS: Networks and Systems Security CSEP: Cybersecurity Standards, Ethics and Practice Possible Engineering Elective Topics: Autonomous vehicles, Internet of Things, Network forensics, Cryptography, Security in infrastructures (Hydro, Air traffic, Traffic systems, Telecom, Healthcare systems),			

Program schedule with cooperative education

Year 1	Year 2	Year 3	Year 4	Year 5
				[1.0 credit] SYSC 4907
[0.5 credit] MATH 1004 MATH 1104 CHEM 1101 PHYS 1004 ECOR 1031 ECOR 1032 ECOR 1033 ECOR 1034 SYSC 1006 [SD] Basic Science Elective	[0.5 credit] MATH 1005 COMP 1895 SYSC 2010 [SD] SYSC 2100 [SD] SYSC 2310 [CSA] SYSC 2320 [CSA] SYSC 2510 SYSC 2821 [CSEP} Complementary Studies Elective Basic Science Elective	[0.5 credit] CCDP 2100 ECOR 2050 ECOR 3800 SYSC 3512 [CNP] SYSC 3310 [CSA] SYSC 4001 [CSA] SYSC 3821 [NSS[SYSC 3822 [NSS] SYSC 3523 [SD]		[0.5 credit] ECOR 4995 SYSC 4822 [CNP - NSS] SYSC 4832 [NSS] SYSC 4821[CSEP} SYSC 4831 [NSS} Engineering Elective Engineering Elective Engineering Elective Engineering Elective Complementary Studies Elective
[0.0 credit] ECOR 1055	[0.0 credit] **COOP 1000**	[0.0 credit] ECOR 2995	[0.0 credit] **SYSC 3999 [Fall]**	

ECOR 1056 ECOR 1057	**SYSC 3999 [Summer]**	**SYSC 3999 [Summer]**	**SYSC 3999 [Winter]** **SYSC 3999 [Summer]**	

A minimum of four successful registration in SYSC 3999 is required to graduate with the COOP designation.

Current International, National and Provincial Profile

There is currently no accredited Bachelor of Engineering degree in systems security or in cybersecurity, in Canada (https://engineerscanada.ca/). The accredited Engineering degrees in IT are in Software Engineering or Computer Systems or Computer Engineering, and cybersecurity is often covered either in overview core courses or as electives.

The Accreditation Board for Engineering and Technology (https://www.abet.org/) in the United States reports the following accredited Bachelor of Science degrees in cybersecurity:
(a) Bachelor of Science in Cybersecurity Engineering[1], at the University of Alabama in Huntsville, which has a stronger emphasis on secure software development.
(b) Bachelor of Science in Cyber Security Engineering[2], at George Mason University, which has similar academic objectives on security in computer and network systems but with a focus on the cyber-physical systems, such as industrial control systems and critical infrastructures.
(c) Bachelor of Science in Cyber Security Engineering[3], at the Iowa State University, whose curriculum is focused on the physical, software and human components of the system.

The Government of Canada web site https://www.cyber.gc.ca/ dedicated to Post-secondary cyber security related programs lists:
(a) the Bachelor of Information Technology in Networking and Information Technology Security[4] at the University of Ontario Institute of Technology (UOIT), which allocates larger credits to system and network configuration, administration and management to secure the infrastructure.
(b) the Bachelor of Science in Computer Security[5] at York University, which has limited credits on security in network protocols and larger content in software.
(c) the Bachelor of Science in Information Security[6] at the University of Toronto, which covers computer security on a more theoretical approach with content number theory and computation complexity.

A.2. Mission and strategic directions

Carleton Strategic Integrated Plan (SIP) defines three strategic directions:

[1] https://www.uah.edu/eng/departments/ece/programs/undergraduate/cybersecurity
[2] https://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/cyber-security-engineering-bs/#requirementstext
[3] https://catalog.iastate.edu/collegeofengineering/cybersecurityengineering/#fouryearplantext
[4] https://ontariotechu.ca/programs/undergraduate/computers-and-technology/information-technology-networking-and-information-technology-security/index.php
[5] https://calendars.students.yorku.ca/academic-calendar#/programs/Hyx5YfX1d/S1qlzret_?searchTerm=computer%20s&bc=true&bcCurrent=Computer%20Security%20-%20Bachelor%20of%20Science%20-%20Specialized%20Honours&bcItemType=programs
[6] https://future.utoronto.ca/undergraduate-programs/information-security/

1) Share the knowledge, shape the future
2) Serve Ottawa, serve the world
3) Strive for wellness, strive for sustainability

The proposed program fits the first two directions:

Share the knowledge, shape the future: This BEng program in Systems Security will meet the demand for professionals in cybersecurity and who can cooperate with experts in other IT or more generally engineering fields. It will prepare the students for a successful career in a world of fast-paced technological innovations in computer systems and telecommunications and with continuously increasing threats inherent to the heterogenous and complex nature of the technologies. The expertise of the new faculty hires will strengthen the contributions of Carleton to the field and to the development of solutions to new challenges in cybersecurity.

Serve Ottawa, serve the world: Ontario in general, and more specifically Kanata, is the largest technology park in Canada. Ottawa is also the home of many governmental offices, with strong interest and legal requirements in information systems security and cybersecurity in general. Offering the new program will result in highly trained professionals, who can work with the IT teams, at the design, development, deployment or management of new services. The employers from the private sector or government agencies will also benefit from the future research and development collaborations with new faculty members.

Inclusivity and Accessibility: As mentioned previously, the department plans to implement online synchronous delivery of selected courses in upper years, with a special focus on the new courses in cybersecurity. The development of the courses content will offer the opportunity to integrate modern software tools in teaching activities and to support the learner's experience. The long-term aim is to develop a general teaching framework that can be applied to more courses in Engineering, enabling flexible learning experiences to all students, regardless of their individual learning needs.

A.3. Relationship to other academic programs at Carleton

A3.1 – Relationship to Other Programs within the University

Cybersecurity is a multi-disciplinary field that combines Computer Engineering, Computer Science, Information Systems, Information Technology and Software Engineering[7]. Designing an academic curriculum in the field may have focus on data security, software security, components security, connections security or systems security. The proposed program sets the emphasis on the latter, by considering security in the complete full stack (network components and protocols, computer systems and software).

We do not expect the new program to significantly modify the enrollment of the other BEng programs. Each existing BEng program and the proposed one are distinct disciplines, with overlapping competencies, and leading to different career paths. The proposed program is a response to the increasing need for professionals and problem solvers in cybersecurity.

[7] https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf

As far as programs in Computer Science are concerned, the proposed program is distinct enough in its design and its content that we expect it to attract a different pool of students. The Bachelor of Cybersecurity program sets the primary focus on security at the software level (either at the development stage or services deployment stage). It covers in depth contents with a significant software component, such as Human-Computer interaction, Web applications, Software Quality and Cryptography.

The Bachelor in Systems Security Engineering addresses security from a holistic point to view by considering the whole computer system composed of components (hardware), connections (network devices and protocols), operating systems and software. Mechanisms supporting computer communications and distributed systems will be covered in details by pairing the logic and implementation of the system with the inherent vulnerabilities. And security at the software development level has much less emphasis. Graduates of the proposed program in Systems Security will be well prepared for a career in cybersecurity architecture for networked systems and in forensic analysis.

A3.2 – Service courses offered by the Faculty of Engineering and Design and the other Faculties

The curriculum of the proposed program comprises 3.5 credits of Engineering common core (ECOR) courses (along with 4 0.0-credit ECOR courses). The ECOR courses are offered by the four Engineering departments. The curriculum also includes 1.5 credits in MATH, 3.0 credits in Natural Science and in Computer Science, and 2.5 credits in Complementary Studies and in Communications, from the Faculty of Arts and Social Sciences.

B. Program Learning Outcomes and Assessment

B.1 Program learning outcomes and degree level expectations

The program learning outcomes (Table B.1) for the proposed program in Systems Security have been developed to align with the Graduate Attributes[8] defined by the Canadian Engineering Accreditation Board.

Table B.1: Learning outcomes

Learning Outcomes
1 – Demonstrate competence in University level mathematics, natural sciences, engineering fundamentals, and software, computer systems and networks engineering
2 – Formulate system's functional and non-functional requirements. Analyze computer networks and systems security to identify vulnerabilities and propose recommendations or remediation techniques
3 – Define appropriate testbed environment and define simulation setup to evaluate computer systems. Identify systems vulnerabilities from collected data or produced results.

[8] See https://engineerscanada.ca/sites/default/files/2023-12/Accreditation_Criteria_Procedures_2023.pdf, Section 3.1

4 – Design and develop secure networked systems to meet technical and functional constraints using engineering techniques and methods in software, computer systems and networks
5 – Select appropriate techniques and software tools to analyze computer systems vulnerabilities and or simulate systems attacks.
6 – Work effectively as a member of a team or as a team leader, in a context of project development, using interpersonal skills and group dynamics to resolve conflicts
7 – Communicate complex engineering concepts within the profession and with society at large, that includes oral presentation, technical reports, design documentations and instructions.
8 – Understand the roles and responsibilities of a professional engineer in computer network and systems security, especially in the protection of the public and the public interest. Understand of the impact that computer security has with the economic, health, safety, and legal aspects of society.
9 – Incorporate economics and business practices including project, risk, and change management into the practice of engineering and to understand their limitations.
10 – Identify and address professional development needs in a fast evolving information and computer technology world, to maintain adequate level of competence and to contribute to the advancement of knowledge.

B2: MAPPING LEARNING OUTCOMES TO PROVINCIAL DEGREE-LEVEL EXPECTATIONS (DLEs)

Table B.2: Learning outcomes and degree level expectations

Learning Outcomes	Degree Level Expectations Met[9]
1	1. Depth and breadth of knowledge
1, 2, 3	2. Knowledge of methodologies
3, 4, 5	3. Application of knowledge
7, 8	4. Communication skills
5, 10	5. Awareness of the limits of knowledge
6, 8,9,10	6. Autonomy and professional capacity
2, 3, 4, 5, 6	7. Experiential Learning

B.3 Program structure and curriculum map

a. Program structure

Table B3.1 – Program Components

Component/Teaching topic	Comments	Total credits
Math / Natural Sciences	3 courses in Math. 1 course in SYSC 1 course in Chem. 1 course in Phys. 2 science electives	1.5 0.5 0.5 0.5 1.0

Additional information on the DLEs can be found at: https://oucqa.ca/framework/appendix-1/

Computer Science	12 course	0.5
Engineering core course	6 courses	3.0
Engineering profession related course	1 course 4 courses	0.5 0.0
Complementary Studies / Communications	3 courses	1.5
Software Development	3 courses	1.5
Computer Systems	4 courses	2.0
Computer Networks	2 courses	1.0
Networks and Systems Security Cybersecurity Standards, Ethics and Practice	4 courses 3 courses	2.0 1.5
Capstone Project	1 course	1.0
Engineering Elective	4 courses	2.0
Total	45 courses	21.0

Table B3.2 – Course requirements

Math / Natural Sciences – 4.0 credits		
MATH 1004	0.5	Calculus for Engineering Students
MATH 1104	0.5	Linear Algebra for Engineering Students
MATH 1005	0.5	Differential Equations & Infinite Series for Engineering Students
CHEM 1101	0.5	Chemistry for Engineering Students
PHYS 1004	0.5	Introductory Electromagnetism & Wave Motion
SYSC 2510	0.5	Probability, Statistics and Random Processes for Engineers
Elective	1.0	Basic Science Elective
Computer Science – 1.0 credit		
COMP 1805	0.5	Discrete Structures I
Engineering Core courses – 3.0 credits		
ECOR 1031	0.5	Programming and Data Management
ECOR 1032	0.5	Circuits and Mechatronics
ECOR 1033	0.5	Statics
ECOR 1034	0.5	Dynamics
ECOR 2050	0.5	Design and Analysis of Engineering Experiments
ECOR 3800	0.5	Engineering Economics
Engineering profession related course – 0.5 credit		
ECOR 1055	0.0	Introduction to Engineering Disciplines I
ECOR 1056	0.0	Introduction to Engineering Disciplines II
ECOR 1057	0.0	Engineering Profession
ECOR 2995	0.0	Engineering Portfolio
ECOR 4995	0.5	Professional Practice
Complementary Studies / Communications – 1.5 credits		
CCDP 2100	0.5	Communication Skills for Engineering Students
Elective	1.0	Complementary Studies
Software Development – 2.0 credits		
SYSC 1006	0.5	Foundations of Imperative Programming (formerly SYSC 2006)
SYSC 2010	0.5	Algorithms and Data Structures
SYSC 2100	0.5	Programming Project
or SYSC 2004		Object-Oriented Software Development

SYSC 3823	0.5	Introduction to distributed applications
Computer Systems – 2.0 credits		
SYSC 2310	0.5	Introduction to Digital Systems
SYSC 2320	0.5	Introduction to Computer Organization and Architecture
SYSC 3310	0.5	Introduction to Real-Time Systems
SYSC 4001	0.5	Operating Systems
Computer Networks – 0.5 credits		
SYSC 3512	0.5	Computer Communications (formerly SYSC 4602))
[NSS] Networks and Systems Security – 2.0 credits		
SYSC 3821SYSC 3822SYSC 4832SYSC 4831	0.5 0.5 0.5	Data security and cryptographic Network security I Network security II Software security
[CSEP] Cybersecurity Standards, Ethics and Practice – 1.5 credits		
SYSC 2821SYSC 4822SYSC 4821	0.5 0.5 0.5	Intro to cybersecurity Network Security Development Project Security in emerging technologies
Artificiial Intelligence – 0.5 credit		
SYSC 4416	**0.5**	**Artificial Intelligence in Engineering**
Engineering Capstone Project – 1.0 credit		
SYSC 4907 Or ECOR 4907	1.0	Engineering Project
Engineering Elective – 2.0 credits		
SYSC at the 3000 level or above (may include 1.0 credit in SYSC at the 5000 level)		

b. Program curriculum map

Table B.3: Program curriculum map summary

Learning Outcomes	Year(s) to be Assessed[1]	Program Components[10]	Level[11] (I, R, M)	Activities and Artifacts[12]
1. Demonstrate competence in University level mathematics, natural sciences, engineering fundamentals, and software, computer systems and networks engineering	1st and 2nd year	ECOR 1xxx, Math, Natural Sciences, Computer Science, SYSC 1006	I	Exam, Lab, Assignment
	2nd year and 3rd year	SYSC 2xxx, SYSC 3310, SYSC 4001, SYSC 3512	R	
	3rd and 4th year	, New courses in NSS	M	
2. Formulate system's functional and non-functional requirements. Analyze computer networks and systems security to identify vulnerabilities and propose recommendations or remediation techniques	2nd	SYSC 2010	I	Exam, Lab, Assignment
	3rd and 4th	New courses in NSS and CSEP	R/ M	
3. Define appropriate testbed environment and define simulation setup to evaluate computer systems. Identify systems vulnerabilities from collected data or produced results.	3rd and 4th	ECOR 2050 New course in NSS	I R, M	Exam, Lab, Assignment

[1] The year the learning outcome will be assessed, with each learning outcome assessed a minimum of two times.
[10] Program components should include those core courses, elective courses, options (co-op, internship, mention Français, international experience), and other program requirements (language requirement, international experience) which contribute most directly to the achievement of the particular learning outcome.
[11] Level of delivery of each program component related to the particular learning outcome: I = introductory; R = Reinforcement; M = Mastery (relevant to the expected outcome at the degree level).
[12] Activities can include presentations, group work, performance, role play, etc. Artifacts can include exams, papers, reports, portfolios, cases, etc.

4. Design and develop secure networked systems to meet technical and functional constraints using engineering techniques and methods in software, computer systems and networks	2nd 3rd and 4th	SYSC 2010 New courses in NSS, Capstone Project	I R, M	Exam, Lab, Assignment, or Project report
5. Select appropriate techniques and software tools to analyze computer systems vulnerabilities and or simulate systems attacks.	3rd and 4th	New courses in NSS	I, M	Exam, Lab, Assignment
6. Work effectively as a member of a team or as a team leader, in a context of project development, using interpersonal skills and group dynamics to resolve conflicts	3rd and 4th	Engineering Core project in 1st year, and project-based courses (new course in CSEP and capstone project)	R, M	Lab or Project report
7. Communicate complex engineering concepts within the profession and with society at large, that includes oral presentation, technical reports, design documentations and instructions.	3rd and 4th	Complementary Studies, CCDP 2100, New course in CSEP and Capstone project	R, M	Exam, Lab, Assignment, or Project report
8. Understand the roles and responsibilities of a professional engineer in computer network and systems security, especially in the protection of the public and the public interest. Understand of the impact that computer security has with the economic, health, safety, and legal aspects of society.	2nd, 3rd and 4th	ECOR 4995 And new courses in CSEP	R, M	Exam, Lab, Assignment or Project report

9. Incorporate economics and business practices including project, risk, and change management into the practice of engineering and to understand their limitations.	3rd and 4th	ECOR 3800, and project-based new course in CSEP	R, M	Exam, Lab, Assignment, or Project report
10. Identify and address professional development needs in a fast-evolving information and computer technology world, to maintain adequate level of competence and to contribute to the advancement of knowledge.	3rd and 4th	Complementary Studies, Communications and Professional related courses, and engineering electives	I, R, M	Exam, Lab, Assignment

B.4 Program learning outcomes assessment plan

The accreditation criteria and procedures are defined by the Canadian Engineering Accreditation Board (CEAB) and require the implementation of the Graduate Attributes (GAs), along with a clearly defined Continual Improvement process. In the evaluation of an undergraduate Engineering program, the following criteria will be assessed:

- **Organization and engagement**: requirement of an organization structure to assure the sustainable development and measurement of the GAs. And requirement of engagement of faculty members and engineering leadership.
- **Curriculum maps**: requirement to map the learning activities for each GA and to record the semesters in which the assessment takes place
- **Assessment tools and results**: requirement to document the assessment tools that are appropriate to the GAs and that are used as the basis for obtaining the data on student learning with respect to the GAs over a cycle of six years or less. Requirement to collect assessment results over a period of six years of less, along with the either clear evidence that the graduates possess the GAs defined for the program or that remedial action is in progress.
- **Improvement process and actions**: Requirement that program outcomes are being assessed and the results are validated, analyzed and applied to further development of the program.

The assessment of the proposed program will be conducted based on the same process used for the other programs:

- The curriculum mapping defines the GAs or learning outcomes associated to each course.
- Before the term starts, instructors will be provided with a template of the course syllabus with the course objectives and the associated GAs. Instructors select the assessment tools, possibly after consulting the archives from previous terms.

- At the end of the term, the instructors submit the GA data and upload the course material (course syllabus, assignments, laboratory description, examination papers, and three samples of students work (below average, average, and above average samples)) to the course archive.
- Instructors also submit a GA report, where they describe the assessment tools used to evaluate the class. They also have the opportunity to comment the collected GA data and make suggestions on actions to improve or change the course delivery and/or the assessment.
- The review of the assessment results is completed at the department level and at the faculty level:
    a) The Faculty deployed an application that manages the courses material, and the GA data; it generates reports of GA charts, enables download of samples of students' work. Samples can be selected from submitted assignments, laboratory reports, project reports, or examinations answers. Once all GA data is submitted and approved by the department Chair or by the GA coordinator, the report for each GA can be generated.
    b) In the context of the GAs review and the Continual Improvement process, all GAs must be reviewed during a period of six years. F-APC reviews three GAs every academic year. The list of GAs scheduled for review in an academic year is communicated to the Department Chair and Associate Chair (Undergraduate Studies).
    c) Once the most recent GA data is submitted and approved, the generated GA data and report, along with the relevant assessment tools are made available to the department.
    d) The Department Academic Planning Committee (D-APC) compiles the assessment results per learning outcome, validates, analyzes the data and makes recommendations for calendar change or curriculum mapping. Any course or program change will be brought to the Department for approval. D-APC is chaired by the Associate Chair (Planning) and opened to any faculty member of the department.
    e) The Faculty Academic Planning Committee (F-APC) collects the calendar changes from all engineering departments, discusses and approves the proposed changes, before the final approval by the Engineering Faculty Board.

Since the proposed program introduces new courses mostly in the third and fourth year, the department will review the academic content, courses delivery and any assessment results at the end of Year 3 and Year 4 to make any appropriate adjustments to the curriculum.

B.5 Program Essential Requirements

PREAMBLE

"Program essential requirements are defined by the Ontario Human Rights Commission as "the knowledge and skills that must be acquired or demonstrated in order for a student to successfully meet the learning objectives of that… program." The program essential requirements are components that contribute to the achievement of the learning outcomes of the program.

"An appropriate accommodation at the post-secondary level would enable a student to successfully meet the essential requirements of the program, with no alteration in bona fide standards or outcomes, although the way the student demonstrates mastery, knowledge and skills may be altered."

-Ontario Human Rights Commission's Policy on Accessible Education for Students with Disabilities (2018)

The aim of accommodation in a post-secondary context is to provide equal opportunities to all students to enjoy the same level of benefits and privileges and meet the requirements for acquiring an education. Based on these principles, an accommodation will be considered appropriate where it will result in equal opportunity for an otherwise qualified student with a disability to attain the same level of performance, or enjoy the same level of benefits and privileges experienced by others, without compromising bona fide academic requirements.

Paul Menton Centre for Students with Disabilities (PMC)

The Paul Menton Centre is responsible for assessing requests for academic accommodation of students with disabilities through evaluations that are carried out on an individual basis, in accordance with human rights legislation and University policy, and with the support of relevant, professional/medical documentation. Students will only receive academic accommodation if the functional limitations of their disability impact directly on their academic performance."

The program essential requirements of the Bachelor of Engineering in Systems Security Engineering program have been reviewed in consultation with the Paul Menton Centre to ensure capacity for reasonable academic accommodation of students with disabilities, in accordance with the Carleton University Academic Accommodation Policy. The learning outcomes can be attained as outlined in the program description with the use of appropriate academic accommodations.

C. Governance

The proposed program is solely managed by the Department of Systems and Computer Engineering. The primary committee in charge of the governance will be the Department Academic Planning Committee (D-APC). The Department Chair will appoint a Program Coordinator who will work closely with the Associate Chair for undergraduate program planning to monitor the delivery and the students learning experience and to coordinate any program or course change. Besides the academic content, D-APC will also monitor any requirement change adopted by the Canadian Engineering Accreditation Board (CEAB). As described in Section B.4, D-APC will make recommendations for calendar changes to the department, before forwarding them to the Faculty for approval.

D. The Faculty

D.1. Faculty appointed to the unit or program.

1) Table D.1 provides the list of faculty who will be involved in the delivery of the core courses, in software development, computer systems and architecture and computer communications. The program will introduce seven new courses in computer security covering from the physical components to the software and deployed services components. The plan to develop the new courses, to ensure a stable delivery of the program and to strengthen the research in cybersecurity will require four new continuing faculty members (one assistant professor teaching stream and three in the research stream.

- **Current and missing expertise**: In addition to the faculty members from Communications Engineering program, the department counts also faculty with strong research in security either at the software components level or at the operating systems level. Additional faculty positions with research interests in security in advanced technologies such as cloud computing or autonomous vehicles, or in the integration of artificial intelligence to security approach will ensure a solid delivery of the proposed program but also the other undergraduate and graduate programs.
- **Retirements**: One core faculty member with research interest in advanced computer communications will retire in 2027. A second faculty member will retire the following year; even though they are not involved directly in teaching of the core courses of the proposed program, it will be having an impact on the department teaching assignment and program delivery.
- **Teaching needs**: The standard teaching workload of a faculty member includes one graduate course, two undergraduate courses and the supervision of the capstone project. Some of the first- and second-year core courses, common to other engineering programs, will see a significant increase in enrollment with the introduction of the propose program. The additional new faculty positions (in research) will be essential to maintain the teaching workload.

The department as a whole has a good balance of senior and junior faculty. However, core faculty in the department currently include various ranks with more junior faculty in the teaching stream. Senior faculty have research programs including post-doctoral fellows and collaborate with adjunct faculty which will help influence the evolution of the curriculum. With the addition of the new faculty members,

the department will focus on improving the EDI ratios, encouraging gender balance and diversity in our faculty members. This is a long-term endeavour that we continue to make progress on.

The teaching workload in the departments is balanced between the graduate programs and undergraduate programs such that, except for an otherwise approved reduced teaching load, each faculty member generally teaches one graduate course, and the rest of the default overall course load is dedicated to undergraduate education, including the supervision of undergraduate 4th year level capstone engineering projects (similar to honours projects in other disciplines). This will continue with the introduction of the mechatronics program and will not impact the delivery of existing undergraduate/graduate programs, provided new faculty positions are created and filled.

Table D.1: Core program faculty

Faculty Name	Rank	Appointment Status	Percentage Appointment	Supervision Privileges*	Area of Specialization/Field Affiliations
Banihashemi, Amir	Full Professor	Tenured	100	D	Digital and Wireless Communications, Coding and Information Theory, Signal Processing and Algorithms
Dansereau, Richard	Full Professor	Tenured	100	D	Signal processing (audio, video), multimodal signal processing
Huang, Changcheng	Full Professor	Tenured	100	D	Stochastic Control in Computer Networks, Modelling and Simulation Techniques, Resource Optimization in Wireless Networks, Reliability Mechanisms for Optical Networks, Network Protocol Design and Implementation Issues
Ibn Khala, Mohamed	Full Professor	Tenured	100	D	Wireless sensor networks, Internet of Things (IoT), cognitive radio networks, adaptive signal processing, reconfigurable networks, sensor integration, radio frequency identification (RFID) systems
Lambadaris, Ioannis	Chancellor's Professor	Tenured	100	D	Applied Stochastic Processes and Control Performance Analysis of IP Network, Cross Layer design for Wireless Networks, Wireless Ad-hoc networks, Network Security
Liu, Xiaoping Peter	Full Professor	Tenured	100	D	Interactive networked systems, Haptics with applications to medical simulations, Robotics, control and intelligent Systems, Context-aware smart networks, Wireless sensor networks
Lung, Chung-Horng	Full Professor	Tenured	100	D	Software Architecture, Self-Managing Systems, Software Defined Networking (SDN), Traffic Engineering and QoS,

					Wireless Communications, Ad-Hoc Networks, Network-Based Control Systems, IoT, Big Data Analytics, Real-Time Concurrent Software
Majumdar, Shikharesh	Chancellor's Professor	Tenured	100	D	Parallel and Distributed Systems, Performance Modelling and Performance Evaluation of Computer Systems, Resource Management on Clouds and Grids, Resource Management on Wireless Sensor Networks, Web Services and Service Oriented Architecture
Rajan, Sreeraman	Full Professor	Tenured	100	D	Sensor systems, signal processing, adaptive signal processing, compressive sensing,
Wainer, Gabriel	Full Professor	Tenured	100	D	Real-Time modelling, Cellular models, Modelling and simulation methodologies and tools, Parallel/distributed/Web-based simulation, Real-Time operating systems
Yanikomeroglu, Halim	Chancellor's Professor	Tenured	100	D	Cellular networks (5G, 4G, LTE/LTE-A), Radio access networks, Relay / multihop / mesh networks, Cooperative communications, Multiple access, OFDMA, MAC Routing, scheduling, Sensor networks, User-in-the-loop in wireless networks, Intelligent transportation systems
Atia, Mohamed	Associate Professor	Tenured	100	D	Advanced sensor fusion methods on real-time embedded systems.
Gohary, Ramy	Associate Professor	Tenured	100	D	Machine-to-machine communications, IoT, Analysis and design of MIMO wireless communication systems, Cooperative communications,

					Applications of iterative detection and decoding techniques in multiple antenna and multiuser systems
Jaskolka, Jason	Associate Professor	Tenured	100	D	Cyber Security Evaluation and Assurance, Engineering Secure and Trustworthy Software-Dependent Systems, Formal Methods for specification, verification and validation
Marsland, Ian	Associate Professor	Tenured	100	D	Wireless digital communications (stationary and mobile), Error control coding (convolutional and turbo codes), Applications of iterative decoding
Assal, Hala	Assistant Professor (Teaching)	Preliminary	N/A	N/A	Human-centric research, User-centric cybersecurity and privacy, Human-centric software security, Security and privacy in emerging technologies
Bedawi, Safaa	Assistant Professor (Teaching)	Preliminary	N/A	N/A	Software Engineering
Gomar, Shaghayegh	Assistant Professor (Teaching)	Preliminary	N/A	N/A	Digital Systems Design, Embedded Systems and FGPAs. Bio-inspired Neural Networks
Marshall, Lynn	Assistant Professor (Teaching)	Preliminary	N/A	N/A	Software engineering
Ruiz Martin, Cristina	Assistant Professor (Teaching)	Preliminary	N/A	N/A	Organizational Resilience, Discrete-Event Modeling and Simulation. Agent-Based Modeling, Network Theory
Taha, Mostafa	Assistant Professor	Preliminary	100	CD	Security of Embedded Systems and the Internet of Things., Implementation Attacks and Countermeasures, Side-Channel Analysis. Secure Implementation of Cryptographic Algorithms. Design of Side-Channel Resilient Cryptographic Algorithms.

Talim, Jerome	Assistant Professor	Tenured	100	CD	Distributed Systems. Web Services. Traffic Engineering and QoS, Optimization in Computer Networks, Systems Modelling and Simulation, Performance Evaluation.

*D=full privileges; M=full privileges at master's level only; CD=co-supervision privileges at doctoral level, full privileges at master's level; CDM=co-supervision privileges only at both doctoral and master's level; CM=co-supervision privileges at master's level, no privileges at doctoral level

D.2. Faculty research funding.

Faculty members are very active in research. The Table D.2 below provides the research funding over the period of 5 years. Senior faculty members have established strong and sustainable research funding, in addition to partnerships with industries. The research contributes to the undergraduate programs delivery in two ways:

- Solid research in either computer network technologies or in cybersecurity attracts excellent graduate students. Those students are usually offered Teaching Assistant grants while working on their thesis and have the experience and knowledge to supervise the laboratory sessions.
- Colleagues take every opportunity to instill knowledge acquired through research into undergraduate education, by offering engineering electives in selected or advanced topics, by defining laboratory experiments based their research, or co-supervising capstone projects with a researcher from an industry partner. Such a support of undergraduate student learning through research expertise/experience, is evidenced by the many undergraduate students whom colleagues have supervised over the years (see section D.3).

Table D.2: Operating Research Funding by Source and Year

	Source						
Year	Tri-Council	Internal	Canadian	US	International	Other	Totals
2020	$1,102,500	$140,000	$4,547,984	-	$73,420	-	$5,863,904
2021	$1,460,628	$459,000	$1,635,897	-	-	-	$3,555,525
2022	$1,395,500	$1,060,000	$411,417	-	-	$62,000	$2,928,917
2023	$688,000	-	$424,741	-	$48,000	$49,000	$1,209,741
2024	$520,000	$40,000	$741,980	$53,880		$874,349	$2,230,209
TOTALS	$5,166,628	$1,699,000	$7,762,019	$53,880	$121,420	$985,349	$15,788,296

D.3. Distribution of thesis supervision.

At the undergraduate level, supervisory activities typically take place in fourth year with a two-semester long, 1.0 credit capstone project course. Engineering program accreditation requires a substantial content in design and in collaborative team work. The capstone project offers an important opportunity to work on more complex problems, where students can demonstrate their problem-solving skills, research abilities, project and time management skills, group-work dynamics and communications skills. Students can either register in SYSC 4907 (department capstone project) or in ECOR 4907 (multi-disciplinary project). In the latter option, they will cooperate with students from another department.

Most projects are proposed by faculty members. The list of active projects is posted on the department web site for students to consult and identify topics of interest to them and potential supervisors. Occasionally they are proposed by student groups themselves, in such a case a faculty member validates the content and agrees to supervise the group. Students must select a project with respect to their discipline. The students of the proposed program will be required to complete a capstone project with application to and/or design in systems security.

At the graduate level, students typically find a faculty supervisor prior to admission through website information and direct inquiries. Or, in certain cases, the Associate Chair, Graduate Studies, can help connect students with thesis supervisors. As far as graduate research supervision is concerned, it is expected that the listed faculty will continue at their current pace.

Table D.3: Distribution of thesis supervision

Faculty Name	Rank	Completed				Current			
		Undergraduate	Master's	PhD	PDF	Undergraduate	Master's	PhD	PDF
Banihashemi, Amir	Full Professor	(19)	(0)	(4)	(1)	(0)	(1)	(1)	(0)
Richard Dansereau	Full Professor	(43)	(1)	(3)	(1)	(22)	(1)	(3)	(0)
Huang, Changcheng	Full Professor	(48)	(3)	(6)	(1)	(0)	(2)	(3)	(0)
Ibn Khala, Mohamed	Full Professor	(40)	(5)	(3)	(2)	(6)	(0)	(5)	(0)
Lambadaris, Ioannis	Chancellor's Professor	(12)	(3)	(0)	(4)	(5)	(2)	(5)	(5)
Liu, Xiaoping Peter	Full Professor	(24)	(0)	(3)	(0)	(9)	(0)	(2)	(0)
Lung, Chung-Horng	Full Professor	{22)	(12)	(2)	(1)	(5)	(4)	(3)	(1)
Majumdar, Shikharesh	Chancellor's Professor	(14)	(5)	(3)	(0)	(0)	(3)	(0)	(0)
Sreeraman Rajan	Full Professor	(32)	(7)	(4)	(4)	(0)	(5)	(8)	(2)
Wainer, Gabriel	Full Professor	(23)	(12)	(8)	(7)	(10)	(6)	(2)	(2)
Yanikomeroglu, Halim	Chancellor's Professor	(21)	(6)	(13)	(19)	(5)	(11)	(11)	(4)
Mohamed Atia	Associate Professor	(23)	(7)	(3)	(1)	(0)	(2)	(2)	(0)
Gohary, Ramy	Associate Professor	(43)	(3)	(5)	(1)	(0)	(0)	(2)	(1)
Jaskolka, Jason	Associate Professor	(4)	(9)	(0)	(1)	(0)	(2)	(6)	(0)
Marsland, Ian	Associate Professor	(16)	(1)	(0)	(0)	(4)	(1)	(3)	(0)

Assal, Hala	Assistant Professor	(9)	(4)	(0)	(1)	(4)	(3)	(1)	(0)
Bedawi, Safaa	Assistant Professor, Teaching Stream	(9)	N/A	N/A	N/A	(16)	N/A	N/A	N/A
Gomar, Shaghayegh	Assistant Professor, Teaching Stream	(13)	N/A	N/A	N/A	(11)	N/A	N/A	N/A
Marshall, Lynn	Assistant Professor, Teaching Stream	(91)	N/A	N/A	N/A	(30)	N/A	N/A	N/A
Ruiz Martin, Cristina	Assistant Professor	(27)	(2)	N/A	N/A	(2)	N/A	N/A	N/A
Taha, Mostafa	Assistant Professor	(23)	(1)	(0)	(1)	(12)	(0)	(3)	(0)
Talim, Jerome	Assistant Professor	(18)	(2)	(0)	(0)	(8)	(0)	(0)	(0)

D.4. Current teaching assignments

The typical teaching workload includes two undergraduate 0.5-credit courses, one graduate 0.5-credit course and the supervision of capstone projects. Faculty members in teaching streams are typically assigned a total of 2.0 credit courses. Flexible arrangements may be made to accommodate specific situation, such as a third undergraduate course instead of a graduate course, or reduced workload. The workload involved with the capstone projects includes the supervision and the evaluation of projects supervised by other faculty members.

Most courses in upper years are core courses to some program and valid electives to others. Only very few courses are offered as electives and in most cases, they can be used for credit for more than one programs. That will also be the case of the electives defined for the proposed program as topics in Internet of Things, Cloud computing, autonomous vehicles or security in infrastructures are relevant to students in software engineering, computer systems engineering, communications engineering or electrical engineering.

The hiring of new faculty members for the proposed program will facilitate the distribution of teaching assignment, including such things as allowing additional sections of currently offered courses to be created as enrollment increases, and the creation of new elective courses to meet the needs of the new program.

Table D.4: Distribution of Teaching Assignments

Faculty Name	Courses Taught			Notes
	2024/25	2023/24	2022/23	
Banihashemi, Amir	SYSC 5503 SYSC 4607	SYSC 5506 SYSC 4607	SYSC 5503 SYSC 4607	Reduced workload
Dansereau, Richard	SYSC 4405 SYSC 5602	SYSC 4405	SYSC 4405 SYSC 5602	Reduced courseload (Associate Dean)
Huang, Changcheng	SYSC4502 SYSC5108	SYSC4602	SYSC4602 SYSC4907 SYSC4005/5001 SYSC5108	SYSC 4907: Capstone project coordinator
Ibn Khala, Mohamed	ECOR1055 SYSC4602 SYSC5809 SYSC4906	ECOR1055 SYSC5809	SYSC5809	
Lambadaris, Ioannis	SYSC3501	SYSC3501 SYSC5502	SYSC3501 SYSC5502	
Liu, Xiaoping Peter	SYSC3501 BIOM5402 SYSC3200 SYSC5303	BIOM5402 SYSC3200 SYSC5303	SYSC3501	
Lung, Chung-Horng	SYSC4701 SYSC2006 SYSC4907 SYSC5801	SYSC4001 SYSC4701 SYSC4907 SYSC5801	SYSC4001 SYSC4701 SYSC5801	SYSC 4907: Capstone project coordinator SYSC 2006 will be renumbered as SYSC 1006
Majumdar, Shikharesh	SYSC3310 SYSC5206	SYSC3310 SYSC5206	SYSC4001 SYSC5206	
Rajan, Sreeraman	SYSC3500 SYSC3501	SYSC3500 SYSC5602		
Wainer, Gabriel	SYSC4001 SYSC5104	SYSC3310 SYSC4001 SYSC5104	SYSC3310 SYSC4001 SYSC5104	
Yanikomeroglu, Halim	SYSC4700 SYSC5608	SYSC4604 SYSC4700	SYSC4700 SYSC5608	

		SYSC5608		
Atia, Mohamed	SYSC 2320 SYSC 5702	Sabbatical	SYSC 3310	
Gohary, Ramy	SYSC2320 SYSC3006	SYSC2320 SYSC3006 SYSC2320 SYSC5004	SYSC2320 SYSC2320 SYSC5004	
Jaskolka, Jason	SYSC3120 SYSC4120 SYSC5805	Sabbatical	SYSC4810 SYSC4120 SYSC5805	
Marsland, Ian	SYSC3600 SYSC3503 SYSC4600	SYSC5504 SYSC3503	SYSC3503 SYSC4600	
Assal, Hala	SYSC 4810 SYSC 4130 SYSC 5807	SYSC 4810 SYSC 4130 SYSC 5807	SYSC 3020 SYSC 4906 SYSC 5807	
Bedawi, Safaa	SYSC3110 SYSC2100 SYSC2100 SYSC3101	ECOR1042 ECOR1042 SYSC2006 SYSC2100 SYSC3101	ECOR1041 ECOR1042 ECOR1041 ECOR1042 SYSC2006	ECOR 1041 [0.24 cr] and ECOR 1042 [0.25 cr] will be combined to ECOR 1031 [0.5 cr] SYSC 2006 will be renumbered as SYSC 1006
Gomar, Shaghayegh	SYSC2310 SYSC2310 SYSC4310 SYSC2310 SYSC3320	SYSC2310 SYSC4310 SYSC2310 SYSC3320	SYSC4310 SYSC2310 SYSC3320	
Marshall, Lynn	ECOR1041 ECOR1041 SYSC2006 ECOR1042 ECOR1042 SYSC2004	ECOR1041 ECOR1041 ECOR1041 ECOR1041 ECOR1041 SYSC2004 SYSC2004	SYSC2006 SYSC2310 SYSC2004 SYSC2004	ECOR 1041 [0.24 cr] and ECOR 1042 [0.25 cr] will be combined to ECOR 1031 [0.5 cr] SYSC 2006 will be renumbered as SYSC 1006

Ruiz Martin, Cristina	ECOR1042 ECOR1042 SYSC2006 ECOR1041 ECOR1041 SYSC2004	SYSC2006 SYSC2006	ECOR1042 SYSC2006 SYSC2004	ECOR 1041 [0.24 cr] and ECOR 1042 [0.25 cr] will be combined to ECOR 1031 [0.5 cr] SYSC 2006 will be renumbered as SYSC 1006
Taha, Mostafa	SYSC4805 SYSC4810 SYSC5807	SYSC5807	SYSC4805 SYSC4810 SYSC5807	
Talim, Jerome	SYSC4906	ECOR2995 SYSC2100	ECOR2995 ECOR1057 ECOR1057 ECOR1057 ECOR1057 ECOR2995 ECOR1056 ECOR1056 ECOR1056 ECOR1056 SYSC3303	Currently reduce courseload

D.5. Contract instructors

Contract instructors can be an important resource to help manage year to year variations in available teaching resources due to sabbaticals, illnesses, teaching release, and unanticipated changes in teaching requirements. However, our reliance on contract instructors is relatively low and has been declining overall in recent years. Increasing numbers of full-time faculty through new hires have allowed us to significantly reduce our reliance on contract instructors.

The delivery of the proposed program is planned to rely only on full-time faculty members. A higher number of students in some the courses in early years may require the creation of additional sections which may require the temporary use of extra contract instructors until new faculty members are hired. However, like all the other programs, with the addition of new faculty positions as expected, the proposed program should not rely on contract instructors.

E. Program Admission and Enrolment

E.1. Admissions requirements

The admission requirements for all B.Eng. programs are the same. Admission requirements are based on the Ontario High School System. Prospective students can view the admission requirements through the Admissions website (https://admissions.carleton.ca/). The overall average required for admission is determined each year on a program-by-program basis. Holding the minimum admission requirements only establishes eligibility for consideration; higher averages are required for admission to programs for which the demand for places by qualified applicants exceeds the number of places available. All programs have limited enrolment and admission is not guaranteed.

For admission into first year, an Ontario Secondary School Diploma (OSSD) or equivalent including a minimum of six 4U or M courses is required. The six 4U or M courses must include four prerequisite 4U courses: Advanced Functions, Chemistry, Physics, and one of Calculus and Vectors (recommended), or Biology, or Earth and Space Science. Although it is not an admission requirement, at least one 4U course in either English or French is recommended.

Applications for admission beyond 1st-year (*i.e.*, Advanced Standing) will be assessed on their merits. Successful applicants will have individual academic subjects, completed with grades of C- or higher, evaluated for academic standing, provided the academic work has been completed at another university or degree-granting college, or in another degree program at Carleton University.

All engineering programs come with a co-op option. Direct admission to the first year of the co-op option requires the applicant to meet the required overall admission cut-off average and prerequisite course average. These averages may be higher than the stated minimum requirements; be registered as a full-time student in the Engineering degree; and be eligible for work in Canada (for off-campus work placements).

For international students, Carleton University has established procedures to determine equivalency on academic proficiency, as well as a need for proof of English competency for different countries.

E.2. Class sizes and course and program capacity

Based on the projected enrolment, after six years, the enrolment of the proposed program in Systems Security could be approximately 20% of the total number of undergraduate students in the department. It is essential to keep the class sizes of current core courses at today's levels. And it is likely that some courses will need to be broken into more sections to preserve the quality of material delivery and the learning experience.

With respect to the first year (1000-level) courses, many of these common core courses are based around large lecture sections, supported by scheduled smaller group problem solving sessions. It is expected that the addition of more students will trigger the need for more sections. The following Table provides the current distribution for 2023/24, of 1000 level ECOR courses (Engineering Common Core) offered by the four departments: Civil and Environmental Engineering (CEE), Dept. of Electronics (DOE), Mechanical and Aerospace Engineering (MAAE), Systems and Computer Engineering (SCE)

Table E.2a – Number of lecture sections of ECOR 1xxx vs. enrolment

Course enr.	**1-10**	**11-20**	**21-30**	**31-40**	**41-60**	**61-80**	**81-100**	**101-120**	**121-140**	**141-160**	**161-180**	**181-200**	**201-220**	**221-240**	**240+**
CEE			1	1		2	1		1	2	3		2	2	2
DOE		2			1			1						2	6
MAAE				1			1				1		1	1	6
SCE		1				1		1		1			1	1	6

The courses with an enrolment less than 100 are mostly ECOR 1055 (Introduction to Engineering Professions I). There is a section assigned to each program, and the course provides an overview of the program discipline (academic content, and/or career paths).

The following Table provides the number of lecture sections distributed with respect to course enrolment, from 2023/24. The Table provides the distribution of the course SYSC, offered by the department and for various course levels (1000, 2000, 3000, and 4000). Some of the third- and fourth-year courses have some atypically large class sizes and more section offerings will be needed in future years. The resources needed for these sections are described in detail later, but they are part of the investment plan from the University and Faculty.

Table E.2a – Number of lecture sections of SYSC course vs. enrolment

Course enr.	**1-10**	**11-20**	**21-30**	**31-40**	**41-60**	**61-80**	**81-100**	**101-120**	**121-140**	**141-160**	**161-180**	**181-200**	**201-220**	**221-240**	**240+**
1000		1				1		1		1			1	1	6
2000		1		1	1	1	1	2	3	1	1		3		
3000	2			1	2	2	3	5	1	4	2	1			
4000		3	5	4	4	3	4		3	4	1	1			

E.3. Projected enrolment

The proposed enrolment shown in the Table E.3 is based exclusively on domestic students. The data is extracted from the business plan generated by the Office of Institutional Research & Planning. The basic parameters of the model are:

- Undergraduate Retention – Bachelor of Engineering
    - One Year retention 92%
    - Two Year retention 84%
    - Three year retention 74%
- Admission Targets into First Year:
    - Year 1: 80
    - Year 2: 90
    - Year 3 and beyond: 100

Table E.3: Enrolment Projections

	Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**
First year						
Domestic	80.0	90.0	100.0	100.0	100.0	100.0
Second year						
Domestic		73.8	83.1	92.3	92.3	92.3
Third year						
Domestic			67.4	75.8	84.2	84.2
Fourth year						
Domestic				59.3	66.7	74.1
Total	**80.0**	**163.8**	**250.4**	**327.4**	**343.2**	**350.6**

F. Student Experience and Satisfaction

F.1. Student orientation, advising, and mentoring

All first year student affairs (registration and advising) are taken care of by the Faculty Academic Support Office and the team dedicated to the first year students includes:

- the First Year Curriculum Coordinator who oversees the common core courses schedule
- the Elsie McGill Learning Center Coordinator who oversees the tutoring sessions (for Math and Science courses, and ECOR courses)
- a third staff member works with the two previous positions to coordinate the academic advising.

The department undergraduate studies team comprises:

- the Associate Chair, Planning who coordinates the curriculum changes and the courses offering

- the Associate Chair, Undergraduate Studies whose portfolio includes student (from second year) advising and petitions,
- the Program Coordinator who works with both Associate Chairs for either calendar changes or advising.
- the Undergraduate Administrator who advises students on course registration and academic procedures.

Student orientation will be delivered at the Faculty level under the supervision of the Associate Dean, Student Success and at the Department level coordinated by either the Associate Chair (Undergraduate Studies) or the Program Coordinator.

As far as academic advising is concerned, the students will find assistance from the Faculty Academic Support Office while completing their first year. Either they wish to register in a reduced course load, or they wish to make some adjustments to their schedule, the staff is fully trained to assist the students navigate the challenges of the first year. From the second year and on, students will interact with the department advising team to get more specific assistance with their program and courses. In particular in fourth year, students can seek guidance when selecting their capstone project, which could be a project in SYSC 4907, supervised by a faculty member from the department or a multi-disciplinary project in ECOR 4907, involving students from at least two departments. Besides academic advising, Carleton University also offers Health and Counselling Services, to support students with their mental health and well-being.

Supporting staff interacting with students have access to training sessions about courses registration or to information sessions about available services supporting students, such as Students in Distress, procedures and offices dedicated to Health and Counselling Services. The sessions are either organized by Carleton University and destined to the general community, or by the Faculty of Engineering and Design Dean's office.

The students in the proposed new program will find a very active preexisting community to join, and will enrich it through their diverse interests, backgrounds, and through sheer numbers. The expectation is that students will form a subgroup in parallel to the existing societies in faculty of engineering and design. The assumption is that there may be a physical space, such as a lounge and labs, where students can congregate and work.

F.2. Career paths of graduates

From the Government of Canada web site, dedicated to careers in cybersecurity (https://www.cyber.gc.ca/), there is an increasing demand for expertise in computer systems security in Canada and worldwide. Major sectors of our society: finance and banking systems, government agencies and offices, healthcare systems, energy and utilities distribution systems, transportation, communications tools and media platforms, safety and emergency response systems are subject to cyber-attacks and system intrusions.

The proposed program is designed as a holistic approach to security in computer systems, with overlap with other IT disciplines (in software engineering, middleware design and development and network

technologies development and management). The program will train students to integrate security in the solution design phase and at the service deployment and management phase. Graduates will be able to select a specific cybersecurity sector or remain a generalist as cybersecurity forensic expert or consultant. Similar to the other BEng programs, graduates will be able to continue their academic path into graduate studies in Engineering.

The Government of Canada web site: https://www.cyber.gc.ca/ and the American National Initiative for Cybersecurity Careers and Studies web site: https://niccs.cisa.gov/ provide detailed career paths in cybersecurity. These include the following:

- Information system consultant
- Cybersecurity architect
- Security and vulnerability analysis
- IT security specialist
- Cyber security operations analyst
- Cyber security researcher
- Cyber security engineer
- Digital forensic analyst
- Information system security manager
- Cyber Security Manager

The program will also include the CO-OP education with a schedule that allows students

- To start an optional first work term at the end of the second year, after completing an introductory course in computer security, and project course in software development.
- To experience three or four consecutive work terms at the end of the third year, after completing the courses in computer architecture, operating systems, computer communications and two courses in security at the network layer or at the software layer.

G. Resources

G.1. Support and technical staff

The proposed program relies heavily on the hardware and laboratory equipment used in the Computer Systems and Software development courses. It will also introduce new laboratory material to train the students in techniques and software tools used in cybersecurity. The additional workload and expertise will require the hiring of an additional technician to maintain the equipment and to install and deploy the software tools.

G.2 Laboratory Equipment

The curriculum includes three courses dedicated to the Computer Systems content and which require some specific hardware components. Moreover, one second year course in Software project development relies on an equipment for its laboratory work. The total is evaluated to $39,000 (with a projected enrollment of 100 students), with an equipment renewal rate of 20%, starting Year 4.

G.3. Space

No new space will be added with the introduction of this program. Students enrolled in a Bachelor of Engineering are required to bring their own laptop to the lecture and laboratory/problem analysis sessions. Software used in courses are available for download for free and software-based laboratory work may be scheduled in regular seminar rooms or classrooms. Only courses requiring electronic equipment or computer hardware will be scheduled in a specific room within the department. It should be noted that most first and second year courses include three hours of hardware laboratory to be scheduled in a designated space. The current enrollment in engineering programs in general along with the increase number of students from this program will maximize the use of the hardware laboratories, with sessions scheduled late in the day.

G.3. Library Resources

The Library report is prepared by the librarian or subject specialist responsible for the subject area(s) covered by the program, using a common template developed from guidelines established by the Ontario Council of University Libraries. The main purpose of the report is to specify whether any new resources or services are necessary in order to support the program, for example, whether the Library needs to purchase new books or subscribe to new journals or electronic resources.

The librarians and subject specialists preparing the reports rely on their own professional experience with collecting resources in the subject areas in order to make assessments about whether there are gaps in the collection that need to be filled in order to provide the appropriate teaching and research support for new, modified, or reviewed programs. They consult various sources for information about published resources in the subject area, including the database maintained by the Library's main monographs vendor, publishers' lists and websites, handbooks and guides to the literature, the library collections of universities that offer the program, various specialized sites relevant to the subject from professional societies and organizations, as well as basic information available in tools such as Google Scholar or generally on the web. They also generally consult faculty members (e.g., the Library representative or the department chair) to discuss their assessment of the strengths and gaps. The Library makes a clear distinction between those resources which are essential to the program and those which are simply "nice to have." Generally speaking, the reports list only the essential resources, with costing obtained from the vendors or agents from which the Library would obtain the materials: each item is listed and costed individually and the total amount is recorded in the report.

The report also provides context by providing information about the following, when possible or applicable: percentage of top-ranked journals which the Library subscribes to in the subject area(s); how much funds have been spent in the past fiscal year on e-resources, journals, and printed books in support of the subjects covered by the program; how much funds have been spent in the past 8 years on printed monographs for the program; specialized collections in archives, maps, data, and government information; instruction, teaching, and practicums carried out by Library staff in the classroom or in the Library; highlights from the Library website (e.g., links for subject and course guides and to online tutorials); research partnerships between the Library and the department or program; research consultations; help desk visits; and selected detailed statistical information about the Library.

H. Development of the Self-Study

The new program in Systems Security, with a strong emphasis on communications networks was started by the Department Chair Yvan Labiche, with the preliminary technical survey conducted by a collaborator Rami Sabouni. Two main references provided the foundations of the academic program content in cybersecurity:

- https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf
- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9529234

Further discussions in defining the curriculum involved Jason Jaskolka, a faculty member from the Department before a review by the Department Academic Planning Committee. The program proposal also involved consultation with the department advisory board (https://carleton.ca/sce/advisory-board/) to get their feedback in terms of program value, and societal need for professionals in the computer security with extensive network expertise.

Additional data included in this document was obtained from the University's Office of Institutional Research and Office of the Vice-President of Research and International. This program proposal was shared in part with the COOP office and the Paul Menton Centre. Finally, the Library's report is inserted verbatim in the appendices.

Appendix 1. Proposed calendar copy – course descriptions

Year 1 Courses [5.0 credits plus three 0.0 credit engineering foundation courses) – This is a common year for all engineering programs at Carleton University. This year consists of the following courses:

MATH 1004 [0.5]
Calculus for Engineering Students
Limits. Differentiation of the elementary functions. Rules of differentiation. Inverse trigonometric functions. Applications of differentiation: max-min problems, curve sketching, approximations. Definite and indefinite integrals, techniques of integration. Applications to areas and volumes.

MATH 1104 [0.5]
Linear Algebra for Engineering Students
Systems of linear equations. Matrix algebra. Determinants. Invertible matrix theorem. Cramer's rule. Vector space R^n; subspaces, bases. Eigenvalues, diagonalization. Linear transformations, kernel, range. Complex numbers (including De Moivre's theorem). Inner product spaces and orthogonality. Applications.

CHEM 1101 [0.5]
Chemistry for Engineering Students
Topics include stoichiometry, atomic and molecular structure, thermodynamics and chemical equilibrium, acid-base chemistry, carbon dioxide in water, alkalinity, precipitation, electrochemistry, kinetics and basic organic chemistry. Laboratory components emphasize techniques and methods of basic experimental chemistry. Includes: Experiential Learning Activity

PHYS 1004 [0.5]
Introductory Electromagnetism & Wave Motion
This calculus-based course introduces potential energy, work, electricity, magnetism, oscillations and waves. Includes: Experiential Learning Activity

ECOR 1031 [0.5]
Programming and Data Management
Software development as an engineering discipline, modern programming language. Syntax and semantics. Tracing and visualizing program execution. Style and documentation. Testing and debugging. Binary number system. Container datatypes for data management. Introduction to designing and implementing numerical algorithms. Modules. Data files. Incremental, iterative development.

ECOR 1032 [0.5]
Circuits and Mechatronics
Electrical circuit fundamentals: resistance, capacitance, inductance, voltage and current sources, Ohm's law, nodal analysis, mesh analysis, source transformation, superposition. Components for mechatronics: filters, operational amplifiers, digital logic gates and combinatorial circuits, analog to digital converters, sensors, actuators, simple control schemes. Project in microcontroller-embedded mechatronic system:

ECOR 1033 [0.5]

Statics

Force vectors, Dot product. Forces components and resultants. Particle equilibrium. Moments. Cross product. 2D Truss analysis. Centre of gravity and centroids. Rigid body equilibrium. 2D Frames and machines. Internal loads at a point.

ECOR 1034 [0.5]

Dynamics

Kinematics and Kinetics of a particle. Position velocity and acceleration using cartesian path and polar coordinates. Force and Acceleration. Mechanical work and energy conservation of energy. Principle of impulse and momentum, conservation of momentum. Systems of particles. Harmonic motion. Design Project on Projectile motion.

SYSC 1006 [0.5]

Foundation of Imperative Programming

The imperative programming paradigm: assignment and state, types and variables, static and dynamic typing. Memory management and object lifetimes: static allocation, automatic allocation in activation frames, dynamic allocation. Function argument passing. Recursion. Data structures: dynamic arrays, linked lists. Encapsulation and information hiding.

Complementary Studies Elective [0.5] – This course must meet the following requirements -

(i) has 3 hours of lecture per week (can include up to 1 hour tutorial/discussion time)
(ii) deals with the "thought processes and methodologies of the arts and social sciences."
(iii) includes an evaluation of written material, such as an essay or research paper (not part of an exam)
(iv) includes a proctored final exam scheduled within the examination period.
(v) is not a "language learning" course.

Science Elective [0.5] – A 0.5 credit course from the following list of eligible courses:

BIOL 1103 - Foundations of Biology I
BIOL 1104 - Foundations of Biology II
CHEM 2302 - Analytical Chemistry I
CHEM 2800 - Foundations for Environmental Chemistry
ERTH 24XX - Climate Change (TBD)
PHYS 1001 - Foundations of Physics I
PHYS 1003 - Introductory Mechanics and Thermodynamics

ECOR 1055 [0.0]

Introduction to Engineering Disciplines I

Overview of professional activities oriented to the student's discipline of study: Architectural Conservation and Sustainability. Civil and Environmental. Aerospace and Mechanical. Electrical. Engineering Physics. Computer Systems, Communications and Software. Biomedical (Electrical and Mechanical). Sustainable and Renewable Energy. Graded SAT/UNS.

ECOR 1056 [0.0]

Introduction to Engineering Disciplines II

Selected lectures designed to provide students with exposure to the breadth of Engineering disciplines. Graded SAT/UNS.

ECOR 1057 [0.0]

Engineering Profession

Professional Engineers Act. Engineering documentation. History of the profession. Engineering practice: system life cycle, practice within the discipline, designing with others. Health and safety. Engineering Ethics, Equity and Diversity. Introduction to engineering law: Business, Entrepreneurship and Intellectual Property. Graded SAT/UNS.

Year 2 Courses [5.0 credits] – It consists of the following courses:

COMP 1805 [0.5]

Discrete Structures I

Introduction to discrete mathematics and discrete structures. Topics include: propositional logic, predicate calculus, set theory, complexity of algorithms, mathematical reasoning and proof techniques, recurrences, induction, finite automata and graph theory. Material is illustrated through examples from computing.

.

MATH 1005 [0.5]

Differential Equations & Infinite Series for Eng. Students

First-order differential equations. Second-order linear equations with constant coefficients, undetermined coefficients, variation of parameters. Sequences and series, convergence tests, estimation of sums. Power series, Taylor series, remainders. Fourier series.

SYSC 2004 [0.5]

Object-Oriented Software Development

Designing and implementing small-scale programs as communities of collaborating objects, using a dynamically-typed or statically-typed programming language. Fundamental concepts: classes, objects, encapsulation, information hiding, inheritance, polymorphism. Iterative, incremental development and test-driven development.

SYSC 2010 [0.5]

Programming Project

Programming, testing, and debugging of small team-based software projects that use data from sensors to display results graphically. Modern programming tools: frameworks, libraries, version control, package management, tool chains. Sensors, signal acquisition, display, and basic filtering. Introductory network programming.

SYSC 2100 [0.5]

Algorithms and Data Structures

Thorough coverage of fundamental abstract collections: stacks, queues, lists, priority queues, dictionaries, sets, graphs. Data structures: review of arrays and linked lists; trees, heaps, hash tables. Specification, design, implementation of collections, complexity analysis of operations. Sorting algorithms.

SYSC 2310 [0.5]

Introduction to Digital Systems

Number systems: binary, decimal, hexadecimal. Digital representation of information. Computer arithmetic: integer, floating point, fixed point. Boolean logic, realization as basic digital circuits. Applications: simple memory circuits, synchronous sequential circuits for computer systems. Finite state machines, state graphs, counters, adders. Asynchronous sequential circuits. Races.

SYSC 2320 [0.5]

Introduction to Computer Organization and Architecture

Computer organization: processor, memory, input/output, system bus. Microarchitecture. Instruction set architecture. Assembly language programming: addressing modes, instruction encoding, execution. Assembler. Simple digital I/O, programmable timer. Input/output methods: polling, hardware interrupts.

SYSC 2510 [0.5]

Probability, Statistics and Random Processes for Engineers

Discrete and continuous random variables. Joint and conditional probabilities, independence, sums of random variables. Expectation, moments, laws of large numbers. Introduction to statistics. Stochastic processes, stationarity, additive white Gaussian noise, Poisson processes. Markov processes, transition probabilities and rates, birth death processes, introduction to queueing theory.

SYSC 2xxx [0.5]

Introduction to Cybersecurity

Analysis of cybersecurity case studies. Security concepts. Introduction to security models and policies. Risks analysis and threats modelling. Discussions onlegal and ethical issues.

Complementary Studies Elective [0.5] – This course must meet the following requirements -

(vi) has 3 hours of lecture per week (can include up to 1 hour tutorial/discussion time)
(vii) deals with the “thought processes and methodologies of the arts and social sciences.”
(viii) includes an evaluation of written material, such as an essay or research paper (not part of an exam)
(ix) includes a proctored final exam scheduled within the examination period.

is not a “language learning” course.

Year 3 Courses [5.0 credits plus one 0.0 credit in engineering portfolio] – It consists of the following courses:

CCDP 2100 [0.5]

Communication Skills for Engineering Students

Development of competence in professional written and oral communication in engineering. Focus on written documents (proposals, technical explanations, research reports, summaries) and oral presentations. Attendance is mandatory.

ECOR 2050 [0.5]

Design and Analysis of Engineering Experiments

Statistics and the design of engineering experiments. Basic exploratory data analysis. Central limit theorem. Hypothesis testing: t-test, chi-square test, type-I and type-II errors, multiple-comparison problem. Statistical bias. Design of experiments: randomization, blocking and replication, randomized blocking designs, factorial design. Statistical software packages. Includes: Experiential Learning Activity

ECOR 2995 [0.0]

Engineering Portfolio

Students will be asked to reflect on their skills, strengths, and weaknesses as preparation for the professional practice course. Engineering students must submit samples of their writing and communications (including, for example, laboratory reports and professional memos).

ECOR 3800 [0.5]

Engineering Economics

Introduction to engineering economics; cash flow calculations; methods of comparison of alternatives; structural analysis; replacement analysis; public projects; depreciation and income tax; effects of inflation; sensitivity analysis; break-even analysis; decision making under risk and uncertainty.

SYSC 3310 [0.5]

Real Time Systems

Principles of event-driven systems. Microcontroller organization. Development of embedded applications. Programming external interfaces, programmable timer. Input/output methods: polling, interrupts. Real-time issues: concurrency, mutual exclusion, buffering. Introduction to concurrent processes.

SYSC 3512 [0.5]

Computer Communications

Layered network architectures, TCP/IP suite, circuit switching, packet switching. Physical media, data transmission, multiplexing. Data link controls, MAC protocols, random access, polling, IEEE 802 standards. Bridges, switched Ethernet, VLANs. Routing algorithms, Internet routing protocols, datagram networks, virtual circuit networks. Transport protocols.

SYSC 3523 [0.5]

Introduction to Distributed Applications

Application layer protocols, APIs and socket programming. Client-Server architecture. WWW architecture. Peer-to-Peer architecture. Fault tolerance. Introduction to database and SQL

SYSC 3821 [0.5]

Data Security and Cryptography Source coding. Error control coding. Data format and conversion techniques. Coding for secure communications. Introduction to cryptography. Data center

SYSC 3822 [0.5]

Network Security I Presentation of network vulnerabilities and threats throughout the OSI layers 1 to 4. Secure network protocols. Internet Security Protocols and

Authentication. Firewalls. Intrusion Detection Systems

SYSC 4001 [0.5]

Operating Systems

Introduction to operating system principles. Processes and threads. CPU scheduling. Managing concurrency: mutual exclusion and synchronization, deadlock and starvation. Managing memory and input/output. Concurrent programming, including interprocess communication in distributed systems.

Science Elective [0.5] – A 0.5 credit course from the list of eligible courses.

Year 4 Courses [6.0 credits] – It consists of the following courses:

ECOR 4995 [0.5]

Professional Practice

Presentations by faculty and external lecturers on the Professional Engineers Act, professional ethics and responsibilities, practice within the discipline and its relationship with other disciplines and to society, health and safety, environmental stewardship, principles and practice of sustainable development. Communication skills are emphasized.

Engineering Design Project [1.0] - 1.0 credit in ECOR 4907 or SYSC 4907

During the final year capstone project - Student teams develop professional-level experience by applying previously acquired knowledge to a major design project. A project proposal, interim report, oral presentations, and a comprehensive final report are required.

SYSC 4831 [0.5]

Software Security

Presentation of systems vulnerabilities and preventive solutions throughout the OSI layers 5 to 7. Topics include: Malicious code and code injection.

Viruses. Zero-day attack. Vulnerability analysis and testing. Cryptographic APIs. Development, Security, Operations (DevSecOps)

SYSC 4832 [0.5]

Network Security II Wireless and mobile networks. Cellular systems 1G to 5G. Physical layer security. Attacks on wireless networks. Wireless intrusion detection systems.

Security in the GSM. Bluetooth security

SYSC 4821 [0.5]

Security in Emerging Technologies Data and applications security in the cloud environment. Wireless sensor networks security. Introduction to IoT security. Blockchain

SYSC 4822 [0.5]

Network Security Development Project

Use of modern applications for network monitoring and attack simulations. Standardization and security criteria. Security assessment. Virtualization technology and Security. Network design process to security requirements Network monitoring. Introduction to network forensics.

Engineering Elective Course [2.0] - SYSC at 4000 level (may include 1.0 credit in SYSC 5000 level)

Complementary Studies Elective Course [0.5]

Carleton University | MacOdrum Library

Institutional Quality Assurance Process

Library Report for BEng, Systems Security Engineering

New Program

Date: September 27, 2024

Compiled by: George Duimovich, Collections Librarian, Science, Engineering & Design Team

Submitted to: Angel Wagner, Academic Program Specialist,
Office of Academic Programs & Strategic Initiatives

cc Amber Lannon, University Librarian
Sarah Simpkin, Associate University Librarian, Academic Services
Alana Skwarok, A/Head of Collections & Assessment
Sally Sax, Head of Electronic Resources & Acquisitions
Joel Rivard, Head of Research Support Services

1. OVERVIEW AND RECOMMENDATIONS

An analysis of Carleton University Library's information resources and services in support of the program demonstrates that the Library does not require additional funds to support it.

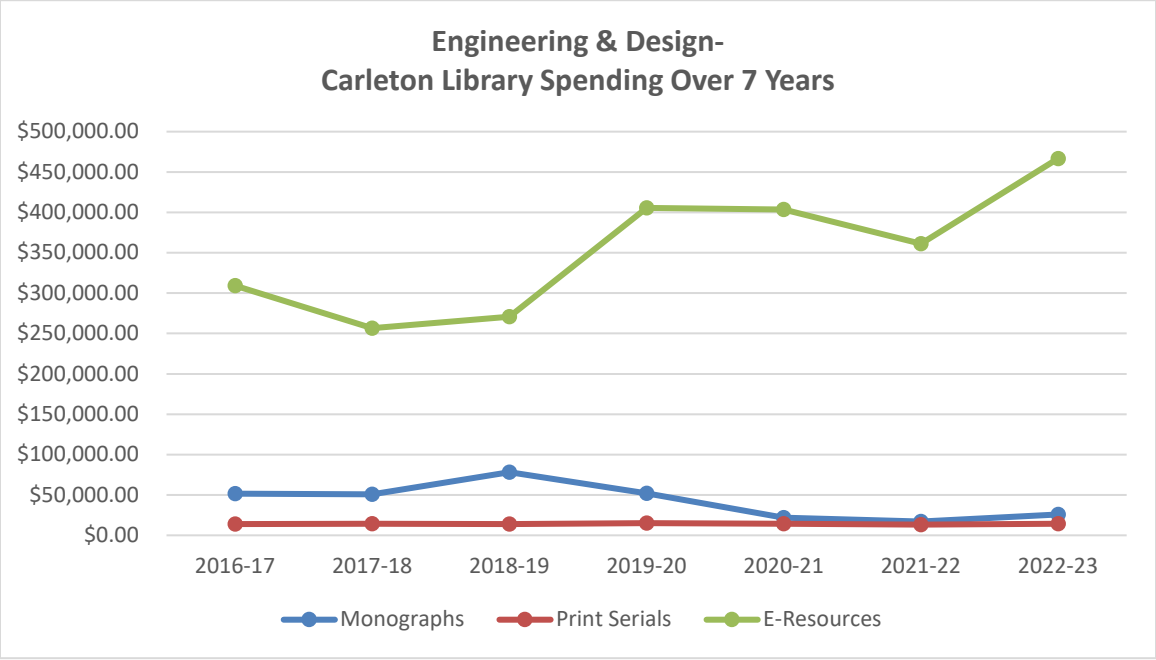
2. LIBRARY COLLECTIONS

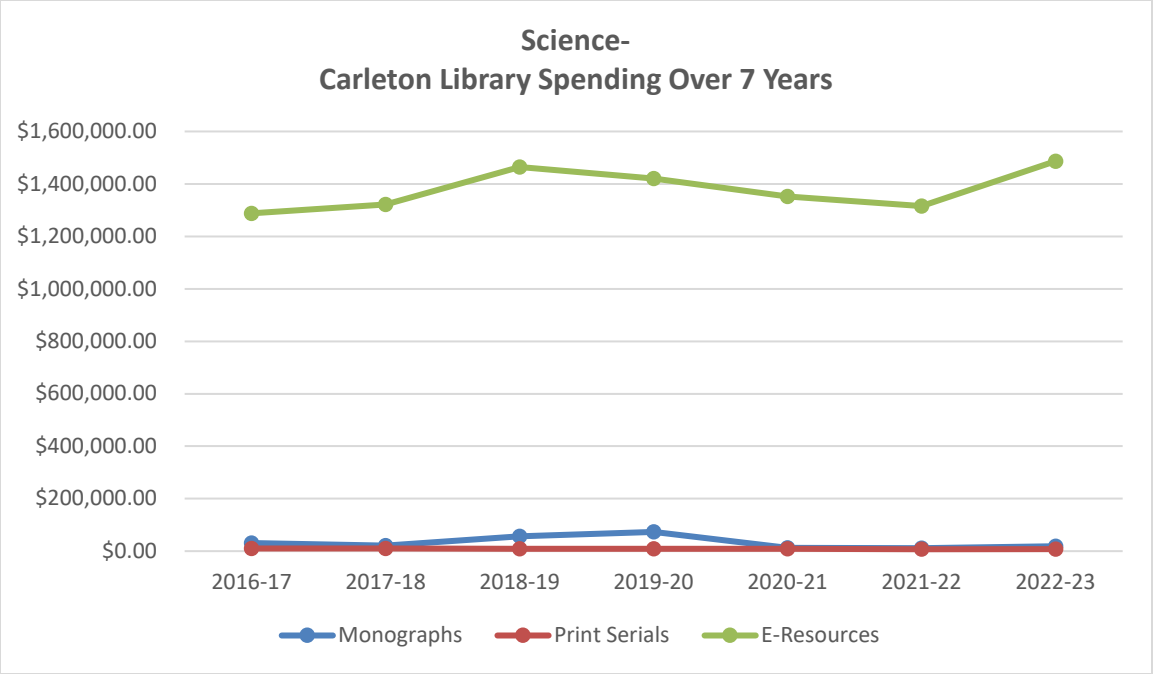
Subject Specific

The Library's collection includes specific resources to support *Systems Security Engineering.* These include 25 of the top-ranked 25 journals in *Journal Citation Reports* classified under the subject categories: *Computer Science*, *Software Engineering* as well as 20 of top 20 journals ranked in *Google Scholar* citations for *computer / information security*. In addition, the Library's collections of journals in related programs are also strong in Computer Science (theory and methods) as well as Software Engineering, Information Technology, and Mathematics & Statistics.

During the 2022-23 academic year, the Library's spending for collection in all areas was about $8.7 million. 88% of the entire collections budget is spent on electronic resources**.** Over $3.1 million was spent on general electronic resources which benefit all subject areas.

In addition to that amount, the following shows the amounts spent on electronic resources (databases, journals, ebook packages, indexes), print journals, and monographs (individual orders) related to *Faculty of Science* and *Faculty of Engineering & Design* for the past seven years***:***





The policy for materials that the Library collects for *Computer System Security Engineering* may be found at:

- Collection Profile: Systems & Computer Engineering
- Collection Profile: Computer Science

3. TEACHING, LEARNING, AND RESEARCH

Carleton Library is a vibrant and active partner in teaching, learning, and research across all disciplines of the university. Library staff take pride in supporting students to develop the skills required to locate, evaluate, use, and communicate information effectively and responsibly. Our programs and services are grounded in Ontario's Quality Assurance Framework.

The Librarian works collaboratively with faculty to address students' information competencies in several ways, including:

Instruction, Teaching, and Practicums

A total of 469 in-class instruction sessions were provided by Library staff in all subject areas during 2022-23, and a total of 12,542 students attended those sessions. These sessions were also supplemented by the creation of over 200 videos with over 31.000 total views. The *Librarian* designs and delivers instruction sessions and practicum opportunities to meet the needs of specific assignments and course requirements while addressing broad learning objectives.

Online Learning Support

The Library website (library.carleton.ca) guides students through each step of the research process: identifying, accessing, borrowing, evaluating, and citing resources. Google Analytics recorded almost 1 million visits to the Library website during 2022-23. Library users can conduct a comprehensive search of the entire collection using the Omni search interface. Recent

enhancements to Omni allow Carleton users to easily request items from university libraries across Canada, the United States, and other countries.

Highlights of the Library website include:

- Subject Guides for Computer Science & Systems and Computer Engineering
- Leading technical, scientific and engineering databases including: ACM Digital Library, Engineering Village, IEEE Xplore Digital Library, IET Digital Library, Web of Science Core Collection, and O'Reilly for Higher Education

Research Partnerships

Active research is the foundation of a strong academic program, and an increasingly important part of student learning and development. The Library provides resources, services, and expertise to facilitate the Carleton research community at all levels and through all stages of the research process. This research support is provided at key service points, and through individual consultations and more formal collaborations.

4. SERVICES

Individual Research Consultations

Library staff provided 2274 individual research consultations across all faculties in 2022-23. Consultations can be scheduled for discipline-based research support, as well as support for numeric and geospatial data, research data management, open access publishing, evidence synthesis, copyright, knowledge mobilization, and many related topics.

Research Help – Desks & Chat

Onsite research help is provided through two service points: a Research Help desk on the main floor of the Library and a help desk in Archives and Special Collections (ASC). These two service points had a total of 2685 visits in 2022-23. This service is supplemented by an extended online Ask a Librarian Chat service. A total of 1860 Carleton patron questions were answered via Ask a Librarian in 2022-23.

Results from recent user surveys show that the Library performs well in providing off-campus access to resources and services, and that these resources help people to be successful at university. It was noted that help is available from Library staff when needed. The Library also does well at providing accurate answers to questions and providing course reserves that help both faculty and students.

5. GENERAL INFORMATION ABOUT THE LIBRARY

Carleton Library consists of five stories, totaling over 214 thousand square feet. Two floors are dedicated to silent study, while three others allow for quiet conversation. As of the Fall of 2019, the Library had a total of 2400 seats for students. This included 179 public computers and 41 bookable group study rooms. User surveys show the need for more group and silent spaces with outlets for power, and so renovations throughout the Library in the past few years continue to focus on new study space for students.

Thanks to $1 million in funding from the Government of Ontario's Training Equipment and Renewal Fund and a matching contribution from the university, the fourth floor of Carleton Library has been transformed into a newly designed space called the Future Learning Lab. This multi-purpose space can be adapted to suit a wide range of needs. It is envisioned as both a physical space and a set of programs designed to foster innovation and incentivize student-centred ways of teaching.

The New Sun Joy Maclaren Adaptive Technology Centre (JMC) provides students access to assistive technologies and accessible individual and group study rooms. Rooms are equipped with a variety of adjustable furniture, desks, and assistive technologies and hardware.

The Library's collection includes approximately 1.2 million print monographs, 2.8 million e-books, and over 277,000 e-journals in a wide range of subjects and disciplines. In addition, the Library has substantial collections of government documents and other resources, maps, data, rare books and other special research collections, printed journals, archives, theses, multimedia resources (audio, DVD, streaming video), musical scores, as well as licensed access to full-text and indexing databases in a broad range of subjects.

Members of the Library's Collections & Assessment Department build and maintain the Library's collection by developing collection policies that guide the systematic selection of materials. The Library welcomes purchase suggestions from members of the Carleton community. A purchase suggestion form is available on the Library's website to gather suggestions.

In order to enhance its purchasing power (particularly for electronic resources), the Library is an active member of two major cooperative partnerships: the Ontario Council of University Libraries (OCUL), a consortium of the 21 academic libraries in the province; and the Canadian Research Knowledge Network (CRKN), a consortium of 75 academic libraries across the country. Carleton Library is also a member of HathiTrust, a not-for-profit collaborative of academic and research libraries which gives students, staff, and faculty access to a digital repository of millions of books, serials, and other materials from research institutions and libraries from around the world.

The Library's annual acquisitions budget for the 2023-24 fiscal year is $8.6 million, and its staffing and operating budget is $14.4 million.

The Library acquisitions budget is not protected from inflation, exchange rates, or cuts, which often challenges the Library's ability to provide all the necessary resources in support of teaching, learning, and research at Carleton. Consideration of the funds necessary for the Library's acquisitions budget is part of the academic planning and Quality Assurance processes for new programs. The Library is dedicated to regular assessment of its resources and services. Staff use an assortment of qualitative and quantitative techniques to evaluate collections and services in order to make sound decisions within budget parameters.

The Library strongly supports the principles and practices of open access (OA). The University's institutional repository was established in 2011 and is maintained by the Library. It includes a growing archive of the broad intellectual output of the University, as well as digitized versions of most of the theses accepted at Carleton since 1955. The Library contributes to CURIE, the University's program to provide funding for faculty and researchers who are publishing in open access journals, and has also entered into a number of agreements with publishers that offer no-charge open access publishing or discounts. The Library's journal hosting service allows

Carleton-affiliated scholars to publish open access journals as a means of increasing availability of scholarly research and writing, as well as to increase involvement in disciplinary discourse. For more information about the Library's support for open access and research dissemination, please see our website.

AT A GLANCE: CARLETON UNIVERSITY LIBRARY

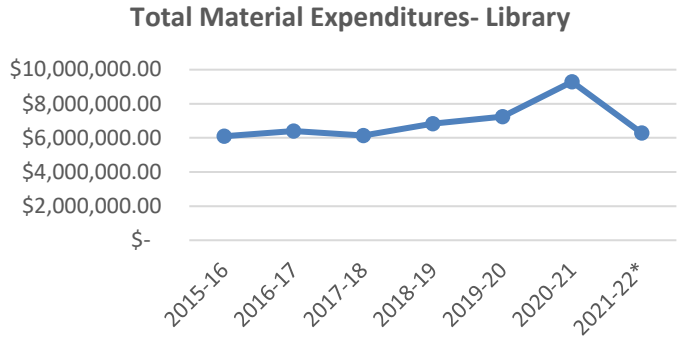
Statistics as of May 1, 2023 except where indicated. Labour disruption, new system implementation & effects of the pandemic** including an entire year online *** has affected some numbers*

Research Highlights

- Carleton's Institutional Repository
- Open Access- Funding for Faculty, Staff, & Students; Open Access Awards for Graduate Students
- Research Data Management Training
- Professional Skills Training for Graduate Students

Collection Spending:

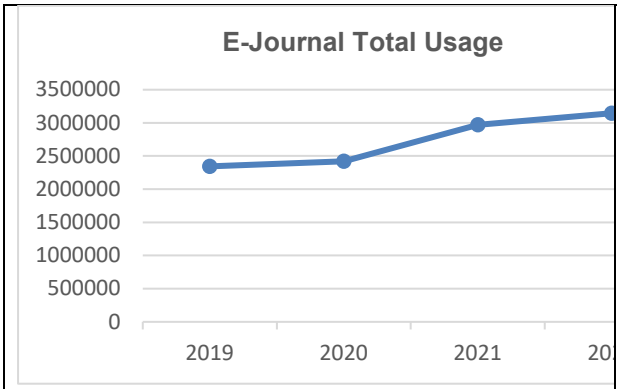
- $8.7 million; 88% of the entire collections budget spent on electronic resources
- $3.1 million spent on general electronic resources which benefit all subject areas

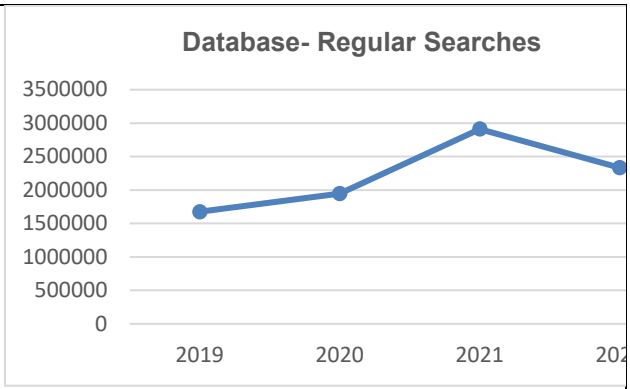


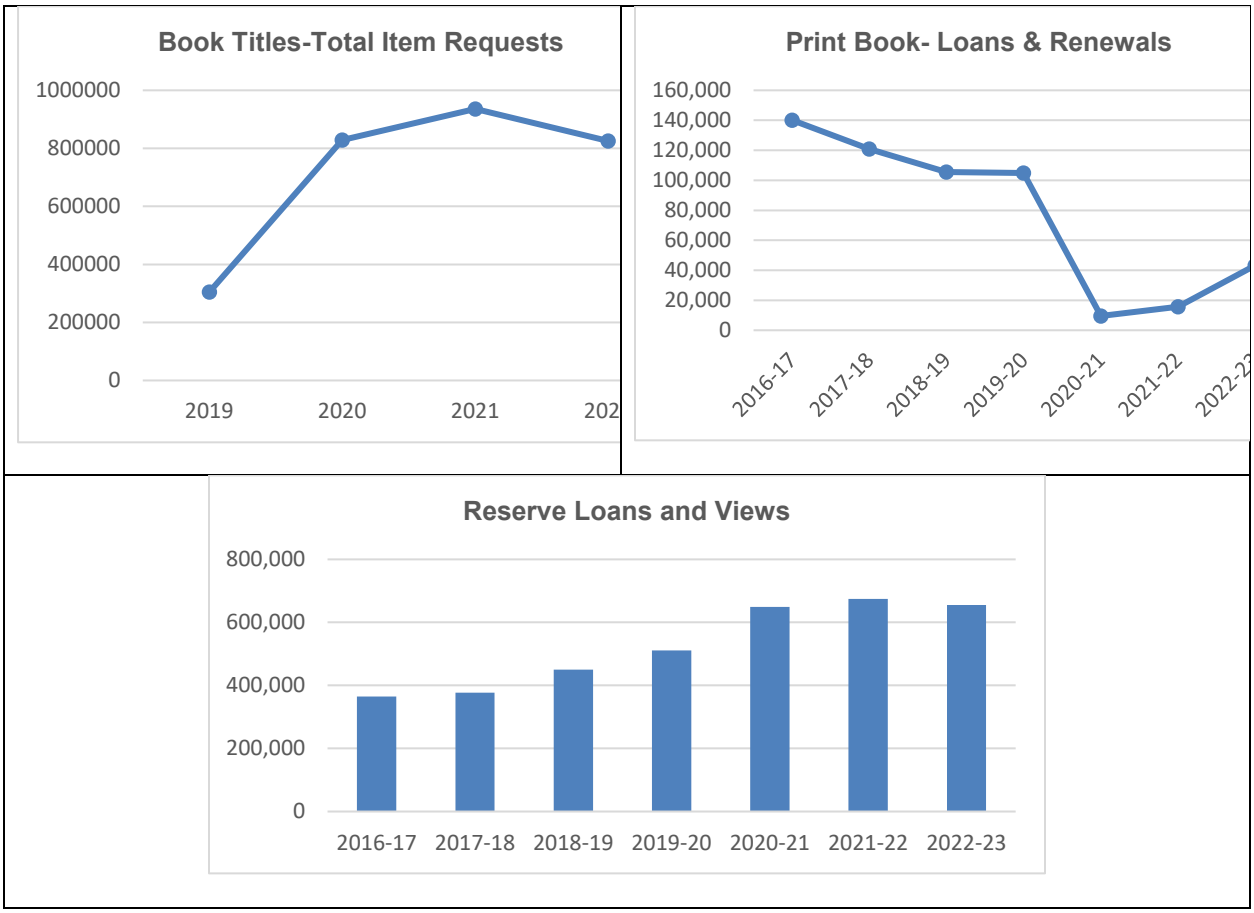
**2020-21- purchased a lot of one-time material to support the switch to online learning which did not have to be paid for again. Annual cost increases for subscriptions were lower than usual due to ongoing pandemic, & a favourable exchange rate lowered our overall spend as most of our invoices are paid in USD.*

Collections- Usage

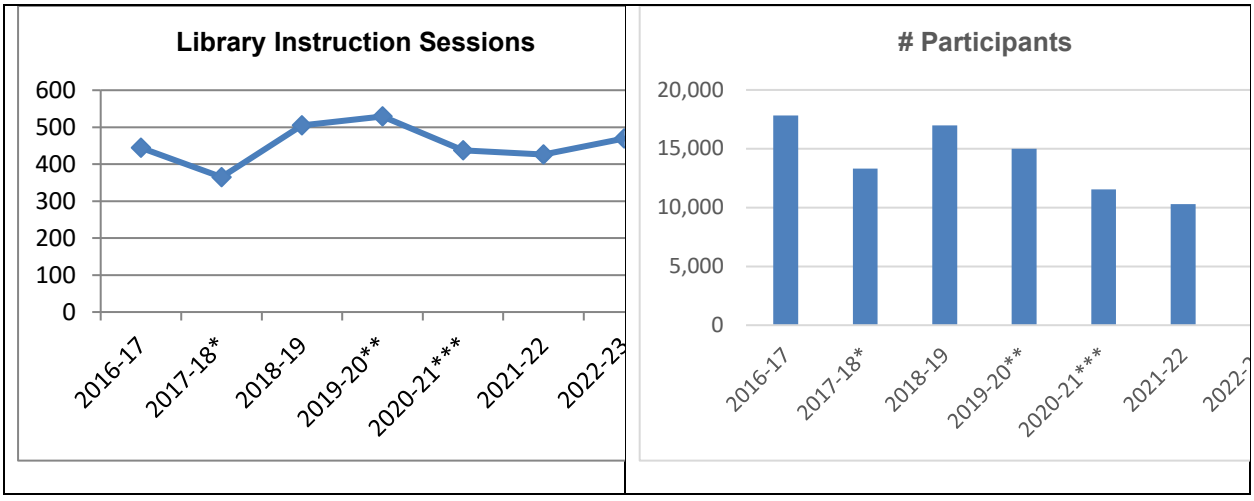
COUNTER 5-compliant data from a selection of major e-publishers/vendors (2019 onward only)

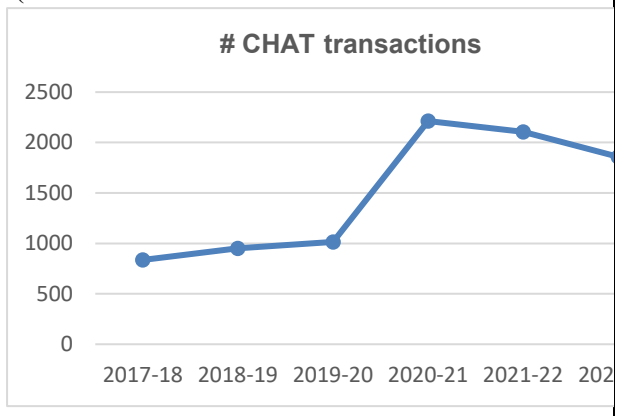






Teaching & Learning





Highlights for 2022-23:

- 469 instruction sessions; 12,542 students attending
- 2274 individual research consultations in 2022-23 for all faculties
- 2685 research help questions answered on site
- 1860 Carleton patron questions answered (CHAT)
- Over 200 instruction videos created with over 31,000 total views

Space

Almost 1 million visits to Library website in a year
Future Learning Lab
Adaptive Technology Centre
Innovative Study areas
Group & graduate study rooms
Book Arts Lab, an experiential learning space

Discussant Report

New Program Review

Name: Hashmat Khan

November 28, 2025

Program being reviewed

Bachelor of Engineering - Systems Security Engineering

Review of self-study (Volume I)

The self-study is well-written and provides a good description of the new Bachelor of Engineering (System Security Engineering) program in the Faculty of Engineering & Design. The BEng is intended to deliver advanced and in-depth knowledge in the field of systems security at the undergraduate level. The Program Learning Outcomes (PLOs) are clearly mapped to Degree Level Expectations (DLEs), with a well-laid-out program curriculum map and an LO assessment rubric in terms of Exam, Lab, Assignment, or Project Report.

Review of External Reviewers' Report

Overall, the External Reviewers' Report is quite positive and views the proposed program as innovative and timely. They note that there is an urgent need to have well-trained graduates as there is a significant shortage in this area. They are happy with the program structure and the PLOs, and in their view it aligns with the requirements of the Canadian Engineering Accreditation Board. They note that since the new courses in the program will be introduced in the third and fourth years, some fine-tuning may be necessary. The reviewers are satisfied with the proposed assessment methods to gauge competencies, progress, readiness for professional practice, and of teaching and learning. In their view, these are appropriate, judicious, rigorous, and comprehensive.

The reviewers have made seven clear recommendations following their assessment of the program, with five categorized as 'opportunities (O)', one as a 'weakness (W)', and one as a 'concern (C)'.

Review of Unit Response and Implementation Plan

Unit Response and Implementation Plan: Summary of Recommendations

The unit response to the recommendations is favourable. It provides clear action items in terms of curriculum improvements down the road and monitoring of enrolment and resource requirements.

Table 1: Recommendations Summary

Rec.		About	Agreed to
#1	W	Sub-areas within cybersecurity (e.g. Operational Technology)	In principle
#2	O	Course on cryptography/cryptanalysis	Unconditionally
#3	O	Cybersecurity concepts	Unconditionally
#4	C	Lab and infrastructure support	Unconditionally
#5	O	Hiring new faculty members	If resources permit
#6	O	Co-op opportunities	Unconditionally
#7	O	Resources if enrolment booms	Unconditionally

DISCUSSANT'S CONCERN:

I do not have any concerns.

DISCUSSANT RECOMMENDATION:

Recommendation of program categorization

Recommended to commence.

Carleton University Site Visit
New Undergraduate Program in Systems Security Engineering
Date: February 3, 2025

External Reviewers: Dr. Ali Dehghantanha, University of Guelph
Dr. Mourad Debbabi, Concordia University

Internal Reviewer: Dr. Masoud Barati, School of Information Technology Carleton University

Time	February 3, 2025	Location
8:45 – 9:00	Meeting with Dr. Hashmat Khan, Associate Vice-President (Academic Programs and Strategic Initiatives)	DT303
9:15 – 10:00	Meeting with Dr. Yvan Labiche, Chair, Department of Systems and Computer Engineering	ME 4359 Dept. meeting room
10:00 –10:30	Department Tour with Dr. Yvan Labiche, Department Chair, Patrick Fairs, Technical Support Services Supervisor Brad Hunter, Teaching Laboratory Technician	
10:45-11:15	Meeting with Departmental Staff: June Creighton Payne, Departmental Administrator, Gift Osarenkhoe, Undergraduate Administrator, Jenese Nugent, Financial and Communications Assistant	ME 4359 Dept. meeting room
11:30 – 1:00	Lunch meeting with External and Internal Reviewers, Faculty members: Jaskolka, Jason Lung, Chung-Horng Marshall, Lynn Marsland, Ian Gohary, Ramy Gomar, Shaghayeg Taha, Mostafa Talim, Jerome	ME 4463 Maker's lab
1:15 -1:45	Meeting with Dr. Larry Kostiuk, Dean, Faculty of Engineering and Design	MC 3010
2:00 – 2:30	Dr. David Hornsby, Vice-Provost and Associate Vice-President (Academic)	DT 405A
2:35 – 3:30	External Reviewers Report Preparation Meeting	DT303
3:30– 4:00	Closing Meeting with Dr. Hashmat Khan, Associate Vice-President (Academic Programs and Strategic Initiatives)	DT303

Please note: The meeting time slots includes travel time between offices and breaks.

External Reviewers' Biographies

New Undergraduate Program in Systems Security Engineering

Dr. Ali Dehghantanha is a Professor of Cybersecurity and Threat Intelligence at the **University of Guelph**, ON, Canada. As a distinguished academic-entrepreneur, he marries deep technical prowess with visionary insights, making him a compelling figure for those steeped in the tech universe of cybersecurity. Recipient of the esteemed IEEE Outstanding Leadership Award in 2021, Dr. Dehghantanha's leadership is indisputable. His distinction as the Canada Research Chair in Cybersecurity and Threat Intelligence since 2020 underscores his exceptional influence. As the founding director of two prestigious master's programs at the University of Guelph in Ontario, Canada, he introduced the "Master of Cybersecurity and Threat Intelligence" and, subsequently, the "Master of Cybersecurity Leadership and Cyberpreneurship" program. His prolific research echoes in his extensive body of work, encompassing 4 influential books, 2 US Patents, over 80 impactful Journal papers, and over 20 influential conference papers. With more than 19,000 citations, Dr. Dehghantanha's contributions are a wellspring of knowledge shaping the evolution of the cybersecurity landscape.

Dr. Mourad Debbabi is the Dean of the Gina Cody School of Engineering and Computer Science at **Concordia University** and a Full Professor at the Concordia Institute for Information Systems Engineering. He holds the Hydro-Quebec Hitachi Partnership Research Chair in Smart Grid Security with support from NSERC and PROMPT and the Government of Quebec Research Chair on the security of public administration networks. He is a founding member of the National Cybersecurity Consortium (NCC) that leads Canada's Cybersecurity Innovation Network (CSIN) program. He served on the expert committee of the Ministry of Cybersecurity and Digital Technology of the Quebec Government. He serves/served on the boards of the Canadian Police College, PROMPT Québec, Cybereco, and Calcul Québec. He served as a member of CATAAlliance's Cybercrime Advisory Council. He is the founder and the Director of the Security Research Centre of Concordia University. Dr. Debbabi holds Ph.D. and DEA degrees in computer science from Paris-XI Orsay University, France, and a B.Eng. from Université de Constantine, Algeria. He published seven books and more than 300 peer-reviewed research articles in international journals and conferences on cybersecurity, cyber forensics, smart grid security, vulnerability research, cyber threat intelligence, malware analysis, reverse engineering, privacy, cryptographic protocols, specification, and verification of safety-critical systems, programming languages, and type theory. He supervised the successful completion of 35 Ph.D. theses, 76 Master's theses, and 15 Postdoctoral Fellows. He served as a Senior Scientist at the Panasonic Information and Network Technologies Laboratory, Princeton, New Jersey, USA; Associate Professor at the Computer Science Department of Laval University, Canada; Senior Scientist at General Electric Research Centre, New York, USA; Research Associate at the Computer Science Department of Stanford University, California, USA; and Permanent Researcher at the Bull Corporate Research Centre, Paris, France.

Carleton University | Office of the Vice-Provost and Associate Vice-President (Academic)

External Reviewer Report Template – New Programs

The external reviewer's joint report serves to inform the Senate Quality Assurance and Planning Committee and Carleton University Senate. This joint report can be brief on those criteria that reviewers feel are being met successfully and focus on 1) criteria that give rise to issues and on recommendations for the program and on 2) significant strengths, including any clearly innovative and creative aspects of the program. In the sections below you will find bullets, taken directly from the New Program Review Terms of Reference and Carleton University IQAP, these are items to consider and can be used as a guide but are not individual questions requiring specific responses. At the end of the document, we ask that you summarize your overall recommendations for the program.

Please note that the Internal Reviewer does not have a role in the writing of this joint report and that this document will be made public, we would ask that you please refrain from using specific names or identifiers as all comments are to be held anonymous on the report.

Recommendations

The most important part of the report from the point of view of the university will be the recommendations made for program improvement (a minimum of 3 are required). We therefore request that all recommendations be clearly listed under 3 main categories:

- **Weakness:** Remedial action is recommended to strengthen compliance with program quality standards.
- **Concern:** Potential risk to future quality that should be considered.
- **Opportunity:** Recommendation for future enhancements

Program(s) being reviewed:	Systems Security Engineering
Date of review:	February 3rd 2025
Names and Emails of External Reviewers:	Mourad Debbabi (Mourad.Debbabi@concordia.ca) Ali Deghantanha (adehghan@uoguelph.ca)
Date of Report:	February 8th, 2025

Considerations for New Program Approval
Note: this document list criteria for both undergraduate and graduate programs, depending on the type of review being conducted not all will need to be considered

Program Objectives

- Clarity of the program's objectives
- Appropriateness of degree nomenclature given the program's objectives
- Consistency of the program's objective with the institution's mission and academic plans

The proposed program aims to educate future professionals with expertise in systems cybersecurity while also equipping them with strong skills in communication systems, security assessment, and cybersecurity risk management. Graduates will acquire the essential technical and analytical abilities needed to safeguard network and system components from emerging threats. They will develop in-depth knowledge of networking technologies, as well as mobile and cloud computing systems, to navigate the evolving digital landscape effectively. The program will offer advanced technical insights into network protocol threats, secure design principles, and effective defense mechanisms to strengthen system security. Emphasizing a hands-on approach, the curriculum will integrate government standards, industry best practices, and legal considerations in cybersecurity. Additionally, students will be trained in cybersecurity risk modeling and impact assessment to ensure informed decision-making.

This program is well-aligned with Carleton University's mission by fostering interdisciplinary education and research while addressing the growing need for cybersecurity professionals. The emphasis on hands-on learning, adherence to government standards, and integration of industry best practices reflects the university's commitment to experiential learning and community betterment. By preparing graduates to tackle modern cybersecurity challenges and enhance the resilience of digital infrastructures, the program contributes to Carleton's vision of fostering innovation and developing future leaders to create a more sustainable and prosperous future for Canada and the world.

Furthermore, the program is particularly timely, addressing the significant shortage of cybersecurity professionals in Canada. According to ISC2, the country faces an estimated shortfall of 26,000 cybersecurity experts, highlighting the urgent need for well-trained graduates in this critical field.

Program Requirements

- Appropriateness of the program's structure and requirements to meet its objects and program-level learning outcomes

The curriculum takes a holistic approach to computer system security by linking cybersecurity to both network and system components and protocols. Advanced coursework and electives will cover emerging technologies such as Software Defined Networks, cloud environments, and security applications.

In the first years, the program provides students with core engineering courses that are shared with other engineering programs. In the upper years, the program proposes a distribution of 8 credits as follows: 1.5 credits in Software Development, 2.0 credits in Computer Systems Engineering with a focus on computer architecture and operating systems, 1.5 credits in Communication Engineering, 1.5 credits in Systems Security, and 1.5 credits in Cybersecurity Standards, Ethics, and Practice. These courses have significantly

broadened my knowledge and skills across various critical areas in the field of engineering and cybersecurity.

The program is set to introduce seven new core courses focusing on systems security and cybersecurity standards, ethics, and practice. Additionally, the department will offer new elective courses covering advanced topics such as autonomous vehicles, the Internet of Things, cryptography, and security. applications for critical infrastructures like hydroelectric systems, air traffic control, traffic management, telecommunications, and healthcare. These courses will also be relevant and beneficial to other IT programs.

The program's structure, requirements, and program-level learning outcomes are meticulously crafted to meet Carleton University's undergraduate degree level expectations. Students are introduced to cybersecurity as early as Year 2, with an increasing number of courses dedicated to this critical field in the following years.

- Appropriateness of the proposed mode(s) of delivery to facilitate students' successful completion of the program-level learning outcomes Ways in which the curriculum addresses the current state of the discipline or area of study

The proposed program's curriculum will leverage existing introductory and advanced courses, seamlessly integrating their content from accredited programs. Additionally, the department is exploring online synchronous delivery for select upper-year courses. This strategic approach, coupled with a well-structured course schedule, is expected to attract a new demographic—particularly professionals looking to upskill in systems security.

- Identification of any unique curriculum or program innovations or creative components, or significant high impact practices

The proposed program is innovative as it emphasizes critical areas in modern cybersecurity. With a focus on cloud and mobile security, it addresses the rapidly evolving threat landscape in these domains. Experiential learning is central to the curriculum, ensuring that students gain hands-on experience through real-world projects, simulations, and industry collaborations. Furthermore, the program is uniquely engineered to develop security solutions from a technical and systems-driven perspective, equipping graduates with the skills to design, implement, and manage robust cybersecurity frameworks.

- Do the program's intellectual profile and learning outcomes match the teaching and research strengths of the academic unit(s)?

The proposed program leverages the faculty's deep expertise in communications, advanced networks, and cybersecurity, ensuring that they bring a wealth of knowledge and industry insights into the classroom.

Assessment of Teaching and Learning

- Appropriateness of the methods for assessing student achievement of the program-level learning outcomes and degree level expectations
- Appropriateness of the plans to monitor and assess:
    i. The overall quality of the program;

ii. Whether the program is achieving in practice its proposed objectives;
iii. Whether its students are achieving the program-level learning outcomes; and
iv. How the resulting information will be documented and subsequently used to inform continuous program improvement

The development of learning outcomes is guided by graduate attributes to ensure alignment with the requirements of the Canadian Engineering Accreditation Board. This approach also entails the implementation of a continuous improvement process, which includes evaluating course organization and engagement, curriculum mapping, assessment tools and results, as well as the overall improvement strategy and corresponding actions. The proposed assessment framework follows the same rigorous process used for other engineering programs. Since the proposed program introduces new courses primarily in the third and fourth years, the department proposes to conduct a comprehensive review of academic content, delivery methods, and assessment outcomes at the end of each year. This ongoing evaluation will facilitate necessary curriculum adjustments, ensuring the program's quality and effectiveness.

The proposed assessment methods for evaluating student achievement of program-level outcomes are both appropriate and judicious, ensuring a rigorous and comprehensive evaluation of learning. By aligning with established accreditation standards and leveraging proven assessment tools, the approach effectively measures students' competencies, progress, and readiness for professional practice.

- Is there a clear indication of essential requirements?

The proposed program aligns with the Ontario Human Rights Commission's definition of essential requirements, which are the fundamental knowledge and skills students must acquire to meet the program's learning objectives. The program will ensure that appropriate accommodations are provided to students with disabilities, allowing them to meet these essential requirements without altering the program's standards or outcomes. The goal of these accommodations is to offer equal opportunities for all students to succeed academically, enabling qualified students with disabilities to achieve the same level of performance and benefit from the program without compromising academic integrity. In this regard, the department will collaborate with the Paul Menton Centre to evaluate requests for academic accommodations for students with disabilities, in accordance with human rights legislation and University policy. This process is supported by relevant professional or medical documentation, and academic accommodations are granted only if the student's disability directly impacts their academic performance. The proposed process and resources are both appropriate and judicious.

Admission Requirements

- Appropriateness of the program's admission requirements given the program's objectives and program-level learning outcomes
- Sufficient explanation of alternative requirements, if applicable, for admission into a graduate, second-entry or undergraduate program, e.g., minimum grade point average, additional languages or portfolios, and how the program recognizes prior work or learning experience.

The proposal states that admission requirements will align with those of all B.Eng. programs, which are standardized and based on the Ontario High School System. Each year, admission averages are

determined on a program-specific basis, and meeting the minimum requirements qualifies applicants for consideration. For first-year entry, applicants must hold an Ontario Secondary School Diploma (OSSD) or an equivalent qualification, including at least six 4U or M courses. Required subjects include Advanced Functions, Chemistry, Physics, and one of Calculus and Vectors (recommended), Biology, or Earth and Space Science. While not mandatory, a 4U course in English or French is recommended. Applications for advanced standing (beyond the first year) are assessed individually. Direct admission to the first-year co-op program requires meeting both the overall admission cut-off average and a higher prerequisite course average. For international applicants, the program will follow Carleton University's policy to assess academic equivalency and determine whether proof of English proficiency is required based on the applicant's country of origin. These admission criteria are both appropriate and well-structured to ensure academic quality.

Resources

Given the program's planned /anticipated class sizes and cohorts as well as its program-level learning outcomes:

- Participation of a sufficient number and quality of core faculty who are competent to teach and/or supervise in the program and foster the appropriate academic environment
- If applicable, discussion/explanation of the role and approximate percentage of adjunct and part-time faculty/limited term appointments used in the delivery of the program and the associated plans to ensure the sustainability of the program and quality of the student experience

  If required, provision of supervision of experiential learning opportunities
- Adequacy of the administrative unit's planned utilization of existing human, physical and financial resources, including implications for the impact on other existing programs at the university
- Evidence that there are adequate resources to sustain the quality of scholarship and research activities produced by students,including library support, information technology support, and laboratory access
- If necessary, additional institutional resources commitments to support the program in step with its ongoing implementation

The department currently possesses an adequate number of faculty members to initiate the program, comprising core engineering faculty as well as three additional faculty members with specialized expertise in cybersecurity. To further bolster the program, the department intends to recruit four additional faculty members with a focus on cybersecurity over the next three years. In alignment with the program's structure, it is recommended to appoint two faculty members in the first year, followed by one faculty member each in the second and third years following the program's launch.

Additionally, it is strongly recommended to initiate planning for the establishment of a dedicated cybersecurity laboratory. Such a facility would provide a specialized environment necessary for conducting offensive and forensic activities, which often require isolation from general-purpose systems. This laboratory could be established either as a physical space or a virtual environment, depending on feasibility and resource availability.

While the program's growth projections are outlined in the proposal, the estimated numbers may be somewhat conservative, particularly considering the growing demand for similar programs in the region. Therefore, it is imperative to remain flexible and prepared to scale teaching capacity and infrastructure beyond the proposed levels should enrollment exceed initial expectations.

Quality and other indicators

- Evidence of the quality of the faculty (e.g., qualifications, funding, honours, awards, research, innovation and scholarly record; appropriateness of collective faculty expertise to contribute substantively to the program and commitment to student mentoring
- Any other evidence that the program and faculty will ensure the intellectual quality of the student experience

The faculty members in the department possess a wealth of expertise across a diverse range of disciplines, including engineering, advanced networking, cybersecurity, communications, and systems design. This multidisciplinary expertise ensures that the program is supported by a robust academic foundation, enabling students to gain both depth and breadth in their learning experience. Faculty members are not only highly qualified but also actively engaged in cutting-edge research, innovation, and scholarly activities, which directly contribute to the intellectual rigor and relevance of the program.

The department has a highly respectable level of research output, evidenced by numerous peer-reviewed publications, competitive research grants, and collaborations with industry and government agencies. In addition to their academic and research accomplishments, faculty members have received numerous honors and awards, recognizing their contributions to their respective fields. The department itself is well-established, with a strong reputation for academic excellence and a proven track record of delivering high-quality programs. Its infrastructure, resources, and institutional support provide a solid foundation for the successful launch and sustainability of the proposed program. Furthermore, the department is committed to continuous improvement, regularly reviewing and updating the program to reflect emerging trends and industry needs.

Additional Comments:

Summary of Recommendations

Use the chart below to summarize your overall recommendations for the program. If possible, it would be beneficial to the university for the recommendations to be prioritized.

Recommendation	**Category** *(Weakness, Concern, Opportunity)*
1) The program should comprehensively address key areas of cybersecurity by incorporating: Operational Technology (OT) security, offensive security, digital forensics, and threat hunting with security monitoring. These critical topics may be integrated within the proposed courses or offered as distinct courses to ensure a well-rounded and in-depth curriculum. By covering these domains, the program will equip students with the specialized knowledge and practical skills needed to navigate complex security challenges, detect and mitigate cyber threats, and safeguard both IT and OT environments in an increasingly digital world.	Weakness
2) It is recommended that the program include a dedicated course on the foundations of cryptography and cryptanalysis to provide students with a strong theoretical and practical understanding of secure communication and data protection. This course would cover essential cryptographic principles, encryption algorithms, cryptographic protocols, and methods for analyzing and breaking cryptographic systems. By integrating this foundational knowledge, students will develop critical skills in designing secure ciphers and evaluating their vulnerabilities, ensuring they are well-prepared to address emerging challenges in cybersecurity.	Opportunity
3) It is recommended that students be introduced to cybersecurity concepts from Year 1 through a foundational Introduction to Cybersecurity course. This early exposure will establish a strong baseline of knowledge, fostering engagement with core security concepts from the outset.	Opportunity

4) It is recommended that the faculty and university provide support for the department in acquiring the necessary software and hardware infrastructure to enhance the cybersecurity teaching lab. Access to state-of-the-art servers and computers, cybersecurity and networking appliances, cybersecurity software, and specialized cybersecurity platforms is essential for delivering a hands-on, experiential learning experience. By investing in these resources, the program will be better equipped to train students in real-world security practices, ensuring they develop the technical proficiency required to administer and manage cybersecurity.	Concern
5) It is recommended that the department proceed with the hiring of two faculty members in Year 2**,** followed by one additional faculty member in Year 3 and another in Year 4 of the program**.** This phased hiring approach will ensure that the program has the necessary expertise and instructional capacity to support its growing curriculum and student enrollment. Expanding the faculty will also strengthen research and industry collaborations, further enhancing the program's impact and sustainability.	Opportunity
6) It is recommended that the department actively pursue fostering agreements with public and private organizations to establish co-op placement opportunities for students. Building strong partnerships with industry, government agencies, and cybersecurity firms will provide students with invaluable hands-on experience in real-world security environments. These collaborations will not only enhance students' professional development but also strengthen the program's ties to industry, ensuring that graduates are well-prepared to meet the evolving demands of the cybersecurity workforce.	Opportunity
7) It is recommended that the university allocate additional teaching capacity and resources should enrollment exceed the planned numbers. This investment would	Opportunity

ensure that the program maintains high-quality instruction, adequate faculty support, and access to essential learning resources. Expanding teaching capacity in response to increased demand will help sustain an optimal student-to-faculty ratio, preserve the program's academic integrity, and continue delivering a rigorous and engaging learning experience.	

Systems Security Engineering
Unit Response to External Reviewers' Report & Implementation Plan
Programs Being Reviewed: New Undergraduate Program

Note: This document is forwarded to Senate, the Quality Council and posted on the Vice- Provost's external website.

Introduction & General Comments

Please include any general comments regarding the External Reviewers' Report.

[Sample Text: The Department/School/Institute was pleased to receive the Reviewers' very positive External Reviewers' report on [date]. This report was shared with our faculty and staff, and we are committed to the continual improvement of our programs to enhance the student, staff, and faculty experience. This document contains both a response to the External Reviewers' Report and an Implementation Plan (Section B) which have been created in consultation with the Dean(s).

For each recommendation one of the following responses must be selected:

Agreed to unconditionally: used when the unit agrees to and is able to take action on the recommendation without further consultation with any other parties internal or external to the unit.
Agreed to **if additional resources permit:** used when the unit agrees with the recommendation, however action can only be taken if additional resources are made available. Units must describe the resources needed to implement the recommendation and provide an explanation demonstrating how they plan to obtain those resources. In these cases, discussions with the Deans will normally be required and therefore identified as an action item.
Agreed to in principle: used when the unit agrees with the recommendation, however action is dependent on something other than resources. Units must describe these dependencies and determine what actions, if any, will be taken.
Not agreed to: used when the unit does not agree with the recommendation and therefore will not be taking further action. A rationale must be provided to indicate why the unit does not agree (no action should be associated with this response).

Calendar Changes

If any of the action items you intend to implement will result in calendar changes, please describe what those changes will be. To submit a formal calendar change, please do so using the Courseleaf system.

The Department was pleased to receive the Reviewers' very positive External Reviewers' report on March 3rd, 2025. This report was shared with our faculty, and we are committed to the continual improvement of our programs to enhance the student, staff, and faculty experience. This document contains both a response to the External Reviewers' Report and an Implementation Plan which have been created in consultation with the Dean(s).

UNIT RESPONSE AND IMPLEMENTATION PLAN **Programs Being Reviewed: Systems Security Engineering** **Prepared by : Jerome Talim, Assistant Professor, Systems and Computer Engineering – March 10, 2025**					
External Reviewer Recommendation & Categorization	**Unit Response:** **1- Agreed to unconditionally** **2- Agreed to if additional resources permit (describe resources)** **3- Agreed to in principle** **4- Not agreed to** **Rationales are required for categories 2, 3 & 4**	**Action Item**	**Owner**	**Timeline**	**Will the action described require calendar changes? (Y or N)**
1) The program should comprehensively address key areas of cybersecurity by incorporating: Operational Technology (OT) security, offensive security, digital forensics, and threat hunting with security monitoring. These critical topics may be integrated within the proposed courses or offered as distinct courses to ensure a well-rounded and in depth curriculum. By covering these domains, the program will equip students with the specialized knowledge and practical skills needed to navigate complex security challenges, detect and mitigate cyber threats, and safeguard both IT and OT environments in an increasingly digital world. **(Weakness)**	*Agreed to in principle* *Rationale : The program is predominantly focused on cybersecurity in Information Technology (IT). The curriculum will present standard practices in major domains (e.g., Finances, government, healthcare systems …) and corresponding solutions (in systems design, analysis and monitoring).* *The department acknowledges the importance of Operational Technology (OT), which nowadays includes IT implementation. At the same time, while the topic is important, exposing students to the topic in a relevant fashion requires training to specific technologies and tools, which is not necessarily the purpose of a B.Eng.*	*[Course development] The course SYSC 4822 (Network Security Development Project) in the final year will comprise two major components: (a) one project offering the students the opportunity to implement solutions or to simulate large-scale systems, and (b) the lectures where the class will discuss real-life scenarios and practical case studies in Information Technology and in Operational Technology. Real-life scenarios, including exposure to OT, will be enriched by guest lectures from the industry or the government.*	*Department*	*Fall 2027*	*Yes* *The calendar description of the course SYSC 4822 will be updated*

2) It is recommended that the program include a dedicated course on the foundations of cryptography and cryptanalysis to provide students with a strong theoretical and practical understanding of secure communication and data protection. This course would cover essential cryptographic principles, encryption algorithms, cryptographic protocols, and methods for analyzing and breaking cryptographic systems. By integrating this foundational knowledge, students will develop critical skills in designing secure ciphers and evaluating their vulnerabilities, ensuring they are well prepared to address emerging challenges in cybersecurity. **(Opportunity)**	*Agreed to in principle* *Rationale: The curriculum presents a holistic approach to computer systems security, by coupling threats to the network and computer systems. Students will learn to assess systems security, propose remedial solutions and integrate security in design solutions.* *The design of the curriculum will present cryptography as a tool to support secure system design and configuration. Students of the program are not expected to be experts in cryptography or in designing new encryption algorithms. Rather than introducing a new course dedicated to cryptography, the curriculum relies on the two courses SYSC 4831 (Software Security) and SYSC 4832 (s Network Security) to present the fundamentals of cryptography and how it is used in network and computer systems. The calendar description of the two courses will be updated to include topics related to cryptography.* *The curriculum includes the course SYSC 3821 (Data Security and Cryptography) to include more theoretical content in cryptography*	*[Course development] The department will take into account the recommendations of the external reviewers during the development of the new courses.* *Possibly, the department may also introduce an elective specific to the topic and which would also be relevant to other programs in Engineering; alternatively, the department may look at courses offered by the School of Computer Science on the topic and which could serve as electives.*	*Department*	*Winter 2026 – Summer 2027*	*Yes* *The calendar description of the courses SYSC 3821, SYSC 4831 and SYSC 4832 will be updated.*
3) It is recommended that students be introduced to cybersecurity concepts from Year 1 through a foundational Introduction to Cybersecurity course. This early exposure will establish a strong baseline of knowledge, fostering engagement with core security concepts from the outset. **(Opportunity)**	*Agreed to unconditionally*	*[Course development] The curriculum includes the introductory course ECOR 1055 (Introduction to Engineering Disciplines I). Each engineering program is assigned a specific section of the course and students are introduced to the general concepts of their discipline. The course also offers an overview of the curriculum and possibly presents potential career paths.*	*Department*	*Fall 2026 – Summer 2027*	*No*

4) It is recommended that the faculty and university provide support for the department in acquiring the necessary software and hardware infrastructure to enhance the cybersecurity teaching lab. Access to state-of-the-art servers and computers, cybersecurity and networking appliances, cybersecurity software, and specialized cybersecurity platforms is essential for delivering a hands-on, experiential learning experience. By investing in these resources, the program will be better equipped to train students in real-world security practices, ensuring they develop the technical proficiency required to administer and manage cybersecurity. **(Concern)**	*Agreed to unconditionally*	*The discussion on teaching lab equipment started with the curriculum development and will move to the planning phase (network devices and software) as the new courses in security are being developed.*	*Department*	*From Winter 2027*	*No*
5) It is recommended that the department proceed with the hiring of two faculty members in Year 2, followed by one additional faculty member in Year 3 and another in Year 4 of the program. This phased hiring approach will ensure that the program has the necessary expertise and instructional capacity to support its growing curriculum and student enrollment. Expanding the faculty will also strengthen research and industry collaborations, further enhancing the program's impact and sustainability. **(Opportunity)**	*Agreed to if additional resources permit* *Rationale: The recommended hiring calendar will certainly contribute positively to the curriculum development (core courses and electives) as well as strengthen research activities in cybersecurity sooner. The hiring of new faculty will be subjected to budget approval by the Dean and the Provost.*	*Discussion with the Dean*	*Department,* *Office of the Dean of the Faculty of Engineering and Design*	*From Fall 2026*	*No*
6) It is recommended that the department actively pursue fostering agreements with public and private organizations to establish co-op placement opportunities	*Agreed to unconditionally*	*The development of the program was conducted with active discussions with the advisory board, which comprises partners from the industry and the government, as*	*Department*	*From Fall 2027*	*No*

	for students. Building strong partnerships with industry, government agencies, and cybersecurity firms will provide students with invaluable hands-on experience in real-world security environments. These collaborations will not only enhance students' professional development but also strengthen the program's ties to industry, ensuring that graduates are well-prepared to meet the evolving demands of the cybersecurity workforce**. (Opportunity)**		*well as key companies (large and small) in the Ottawa region. The department will seek further support and collaboration to promote the program and the students.*			
7)	It is recommended that the university allocate additional teaching capacity and resources should enrollment exceed the planned numbers. This investment would Opportunity ensure that the program maintains highquality instruction, adequate faculty support, and access to essential learning resources. Expanding teaching capacity in response to increased demand will help sustain an optimal student-to-faculty ratio, preserve the program's academic integrity, and continue delivering a rigorous and engaging learning experience. **(Opportunity)**	*Agreed to unconditionally*	*The department and the Faculty of Engineering and Design will monitor the enrollment and will take relevant actions to ensure the high quality of the students' learning experience.*	*Department,* *Office of the Dean of the Faculty of Engineering and Design*	*From Fall 2027*	*No*

Systems and Computer Engineering
Dean's Response
Programs Being Reviewed: Systems Security Engineering
Date: March 18, 2025
Version: 1.0

Instruction
The table below has been pre-populated with the external reviewer recommendations. Please complete the Dean's Response column by providing a separate response to each of the external reviewers' recommendations, as required by the QAF (5.3.1).

Dean's Response **Programs Being Reviewed: BENG Systems Security Engineering** **Prepared by: Larry Kostiuk**		
External Reviewer Recommendation & Categorization	**Dean's response** **A response is required for each recommendation listed.**	
1) The program should comprehensively address key areas of cybersecurity by incorporating: Operational Technology (OT) security, offensive security, digital forensics, and threat hunting with security monitoring. These critical topics may be integrated within the proposed courses or offered as distinct courses to ensure a well-rounded and in depth curriculum. By covering these domains, the program will equip students with the specialized knowledge and practical skills needed to navigate complex security challenges, detect and mitigate cyber threats, and safeguard both IT and OT environments in an increasingly digital world. **(Weakness)**	*Getting the balance right between IT and OT is important for the overall effectiveness of the students after they graduate. Ther external reviewers are challenging the existing balance with the advice that greater emphasis be placed on OT, while recognizing that the current proposed structure could readily be adapted for that purpose. The Unit's acknowledgement of the need for this balance and their plans to address it seems to be sufficient currently.*	
2) It is recommended that the program include a dedicated course on the foundations of cryptography and cryptanalysis to provide students with a strong theoretical and practical understanding of secure communication and data protection. This course would cover essential cryptographic principles, encryption algorithms, cryptographic protocols, and methods	*The department's approach to incorporating the recommendation for greater emphasis of cryptography and cryptanalysis as a program opportunity is an appropriate response to the reviewers' comment. In the end, there is a limited number of courses that can be asked of students to take, and since the recommendation did not provide any suggestions as to what material to remove, the approach of making these topics part of an elective course is fitting*	

for analyzing and breaking cryptographic systems. By integrating this foundational knowledge, students will develop critical skills in designing secure ciphers and evaluating their vulnerabilities, ensuring they are well prepared to address emerging challenges in cybersecurity. **(Opportunity)**	
3) It is recommended that students be introduced to cybersecurity concepts from Year 1 through a foundational Introduction to Cybersecurity course. This early exposure will establish a strong baseline of knowledge, fostering engagement with core security concepts from the outset. **(Opportunity)**	*Fully agree with the recommendation, all engineers should be exposed to the concepts of cybersecurity.*
4) It is recommended that the faculty and university provide support for the department in acquiring the necessary software and hardware infrastructure to enhance the cybersecurity teaching lab. Access to state-of-the-art servers and computers, cybersecurity and networking appliances, cybersecurity software, and specialized cybersecurity platforms is essential for delivering a hands-on, experiential learning experience. By investing in these resources, the program will be better equipped to train students in real-world security practices, ensuring they develop the technical proficiency required to administer and manage cybersecurity. **(Concern)**	*The business plan for this new program included resources for this intent. The details of that investment will have to be address in subsequent budget years.*
5) It is recommended that the department proceed with the hiring of two faculty members in Year 2, followed by one additional faculty member in Year 3 and another in Year 4 of the program. This phased hiring approach will ensure that the program has the necessary expertise and instructional capacity to support its growing curriculum and student enrollment. Expanding the faculty will also strengthen research and industry collaborations, further enhancing the program's impact and sustainability. **(Opportunity)**	*The business plan for this new program included the hiring of a few new faculty members (regular and teaching stream) and was approved in principle. The exact timing of those hires will have to take the institutions current financial situation into consideration.*

6) It is recommended that the department actively pursue fostering agreements with public and private organizations to establish co-op placement opportunities for students. Building strong partnerships with industry, government agencies, and cybersecurity firms will provide students with invaluable hands-on experience in real-world security environments. These collaborations will not only enhance students' professional development but also strengthen the program's ties to industry, ensuring that graduates are well-prepared to meet the evolving demands of the cybersecurity workforce**.** **(Opportunity)**	*Coop programs at Carleton University are managed centrally and the department will provide input into their processes to hopefully secure the appropriate quantity and quality of positions for students.*
7) It is recommended that the university allocate additional teaching capacity and resources should enrollment exceed the planned numbers. This investment would Opportunity ensure that the program maintains highquality instruction, adequate faculty support, and access to essential learning resources. Expanding teaching capacity in response to increased demand will help sustain an optimal student-to-faculty ratio, preserve the program's academic integrity, and continue delivering a rigorous and engaging learning experience. **(Opportunity)**	*The Faculty has every expectation that this program will be successful in attracting students, and will be monitoring the student numbers to consider further investments of instructors and facilities.*

Program Change Request

New Program Proposal

Date Submitted: 09/25/25 11:44 am

Viewing: TBD-2305 : Systems Security Engineering

Last edit: 01/21/26 11:49 am

Last modified by: angelwagner

Changes proposed by: jerometalim

In Workflow

1. **SYST ChairDir UG**
2. **ENG Dean**
3. **ENG FCC**
4. **ENG FBoard**
5. **PRE SCCASP**
6. **SCCASP**
7. SQAPC
8. Senate
9. PRE CalEditor
10. CalEditor

Approval Path

1. 10/01/25 9:48 am Jerome Talim (jerometalim): Approved for SYST ChairDir UG
2. 10/09/25 10:16 am Samuel Ajila (samuelajila): Approved for ENG Dean
3. 10/17/25 10:09 am Samuel Ajila (samuelajila): Approved for ENG FCC
4. 10/28/25 3:36 pm Samuel Ajila (samuelajila): Approved for ENG FBoard
5. 01/20/26 12:52 pm Angel Wagner (angelwagner): Approved for PRE SCCASP

Effective Date	2027-28

Workflow	majormod
Program Code	TBD-2305
Level	Undergraduate
Faculty	Faculty of Engineering and Design
Academic Unit	Department of Systems and Computer Engineering
Degree	Bachelor of Engineering
Title	Systems Security Engineering

Program Requirements

Systems Security Engineering

Bachelor of Engineering (21.0 credits)

First year

1. a) 4.5 credits in: 4.5

CHEM 1101 [0.5]	Chemistry for Engineering Students
ECOR 1031 [0.5]	Programming and Data Management
ECOR 1032 [0.5]	Circuits and Mechatronics
ECOR 1033 [0.5]	Statics
ECOR 1034 [0.5]	Dynamics
MATH 1004 [0.5]	Calculus for Engineering or Physics
MATH 1104 [0.5]	Linear Algebra for Engineering or Science
PHYS 1004 [0.5]	Introductory Electromagnetism and Wave Motion
SYSC 1006 [0.5]	Foundations of Imperative Programming

b) The introduction to Engineering Disciplines requirement must be met through the successful completion of:

ECOR 1055 [0.0]	Introduction to Engineering Disciplines I
ECOR 1056 [0.0]	Introduction to Engineering Disciplines II
ECOR 1057 [0.0]	Engineering Profession

2. 0.5 credit in Science Electives 0.5

Second year

3. a) 3.5 credits in: 3.5

COMP 1805 [0.5]	Discrete Structures I
MATH 1005 [0.5]	Differential Equations and Infinite Series for Engineering or Physics
SYSC 2100 [0.5]	Algorithms and Data Structures

SYSC 2310 [0.5]	Introduction to Digital Systems	
SYSC 2320 [0.5]	Introduction to Computer Organization and Architecture	
SYSC 2510 [0.5]	Probability, Statistics and Random Processes for Engineers	
SYSC 2821 [0.0]	Introduction to Cybersecurity	
b) Successful completion of		
ECOR 2995 [0.0]	Engineering Portfolio	
4. 0.5 credit from:		0.5
SYSC 2004 [0.5]	Object-Oriented Software Development	
SYSC 2010 [0.5]	Programming Project	
5. 0.5 credit in Complementary Studies Electives		0.5
6. 0.5 credit in Science Electives		0.5
Third year		
7. 5.0 credits in:		5.0
CCDP 2100 [0.5]	Communication Skills for Engineering Students	
ECOR 2050 [0.5]	Design and Analysis of Engineering Experiments	
ECOR 3800 [0.5]	Engineering Economics	
SYSC 3310 [0.5]	Introduction to Real-Time Systems	
SYSC 3512 [0.5]	Computer Communications	
SYSC 3523 [0.0]	Introduction to Distributed Applications	
SYSC 3821 [0.0]	Data Security and Cryptography	
SYSC 3822 [0.0]	Network Security I	
SYSC 4001 [0.5]	Operating Systems	
SYSC 4416 [0.5]	Artificial Intelligence in Engineering	
Fourth year		
8. 2.5 credits in:		2.5
ECOR 4995 [0.5]	Professional Practice	
SYSC 4821 [0.0]	Security in Emerging Technologies	
SYSC 4822 [0.0]	Network Security Development Project	
SYSC 4831 [0.0]	Software Security	
SYSC 4832 [0.0]	Network Security II	
9. 1.0 credit from:		1.0
SYSC 4907 [1.0]	Engineering Project	
OR		
ECOR 4907 [1.0]	Multidisciplinary Engineering Project	
10. 2.0 credits from:		2.0
SYSC at the 3000 level or above (may include up to 1.0 credit in SYSC at the 5000 level)		
11. 0.5 credit in Complementary Studies Electives		0.5
Total Credits		21.0

New Resources	Faculty Teaching Assistant
Summary	The Department of Systems and Computer Engineering is proposing a new program in systems security, It offers a holistic view of security across the

	network, computer systems and software layer. What makes the program distinctive is its integration of defense mechanisms to the design of (distributed) systems. The curriculum will include project-based courses where students will assess defense solutions and simulate system attacks. It will also cover security in emerging technologies.
Rationale	A Bachelor of Engineering in Systems Security would be an addition that complements the other existing programs (Software, Computer Systems, Telecommunications). Security at the design, deployment and management phases is an essential requirement in reliable distributed systems. The proposed program will cover the integration of security, as a technical constraint or objective, in the design process of projects in networks, middleware and applications. Graduates will think in end-to-end attack strategies and defense mechanisms rather than isolated approaches.
Transition/Implementation	The documentation (Volume I, II and III) were submitted back in Fall 2024 and the site visit took place during the Winter 2025. With the first cohort in Fall 2027, the department will develop the new courses starting Fall 2026, including some upper year courses, which will be offered as electives to the other programs.

Program reviewer comments	**angelwagner (01/20/26 12:50 pm):** Formatting. **angelwagner (01/21/26 11:49 am):** Updated summary and rationale provided by APSI.

Key: 2305

Program Change Request

New Program Proposal

Date Submitted: 09/25/25 11:44 am

Viewing: TBD-2305 : Systems Security Engineering

Last edit: 01/21/26 11:49 am

Last modified by: angelwagner

Changes proposed by: jerometalim

In Workflow

1. **SYST ChairDir UG**
2. **ENG Dean**
3. **ENG FCC**
4. **ENG FBoard**
5. **PRE SCCASP**
6. **SCCASP**
7. SQAPC
8. Senate
9. PRE CalEditor
10. CalEditor

Approval Path

1. 10/01/25 9:48 am Jerome Talim (jerometalim): Approved for SYST ChairDir UG
2. 10/09/25 10:16 am Samuel Ajila (samuelajila): Approved for ENG Dean
3. 10/17/25 10:09 am Samuel Ajila (samuelajila): Approved for ENG FCC
4. 10/28/25 3:36 pm Samuel Ajila (samuelajila): Approved for ENG FBoard
5. 01/20/26 12:52 pm Angel Wagner (angelwagner): Approved for PRE SCCASP

Effective Date	2027-28

Workflow	majormod
Program Code	TBD-2305
Level	Undergraduate
Faculty	Faculty of Engineering and Design
Academic Unit	Department of Systems and Computer Engineering
Degree	Bachelor of Engineering
Title	Systems Security Engineering

Program Requirements

Systems Security Engineering

Bachelor of Engineering (21.0 credits)

First year

1. a) 4.5 credits in: 4.5

CHEM 1101 [0.5]	Chemistry for Engineering Students
ECOR 1031 [0.5]	Programming and Data Management
ECOR 1032 [0.5]	Circuits and Mechatronics
ECOR 1033 [0.5]	Statics
ECOR 1034 [0.5]	Dynamics
MATH 1004 [0.5]	Calculus for Engineering or Physics
MATH 1104 [0.5]	Linear Algebra for Engineering or Science
PHYS 1004 [0.5]	Introductory Electromagnetism and Wave Motion
SYSC 1006 [0.5]	Foundations of Imperative Programming

b) The introduction to Engineering Disciplines requirement must be met through the successful completion of:

ECOR 1055 [0.0]	Introduction to Engineering Disciplines I
ECOR 1056 [0.0]	Introduction to Engineering Disciplines II
ECOR 1057 [0.0]	Engineering Profession

2. 0.5 credit in Science Electives 0.5

Second year

3. a) 3.5 credits in: 3.5

COMP 1805 [0.5]	Discrete Structures I
MATH 1005 [0.5]	Differential Equations and Infinite Series for Engineering or Physics
SYSC 2100 [0.5]	Algorithms and Data Structures

SYSC 2310 [0.5]	Introduction to Digital Systems	
SYSC 2320 [0.5]	Introduction to Computer Organization and Architecture	
SYSC 2510 [0.5]	Probability, Statistics and Random Processes for Engineers	
SYSC 2821 [0.0]	Introduction to Cybersecurity	
b) Successful completion of		
ECOR 2995 [0.0]	Engineering Portfolio	
4. 0.5 credit from:		0.5
SYSC 2004 [0.5]	Object-Oriented Software Development	
SYSC 2010 [0.5]	Programming Project	
5. 0.5 credit in Complementary Studies Electives		0.5
6. 0.5 credit in Science Electives		0.5
Third year		
7. 5.0 credits in:		5.0
CCDP 2100 [0.5]	Communication Skills for Engineering Students	
ECOR 2050 [0.5]	Design and Analysis of Engineering Experiments	
ECOR 3800 [0.5]	Engineering Economics	
SYSC 3310 [0.5]	Introduction to Real-Time Systems	
SYSC 3512 [0.5]	Computer Communications	
SYSC 3523 [0.0]	Introduction to Distributed Applications	
SYSC 3821 [0.0]	Data Security and Cryptography	
SYSC 3822 [0.0]	Network Security I	
SYSC 4001 [0.5]	Operating Systems	
SYSC 4416 [0.5]	Artificial Intelligence in Engineering	
Fourth year		
8. 2.5 credits in:		2.5
ECOR 4995 [0.5]	Professional Practice	
SYSC 4821 [0.0]	Security in Emerging Technologies	
SYSC 4822 [0.0]	Network Security Development Project	
SYSC 4831 [0.0]	Software Security	
SYSC 4832 [0.0]	Network Security II	
9. 1.0 credit from:		1.0
SYSC 4907 [1.0]	Engineering Project	
OR		
ECOR 4907 [1.0]	Multidisciplinary Engineering Project	
10. 2.0 credits from:		2.0
SYSC at the 3000 level or above (may include up to 1.0 credit in SYSC at the 5000 level)		
11. 0.5 credit in Complementary Studies Electives		0.5
Total Credits		21.0

New Resources	Faculty Teaching Assistant
Summary	The Department of Systems and Computer Engineering is proposing a new program in systems security, It offers a holistic view of security across the

	network, computer systems and software layer. What makes the program distinctive is its integration of defense mechanisms to the design of (distributed) systems. The curriculum will include project-based courses where students will assess defense solutions and simulate system attacks. It will also cover security in emerging technologies.
Rationale	A Bachelor of Engineering in Systems Security would be an addition that complements the other existing programs (Software, Computer Systems, Telecommunications). Security at the design, deployment and management phases is an essential requirement in reliable distributed systems. The proposed program will cover the integration of security, as a technical constraint or objective, in the design process of projects in networks, middleware and applications. Graduates will think in end-to-end attack strategies and defense mechanisms rather than isolated approaches.
Transition/Implementation	The documentation (Volume I, II and III) were submitted back in Fall 2024 and the site visit took place during the Winter 2025. With the first cohort in Fall 2027, the department will develop the new courses starting Fall 2026, including some upper year courses, which will be offered as electives to the other programs.

Program reviewer comments	**angelwagner (01/20/26 12:50 pm):** Formatting. **angelwagner (01/21/26 11:49 am):** Updated summary and rationale provided by APSI.

Key: 2305