McGill

Report of the

Academic Policy Committee D21-28

509th REPORT OF THE ACADEMIC POLICY COMMITTEE TO SENATE
on the APC meeting held on December 9th, 2021

I. TO BE APPROVED BY SENATE

(A) NEW TEACHING PROGRAMS REQUIRING SENATE APPROVAL

Graduate and Postdoctoral Studies – *appendix A*
Faculty of Arts
Graduate Certificate in Cybersecurity (15 cr.)

At a meeting on December 9th, 2021, APC reviewed and approved a proposal to create a new Graduate Certificate in Cybersecurity (15 cr.). The graduate certificate is targeted at students with an information technology background who wish to specialize in information security as well as professionals who wish to expand their skills in this area. This online program will respond to a shortage of cybersecurity professionals and will help students identify, address, and prevent cybersecurity threats and attacks which have seen an increase with the advent of new information technologies such as social media and malware. The program focuses on the fundamental concepts of cybersecurity, ethical concerns in terms of security, information guidelines and policies within national and international contexts.

Be it resolved that Senate approve the creation of the proposed Graduate Certificate in Cybersecurity (15 cr.)

(B) ACADEMIC PERFORMANCE ISSUES / POLICIES / GOVERNANCE/AWARDS - *none*

(C) CREATION OF NEW UNITS / NAME CHANGES / REPORTING CHANGES - *none*

(D) CHANGES IN DEGREE DESIGNATION – *none*

(E) INTER-UNIVERSITY PARTNERSHIPS – *none*

(F) OTHER - *none*

II. TO BE ENDORSED BY SENATE / PRESENTED TO SENATE FOR DISCUSSION – *none*

III. APPROVED BY APC IN THE NAME OF SENATE

(A) DEFINITIONS – *none*

(B) STUDENT EXCHANGE PARTNERSHIPS / CONTRACTS / INTERUNIVERSITY PARTNERSHIPS - *none*

(C) OTHER

IV. FOR THE INFORMATION OF SENATE

I. ACADEMIC UNIT REVIEWS - *none*

II. APPROVAL OF COURSES AND TEACHING PROGRAMS - *none*

1. Programs

a) APC Approvals (new options/concentrations and major revisions to existing programs)

i. New Programs

ii. Major Revisions of Existing Programs
Approved by SCTP on December 2nd, 2021 and reported to APC on December 9th, 2021

Desautels Faculty of Management
B.Com.; Major in Information Technology Management (69 cr.)

Schulich School of Music and Faculty of Education
Concurrent B.Mus. and B.Ed.; Major in Music Education and Major in Music Elementary and Secondary (170 cr.)

b) APC Subcommittee on Courses and Teaching Programs (SCTP) Approvals
(Summary Reports: http://www.mcgill.ca/sctp/documents/)

i. Moderate and Minor Program Revisions
Approved by SCTP on December 2nd, 2021 and reported to APC on December 9th, 2021

Faculty of Agricultural and Environmental Sciences
B.Eng. (Bioresource); Major in Bioresource Engineering (113 cr.)
B.Eng. (Bioresource); Honours in Bioresource Engineering (113 cr.)
B.Eng. (Bioresource); Major in Bioresource Engineering; Professional Agrology (113 cr.)

Desautels Faculty of Management
B.Com.; Major in General Management; Concentration in Information Technology Management (15 cr.)
B.Com.; Major in International Management (81-87 cr.)

Schulich School of Music
B.Mus.; Major in Performance Jazz (126 cr.)
B.Mus.; Major in Performance Piano (125 cr.)
B.Mus.; Major in Theory (124 cr.)
B.Mus.; Minor in Music Theory (18 cr.)
B.Mus.; Major in Composition (124 cr.)
B.Mus.; Faculty Program in Music (123 cr.)
B.Mus.; Major in Music History (124 cr.)

Faculty of Science
B.Sc.; Minor in Geography (18 cr.)

ii. Program Retirements

Graduate and Postdoctoral Studies
School of Continuing Studies
Graduate Certificate in Professional Communication; Spanish (18 cr.).

Desautels Faculty of Management
B.Com.; Major in Information Systems (66 cr.).
B.Com.; Major in General Management; Concentration in Information Systems; IT for Business (15 cr.).
B.Com.; Major in General Management; Concentration in Information Systems; Digital Innovation (15 cr.).

2. Courses

a) New Courses

Reported as having been approved by SCTP on December 2nd, 2021:17
Faculty of Arts: 5
School of Continuing Studies: 1
Faculty of Education: 1
Faculty of Medicine and Health Sciences: 1
Schulich School of Music: 7
Faculty of Science: 2

b) Course Revisions

Reported as having been approved by SCTP on December 2nd, 2021:18
Faculty of Engineering: 4
Desautels Faculty of Management: 6
Faculty of Science: 8

c) Course Retirements

Reported as having been approved by SCTP on December 2nd, 2021:7
School of Continuing Studies: 3
Faculty of Engineering: 2
Schulich School of Music: 1
Faculty of Science: 1

D21-28 APPENDIX A

New Program/Major or Minor/Concentration Proposal Form

CC-18-161 (2017)

1.0 Degree Title
Please specify the two degrees for concurrent degree programs

Graduate Certificate (Gr.Cert.)

1.1 Major (Legacy = Subject) (30-char. max.)

Cybersecurity

1.2 Concentration (Legacy = Concentration/Option)
If applicable to Majors only (30 char. max)

1.3 Minor (with Concentration, if Applicable) (30char. max)

2.0 Administering Faculty/Unit

Graduate and Postdoctoral Studies (GPS)

Offering Faculty/Department

AR - Information Studies

3.0 Effective Term of Implementation
(Ex. Sept. 2004 = 200409)
Term

202209

4.0 Rationale and Admission Requirements for New Proposal

There has been an increase in information security threats with the advent of new information technologies such as social media and malware. The graduate certificate will help students identify, address and prevent cybersecurity threats and attacks. Although there are a number of Master's degrees in this area, the certificate will be a self-paced online program that can be completed in less time than a full degree. Students must have a Bachelor's degree in at least one of the following areas: information studies, computer science, information technology, software engineering, computer engineering, or related area with an academic standing of at least a B. Practitioners with at least 6 years of experience in information and communication technology or related area may be considered but should they wish to pursue a Master's degree later on, they will need to have completed an undergraduate degree.

5.0 Program Information

Please check appropriate box(es)

5.1 Program Type

- ☐ Bachelor's Program
- ☐ Master's
- ☐ M.Sc. (Applied) Program
- ☐ Dual Degree/Concurrent Program
- ☐ Certificate
- ☐ Diploma
- ☒ Graduate Certificate
- ☐ Graduate Diploma
- ☐ Ph.D. Program
- ☐ Doctorate Program (Other than Ph.D.)
- ☐ Private Program
- ☐ Off-Campus Program
- ☐ Distance Education Program (By Correspondence)
- ☒ Other:

Please specify

ONLINE

5.2 Category

- ☐ Faculty Program (FP)
- ☐ Major
- ☐ Joint Major
- ☐ Major Concentration (CON)
- ☐ Minor
- ☐ Minor Concentration (CON)
- ☐ Honours (HON)
- ☐ Joint Honours Component (HC)
- ☐ Internship/Co-op
- ☐ Thesis (T)
- ☐ Non-Thesis (N)
- ☐ Other:

Please specify

5.3 Level

- ☐ Undergraduate
- ☐ Dentistry/Law/Medicine
- ☐ Continuing Studies (Non-Credits)
- ☒ Masters & Grad Dip & Certs
- ☐ Doctorate
- ☐ Post-Graduate Medicine/ Dentistry
- ☐ Graduate Qualifying
- ☐ Postdoctoral Fellows

5.4 FQRSC (Research) Indicator
(For GPS)

☐ Yes ☐ No

5.5 Requires Resources
(financial, personnel, space)

☒ Yes ☐ No

6.0 Total Credits

15

7.0 Consultation with

Related Units	☐ Yes	☒ No
Financial Consult	☒ Yes	☐ No

Attach list of consultations.

8.0 Program Description (Maximum 150 words)

The Graduate Certificate in Cybersecurity is an online program that focuses on the fundamental concepts of cybersecurity: threats, cryptography, and vulnerability; the types of cyber-attacks, how they are implemented, and commonly-used hardening techniques and controls; threat and risk assessments at the network system, operating system, and software application levels; the security readiness of an organization; cybersecurity incidents and how to communicate them within an organization; policies to meet current security standards for an organization to adopt; ethical concerns in terms of security, privacy, and information guidelines and policies within national and international contexts.

9.0 List of proposed program for the New Program/Major or Minor/Concentration

If new concentration (option) of existing Major/Minor (program), please attach a program layout (list of courses) of existing Major/Minor.

Proposed program (list course as follow: Subj Code/Crse Num, Title, Credit weight, under the heading of: Required Courses, Complementary Courses, and Elective Courses).

Proposed Graduate Certificate in Cybersecurity (15 credits)

Required Courses (15 credits)
GLIS 680 Introduction to Information Security and Cryptography (3 cr.)
GLIS 681 Modern Software Exploitation and Defence (3 cr.)
GLIS 682 Network and Endpoint Security (3 cr.)
GLIS 683 Windows and Linux OS Hardening (3 cr.)
GLIS 684 Information Security Management (3 cr.)

EXISTING PROGRAMS:

Graduate Certificate (Gr. Cert.) Digital Archives Management (15 credits)
Offered by: Information Studies Degree: C-DAM

Program Requirements
This program is intended to prepare students to work in the area of digital archives. The graduate courses in the program will focus on principles of organization of information, practices in archival studies, and strategies for digital curation and enterprise content management. This in an entry-level, graduate program that may lead to another graduate certificate or to the M.I.St. program, however, none of the courses taken in the graduate certificate can be credited towards the M.I.St. program once a graduate certificate has been completed.

Required Courses (6 credits)
GLIS 607 Organization of Information (3 credits)
GLIS 649 Digital Curation (3 credits)

Complementary Courses (9 credits)
chosen from the following:
GLIS 609 Metadata and Access (3 credits)
GLIS 633 Digital Media (3 credits)
GLIS 641 Archival Description and Access (3 credits)
GLIS 642 Preservation Management (3 credits)
GLIS 645 Archival Principles and Practice (3 credits)
GLIS 657 Database Design and Development (3 credits)
GLIS 660 Enterprise Content Management (3 credits)

****

Graduate Certificate (Gr. Cert.) Information Architecture and Design (15 credits)
Offered by: Information Studies Degree: C-IAD

Program Requirements
The Graduate Certificate in Information Architecture and Design is intended to prepare students to work as information architects and designers. The graduate courses in the program will prepare students to design and assess information systems (text, multimedia), databases, websites, and interfaces. Techniques for data mining and issues related to information security are also covered. This is an entry-level graduate program that may lead to another certificate or to the M.I.St. (Master of Information Studies).

Required Course (6 credits)
GLIS 617 Information System Design (3 credits)
GLIS 625 Information Architecture (3 credits)

Complementary Courses (9 credits)
GLIS 616 Information Retrieval (3 credits)
GLIS 626 Usability Analysis and Assessment (3 credits)
GLIS 627 User-Centered Design (3 credits)
GLIS 629 Information Security (3 credits)
GLIS 630 Data Mining (3 credits)
GLIS 633 Digital Media (3 credits)
GLIS 634 Web System Design and Management (3 credits)
GLIS 657 Database Design and Development (3 credits)

****

Graduate Certificate (Gr. Cert.) Information and Knowledge Management (15 credits)
Offered by: Information Studies Degree: C-IKM

Program Requirements
This program is intended to prepare students to work as information and knowledge managers in a variety of sectors. The graduate courses in the program will focus on the information behavior of individuals, networks and organizations, and the nature of tacit and explicit knowledge services and strategies for identifying, capturing, organizing, storing, sharing, and using knowledge throughout the IM/KM lifecycle in order to learn and improve. Tools and techniques for codifying knowledge and facilitating collaboration in networks are also covered. This in an entry-level, graduate program that may lead to another graduate certificate or to the M.I.St. program, however, none of the courses taken in the graduate certificate can be credited towards the M.I.St. program once a graduate certificate has been completed.

Required Courses (6 credits)
GLIS 619 Information Behaviour and Resources (3 credits)
GLIS 661 Knowledge Management (3 credits)

Complementary Courses (9 credits)
chosen from the following:
GLIS 607 Organization of Information (3 credits)
GLIS 620 Managing Information Organizations (3 credits)
GLIS 662 Intellectual Capital (3 credits)
GLIS 663 Knowledge Taxonomies (3 credits)
GLIS 664 Knowledge Networks (3 credits)
GLIS 665 Competitive Intelligence (3 credits)

****

Graduate Certificate (Gr. Cert.) Library and Information Studies (15 credits)
Offered by: Information Studies Degree: Graduate Certificate in Library & Info St

Program Requirements
Complementary Courses
9-15 credits, three to five GLIS courses chosen in consultation with the student's adviser with the exception of the following courses:
GLIS 647 Research Project 3 (6 credits)
GLIS 689 Selected Topics (3 credits)
GLIS 696D1 Research Paper 2 (6 credits)
GLIS 696D2 Research Paper 2 (6 credits)

0-6 credits of non-GLIS courses with a maximum of 3 credits from outside McGill. All such courses must be at a graduate level and receive prior approval of the student's adviser(s) and the School's Director.

10.0 Approvals

Routing Sequence	Name	Signature	Date
Department	Kimiz Dalkir, Director	Kimiz Dalkir	Dec. 3, 2018
Curric/~~Acad~~ Committee	Joan Bartlett, Curriculum Committee Chair		Nov 26, 2018
Faculty 1	Susan Sharpe	Susan Sharpe	APR 2 9 2019
Faculty 2	Susan Sharpe	Susan Sharpe	NOV 1 9 2019
Faculty 3			
CGPS		CGPS Approval	January 13, 2020
SCTP	Cindy Smith, SCTP Secretary		December 2, 2021
APC		APC approval	December 9, 2021
Senate			

Submitted by

Name	
Phone	
Email	
Submission Date	

To be completed by ARR:

CIP Code

PROPOSAL FOR NEW online Graduate Certificate in Cybersecurity
School of Information Studies
5 courses (15 credits)

Summary

The School of Information Studies (SIS) is a professional school in the Faculty of Arts. We are proposing a new program, a 100% online Graduate Certificate in Cybersecurity. The program will consist of five courses of 8 weeks each. There is a foundational course that should be taken first and a capstone course that should be taken as the last course. The graduate certificate is targeted at students with an information technology background who wish to specialize in information security as well as professionals who wish to expand their skills in this area.

This initiative aligns with the University's stated goal in the Strategic Academic Plan 2017-2022 to deliver online degree programs and professional Masters within the next five years. It also aligns with the strategic vision for SIS is to convert our three of our existing graduate certificates into similar online programs (in Digital Curation, Information and Knowledge Management and in Information Architecture). This will allow our School to offer more than our single ALA-accredited Masters of Information Studies.

Rationale

Due to our growing reliance on web-based technology, the profession of Cybersecurity has grown quickly over the past two decades. It has become essential for organizations to employ cybersecurity professionals who possess technical knowledge, assess and manage information security risks, and present recommendations to senior management.

According to the (ISC)[2] Cybersecurity Workforce Study in 2018, the cybersecurity workforce shortage has increased to more than 2.8 million globally.[1] Deloitte observes a similar trend in Canada. Its research shows that the cybersecurity labour shortage spans across multiple sectors, and it is not a temporary issue. [2] In 2018, the Government of Canada conducted an on-site recruitment event to attract our students to security compliance and monitoring jobs in information security. Recently, the newly established Canadian Centre for Cyber Security came to McGill and organized multiple information sessions to advertise their broad spectrum of cybersecurity job opportunities. At our annual SIS Advisory Committee meeting, which consists of approximately a dozen organizations who employ McGill SIS students, the subject that garnered the most interest was our update on the Cybersecurity graduate certificate. Organizations such as the BDC, CGI, Canada Health Infoway, and the Canadian Centre for Architecture asked us when it would be ready and whether they could send their employees. While there are some existing programs in Quebec, Canada and internationally, SIS is able to

[1] https://www.isc2.org/Research/Workforce-Study
[2] https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

provide a unique perspective on Cybersecurity through our focus on both individual and organizational threats and through the leadership of our CRC Chair in Cybersecurity, Prof. Benjamin Fung.

The availability of an online graduate certificate will provide learning opportunities for individuals worldwide who are unable to come to campus. In Québec, only HEC offers a comparable certificate, but it is not available online. L'Université de Montréal and the University of Toronto offer blended learning models, but McGill's graduate certificate would be unique in providing a fully online program. We believe that our proposed graduate certificate would provide a new path for students who would be interested in pursuing a graduate degree in this area (Master or PhD as well as graduates who would find careers in a broad range of organizations as information security specialists, risk managers and information policy analysts). To this end, a number of universities and organizations were contacted to request letters of support for our proposed program. This list appears in Appendix A.

CRC Chair in Cybersecurity at McGill

Benjamin Fung is a Canada Research Chair in Data Mining for Cybersecurity and heads the Data Mining and Security Lab (DMaS) at SIS. He is an Associate Professor in the School of Information Studies, an Associate Member of Computer Science, and a Co-curator of Cybersecurity in the World Economic Forum.

Dr. Fung has over 120 refereed publications that span the prestigious research forums of data mining, machine learning, privacy protection, cybersecurity, and building engineering. His data mining works in crime investigation and authorship analysis have been reported by media worldwide. His research has been supported in part by Natural Sciences and Engineering Research Council of Canada (NSERC), Social Sciences and Humanities Research Council (SSHRC), Defence Research and Development Canada (DRDC), Fonds de recherche du Québec - Nature et technologies (FRQNT) and NCFTA Canada.

Dr. Fung is the coordinator and the main Content Expert in the content development for the online graduate certificate. Contributing subject matter experts include Anton Stiglic, Information Security Officer for Lotto Quebec, Eleonore Fournier-Tombs (post-doc), and Steven Ding (PhD).

Dr. Fung's research program aims to enhance the data sharing and data mining capabilities for healthcare and cybersecurity professionals. The field of Cybersecurity includes the tools and systems used to monitor, mitigate, and prevent online threats. Cybersecurity professionals use innovative technology to combat hackers, cyberterrorists, network outages, and other technical problems that could compromise network security.

Proposed Graduate Certificate

Key Learning Outcomes of Proposed Graduate Certificate

The increasing prevalence of cyber-attacks on the critical IT infrastructure of our society emphasizes the need for a new generation of cybersecurity professionals with the latest knowledge and techniques to protect an organization's information. This graduate certificate covers a spectrum of cybersecurity topics, from network to operating systems security, from application security to database security, from basic cryptography to advanced secure protocols, and the management of information security. Using real-world business cases and simulations, graduates will develop skills in assessing the information security needs of an organization and formulating short- and long-term cybersecurity strategies and policies.

The key learning outcomes are:

1. Explain the fundamental concepts of cybersecurity such threats, cryptography, and vulnerability.
2. Describe the types of cyber-attacks, how they are implemented, and propose commonly used hardening techniques and controls.
3. Perform threat and risk assessments at the network system, operating system, and software application levels.
4. Assess the security readiness of an organization.
5. Manage cybersecurity incidents and how to communicate them within an organization.
6. Develop policies to meet current security standards for an organization to adopt.
7. Assess ethical concerns in terms of security, privacy, and information guidelines and policies within national and international contexts.

Students may also go on to take the CISSP certification exam (Certified Information Systems Security Professional). CISSP certification addresses the managerial competence, skills, experience, and credibility to design, engineer, implement, and manage an overall information security program that protects organizations from sophisticated attacks. Our courses touch on the materials in each of the eight modules of the CISSP. Our graduate certificate puts more emphasis on the technical aspect while CISSP focuses a bit more on the managerial aspect. Taking our graduate certificate program will definitely help students better prepare for the CISSP certification, but further training is required before taking the CISSP exams. The CISSP website is: https://www.isc2.org/Certifications/CISSP#.

Course Descriptions

Each course is offered as a 100% online course of 8 weeks (but equivalent to standard 13 weeks). Students are expected to commit 130 and 150 hours for a 3-credit course. The courses will be delivered using McGill's myCourses and will include lectures, activities and individual and group assessment. While majority of the courses will be delivered asynchronously, one or more courses may include a synchronous component when it is most appropriate.

GLIS 680 Introduction to Information Security and Cryptography (3 credits)
A general introduction to cybersecurity and cryptography. This course examines the main threats that organizations face towards the protection of data and information concerning its customers and trade secrets. It also covers, at a high level, the basic control mechanisms and processes that can be put in place to protect against these threats and a general introduction to the concepts of cryptography as a way to secure communications. (No prerequisite)

GLIS 681 Modern Software Exploitation and Defence (3 credits)
This course examines modern exploitation and defence techniques for binary executables and web application and the practices that compromise modern protective techniques. The course is divided in two parts. The binary executable section covers a wide range of topics including reverse engineering, string format vulnerability, and code injection while the web security section will explore tools used against web applications such a cross-site scripting, session hijacking and SQL injection. (Prerequisite: GLIS 680)

GLIS 682 Network and Endpoint Security (3 credits)
This course will cover network security and the various technologies, policies, and procedures that are used in combination to create multiple layers of protection within an organization's computer network. The various vulnerabilities and threats to networks will be explored in detail, as well as the many network security controls that are currently available. (Prerequisite: GLIS 680)

GLIS 683 Windows and Linux OS Hardening (3 credits)
Operating system (OS) hardening techniques for Windows and Linux. This course covers both fundamental and advanced topics in operating system security and aims at arming students with the awareness of potential OS security breaches and practical skills of securing a modern operating system. Topics include credential management, process protection, memory protection, malware mitigation, firewall configuration, and intrusion detection tools. (Prerequisite: GLIS 680)

GLIS 684 Information Security Management (3 credits)
An overview of information security management within an organization. The course aims to train students and practitioners to manage and respond to information security threats, whether they be internal or external, discrete or persistent, non-destructive or catastrophic. Topics include information security policy and governance, risk and vulnerability detection, threat readiness, investigation, recovery, privacy and legislation. This course integrates a capstone project that provides students an opportunity to use the knowledge acquired from prerequisite courses in a simulation of a cybersecurity incident. Working in small groups, learners will experience the full life-cycle of a cybersecurity incident, from preparation to discovery to recovery. The project, worth 60% of their final grade, spans the whole term with one week fully dedicated to an online simulation of a data breach. (Prerequisites: GLIS 680, GLIS 681, GLIS 682 and GLIS 683)

Proposed Schedule

1st semester	GLIS 680
2nd semester	GLIS 680, GLIS 681
3rd semester	GLIS 680, GLIS 682
4th semester	GLIS 681, GLIS 682, GLIS 683
5TH semester	GLIS 682, GLIS 683, GLIS 684

Students will have up to three (3) years to complete the graduate certificate (in line with the maximum for part-time McGill students). Full-time students can complete the five courses within a minimum of 24 weeks (680 followed by 681, 682 and 683 in the same semester and concluding with 684).

Target Audience of Proposed Graduate Certificate

This graduate certificate is targeted to students from diverse undergraduate backgrounds such as information studies, social sciences, humanities, science as well as more technical disciplines (such as computer science). In addition, the graduate certificate is expected to be of interest to IT professionals and managers who already possess experience in the sector of information and communication technology and who would like to refresh their knowledge and skills in this area.

Students should have basic knowledge of information, information security and technology and seek to strengthen their skillset by include cybersecurity knowledge and know-how.

We have received a great deal of interest in this proposed graduate certificate from a number of Quebec organizations (for example, those on the SIS Advisory Committee). They would be interested in having their employees complete the graduate certificate and there is potential to seek sponsorship from them. Employee training is typically paid for by their employers. The graduate certificate should also be accessible to Quebec students, and they will be eligible for the usual awards and scholarships (from McGill and from the School).

Admission requirements

Bachelor's degree in information studies, computer science, information technology, software engineering, computer engineering, or related area from a recognized university with a GPA of 3.0/4.0. Alternatively, practitioners with at least 6 years of industrial experience in information and communication technology or related area will also be considered. However, these students will be advised that should they wish to pursue a Master's degree later on, they will need to have completed an undergraduate degree.

Teaching Resources Required

Most comparable programs have three to six instructors. Prof. Fung will be able to teach one of the courses. We will need at least three other instructors who could be doctoral students or

sessional lecturers. Minimum qualifications for teaching the graduate certificate courses would be a Master's or a PhD degree in an area related to cybersecurity. Industrial experience of managing security risks and incidents in enterprise information systems will be an asset. The graduate certificate would be sustainable through the hiring of sessional lecturers. SIS is a professional school that relies on sessional lecturers to bring in professional/practitioner expertise into our Master's program. For example, our current Information Privacy course is taught by Anton Stiglic, Director of Information Security at Lotto Quebec. We will also have access to wide network of cybersecurity professionals through Prof. Fung's network.

Benchmarking

Existing similar programs in Quebec, Canada, the US and internationally were identified. The benchmarking was limited to U15 universities and to online graduate certificate programs. In summary, we found that there were very few graduate-level courses in most programs that address the target audiences for our proposed program, students who may continue with their academic studies as well as professionals seeking to expand their knowledge and skills. Our program is one of the few not offered only for professional development. In addition, we are not focusing exclusively on the managerial level. Our proposed program covers both technical and managerial aspects and aims at equipping information professionals with the theory and skills needed to address information security threats.

The benchmarked university certificate programs are summarized below. The course offerings of each benchmarked program are provided in Appendix D There are also a number of Bachelor and Master's degrees in Cybersecurity (see Appendix E but these were not analyzed as they are multi-year on-site programs).

In Quebec

The HEC (business school of the University of Montreal) offers the "certificat en analyse de la sécurité de l'information et des systems" (Certificate in the security analysis of information and systems) which consists of 10 courses for 30 credits. Three of these are not directly related to cybersecurity. Courses are on-site and the certificate can be done on a full-time or part-time basis. This course is offered in French only. Their certificate focuses on legal aspects and security norms, especially for more vulnerable businesses such as online businesses. They offer a one-day workshop to prepare students for the Certified Information Systems Security Professional (CISSP). The program is aimed at managers or those who want a career as IT or system managers. They do not seem to cover operating systems security and network security. In general, their courses are less technical than our proposed program courses. Website: https://www.hec.ca/programmes/certificats/certificat-analyse-securite-information-et-systemes/index.html.

The University of Montreal's Ecole Polytechnique offers an undergraduate "Certificat en Cybersécurité des réseaux informatiques" (Certificate in Cybersecurity of Computer Networks). The focus is on computer systems, transactional websites, e-commerce applications. The target audience consists of students already familiar with computer science, managers or

administrators of information system security programs. Graduates will be able to assess the level of risk and the potential consequences of inadequate security measures. There are 10 courses for a total of 30 credits. All courses can be done online and can be done part-time or full-time. Their certificate program is not at the graduate level. Courses are offered in French and English. Students only need to take one introductory course at the undergraduate level in order to be admitted to the certificate. Students need to have a CEGEP diploma and have successfully completed either TCY140 (Piratage informatique in another certificate) or CF160 (judicial software in the Cyberfraud certificate) as well as CR010 Introduction to information technologies (or equivalent course). Their certificate program puts more focus on network security. Our program spans across software, operating systems, network, and management. Website: https://www.polymtl.ca/etudes/programmes/certificat-en-cybersecurite-des-reseaux-informatiques

In Canada

The University of Toronto offers a graduate certificate in Cyber Security Management that consists of 3 courses offered by the School of Continuing Studies. Students have 3 years to complete the 3 courses. One course credit may be given through a Prior Learning Assessment (PLA) where prior education and experience can be taken into account. The certificate is targeted at senior working professionals currently working as a senior security analyst or auditor, network manager, infrastructure engineer, or account or project manager. Courses are offered as in-class and hybrid classes (hybrid classes consist of one-day in-class Saturday class with the remainder delivered online). The learning outcomes include recognizing and managing cyber risks, designing and running a cyber security program that works, aligning the student's IT security strategy with business goals and needs, how to anticipate, recognize and respond to cyber security attacks. The content is broadly aligned with CISSP's major domains and model curriculum. Their certificate is really refresher continuing education training for professionals to "upgrade your knowledge in risk assessment and response, security program design, incident and risk management, compliance and governance." The courses are focused on the organizational level only and are more high-level, less technical than our proposed program. Website: https://learn.utoronto.ca/courses-programs/business-professionals/certificates/cyber-security-management#3205

In the US

In the US, there are seven comparable programs. These are summarized below.

1. Rutgers Cybersecurity Certificate Program

The Rutgers Cybersecurity Certificate Program is offered by the Centre for Innovation Education. It is an intensive 4-day program aimed at executives, cybersecurity experts, innovators, and regulators to address cybersecurity from a business point of view. There are six courses plus a capstone project to complete. The certificate is designed to train and develop

professionals who manage cybersecurity issues within an organization. Participants will be able to solve real world cybersecurity problems, recommend practical and strategic solutions, and to communicate results. Courses make use of group work and scenario assessments to help participants understand privacy concerns, cyber regulations, how to select security tools, how to assess risk and devise security strategies. All courses are offered as self-paced online courses that are 8 weeks in duration. Their program is aimed at managers and executives and provides a more condensed, high-level overview of cybersecurity. Website: http://cybersecurity.rutgers.edu/

2. Colorado State University Graduate Certificate in Cybersecurity

The Graduate Certificate in Cyber Security is an accelerated program designed to train people so they know they have the right to keep their digital information secure in today's global infrastructure and how to keep sensitive information out of the wrong hands. All classes are 100% online and self-paced. Coursework in the Graduate Certificate in Cyber Security aligns with 7 of the 8 CISSP) domains. Students evaluate internal and external threats and vulnerabilities to data assets in the enterprise and provide recommendations to mitigate or eliminate areas of weakness. They compare and contrast the concepts of security and privacy and explain how the imperatives for each may complement or interfere with the imperative for the other. They describe and analyze the implications of major emerging technology trends, issues, and threats to the security and privacy of networks and information.
In addition, students analyze possible threats to organizational data and recommend course(s) of action to mitigate cybercrime attacks and analyze a network for vulnerabilities to common cyber-based attacks. Their certificate is an undergraduate certificate that consists of four courses. Website: https://csuglobal.edu/undergraduate/certificates/cyber-security.

3. University of Virginia Online Cyber Security Management Certificate

Six courses for 18 credits are offered by the School of Continuing and Professional studies. Students can be part-time. On average, students take two courses a term, including the summer, to complete the certificate in 12 months. Participants must have an undergraduate degree. The target audience is managers and information technology professionals seeking a cybersecurity management role. Participants will learn to identify cyber threats; devise appropriate defense strategies; develop policy; plan and conduct security assessments; and understand the ethical, legal, and regulatory environment as it relates to operating in cyberspace. This certificate has a management focus whereas our proposed program has a more technical focus. Website: https://www.scps.virginia.edu/certificates/certificate-detail/certificate-in-cybersecurity-management.

4. Indiana University Bloomington Graduate Certificate in Secure Computing

The certificate can be completed in residence in one semester in the School of Informatics, Computing and Engineering. There are 4 courses for 12 credits that cover security, policy, and the social and practical aspects of protecting privacy.

Cybersecurity is the new frontier and Indiana University is at the forefront. We're taking a comprehensive approach to exploration, bringing together leading minds in security, policy, and research to address our greatest challenges—at home and abroad. Participants receive a foundation in designing, implementing, and managing secure information technology systems as well as the social, legislative, and economic considerations around security. This certificate is open to all graduate students and undergraduates who have completed their undergraduate requirements, although formal graduation is not required. Their program is more general and is not offered online. Website: https://www.sice.indiana.edu/graduate/degrees/informatics/security/cert-requirements.html .

5. UCLA Cybersecurity Certificate

The Cybersecurity certificate is a 4-course program offered by the UCLA Extension school (analogous to Continuing Studies). The target audience is network system security professionals, information systems administrators, and software developers. The program is designed to be consistent with relevant portions of the Certified Information System Security Professional (CISSP) certification exam's Common Body of Knowledge (CBK). Courses cover network security, cryptography, database and network risk management and regulatory policies. Additionally, the certificate includes hands-on training on network security penetration testing and defensive strategies. The certificate consists of four required courses with a total of 16 units that are online. Their program offers more computer science content such as cryptography and is focused on network security. Website: https://www.uclaextension.edu/digital-technology/data-analytics-management/certificate/cybersecurity?method=load&certificateId=1062469

6. Stanford University Graduate Certificate in Cybersecurity

The Cybersecurity graduate certificate is offered by the Centre for Professional Development. It provides an overview of computer systems security, including attack protection and prevention. Participants learn about the basic theory and practice of cryptographic techniques, digital forensics for identifying potential threats, legal issues in computer security, privacy policy business implications, designs for network perimeter defenses and testing methods for possible system penetration. Four out of six courses are required. These are offered on-site and require 1-3 years to complete. The target audience consists of information security managers, web developers, computer network architects and professionals working in computer occupations. A conferred Bachelor's degree with an undergraduate GPA of 3.0 or better is required for admission. This is continuing education for professionals whereas our program is aimed at both students and professionals. Website: https://scpd.stanford.edu/public/category/courseCategoryCertificateProfile.do?method=load&certificateId=58042240.

7. Harvard University Graduate Certificate in Cybersecurity

This Certificate is offered by the Harvard Extension School. There are four required courses and they are all online courses. The courses are typically completed within three years. Participants will gain a critical understanding of the technological needs, threats, and weaknesses in cybersecurity as well as the legal, social, and political dynamics of the cyber universe. The key

learning outcomes include understanding data, network, device and communications technology, architecture, and management. Participants will also become familiar with technical and organizational information security risks and communication tactics to mitigate these risks for both traditional and cloud-based. They will also learn to develop and articulate effective enterprise information security policies that address internal and external national and international threats. This is a more high-level course that is not self-paced. Website: https://www.extension.harvard.edu/academics/professional-graduate-certificates/cybersecurity-certificate.

APPENDIX A: LETTERS OF SUPPORT UNIVERSITIES AND ORGANIZATIONS

1. **Bell Canada**
   Director – Security Operations Centre

2. **École de technologie supérieure** (ETS)
   Professeur, Département de génie production automatisée

3. **Samsung Research America**
   Head of Data Science

4. **Secure Logika**
   Founder and Senior Technical Director

5. **Université de Montréal**
   Associate Professor & Interim Director of École de bibliothéconomie et des sciences de l'information

6. **University of Manitoba**
   Assistant Professor, Department of Computer Science

7. **Zayed University**, UAE
   Associate Professor, College of Technological Innovation

APPENDIX B: CURRICULUM OF BENCHMARKED CYBERSECURITY CERTIFICATES

University of Montreal HEC

8 Required courses:

1. Management Information Systems
2. Analysis and Design of IT Solutions
3. Control and regulations of information and system security
4. Governance and risk management of information and system security
5. Application security
6. Infrastructure security
7. Implementation of information and system security
8. Information technology architecture

One course selected from:

1. Workshop to prepare for CISSP certification
2. Physical security of information and systems and introduction to criminology

One course selected from:

1. A course from another graduate certificate program offered by the HEC
2. A course in business language from HEC

University of Montreal Ecole Polytechnique

3 Required courses:

1. Introduction to Cybersecurity
2. Attack and Defence Methods in the Workplace
3. Governance of Cybersecurity

7 Electives (English courses only listed)

1. Operating Systems
2. Storage
3. Networking and Security
4. Internet of Things and Domestic Security
5. Wireless and Mobile Devices
6. Introduction to Programming and Scripts
7. Intrusion Tests

University of Toronto

1. Cyber Security Incident Management (hybrid)
2. Cyber Security Program Design (hybrid)
3. Enterprise IT Risk Management & Cyber Security (in-class)

University of Rutgers

Module 1 The Evolution of Cybersecurity
Module 2 Cybersecurity Regulations and Forensics
Module 3 Cybersecurity Auditing
Module 4 Regulations for Financial Institutions
Module 5 General Data Protection Regulation (GDPR)
Module 6 Cybersecurity Basics
Module 7 Forensics and Response
Module 8 Cyberintelligence
Module 9 Cyber Regulations
Module 10 Cyber Insurance
Module 11 Cybersecurity Risk Management
Module 12 Cybersecurity Strategy
Module 13 Cybersecurity from a Legal Perspective

Colorado State University

1. ISM527: Cyber Security Management
2. ISM529: Emerging Cyber Security Technology, Threats, and Defense
3. ISM530: Enterprise Cyber Security
4. ISM531: Cyber Security Defense and Countermeasures

University of Virginia

Required Courses (4)

1. BUS 5010 Cyber Security Management
2. BUS 5020 Security Policy Development & Assessment
3. BUS 5040 Creating & Conducting a Security Assessment
4. BUS 5100 Cyber Law, Regulation & Ethics

Elective Courses (select 2)

1. BUS 5030 Designing Dynamic Security Architecture
2. BUS 5050 Threat Assessment & Security Measures
3. BUS 5060 Understanding Technology Used in an Open Access Environment
4. BUS 5080 Understanding Cybercrime & Implementing Mitigating Countermeasures
5. BUS 5120 Securing the Internet of Things
6. BUS 6000 Applied Wireless Network Security

UCLA Extension School

4 Required

1. Fundamentals of Cybersecurity
2. Information Systems Infrastructure Security Management
3. Network, Operating System, and Database Security
4. Cybersecurity Lab (Defensive Tools)

Stanford University Centre for Professional Development

Required 4 from:

1. CS140 Operating Systems and Systems Programming
2. CS144 Introduction to Computer Networking
3. CS155 Computer and Network Security
4. CS251 Cryptocurrencies and blockchain technologies
5. CS255 Introduction to Cryptography
6. MS&E293 Technology and National Security

Harvard University Extension School

Required

1. CSCI E-45A The Cyber World: Hardware, Software, Networks, Security, and Management
2. CSCI-45B The Cyber World: Governance, Threats, Conflict, Privacy, Identity, and Commerce

2 Electives from:

1. Introduction to the Challenges and Opportunities of Big Data, the Internet of Things, and Cybersecurity
2. Communication Protocols and Internet Architectures
3. How to Assess and Communicate Risk in Information Security
4. Cybersecurity Incident Response
5. Network Intelligence and Event Monitoring
6. The Cyber World: Hardware, Software, Networks, Security, and Management
7. The Cyber World: Governance, Threats, Conflict, Privacy, Identity, and Commerce
8. Applied Network Security
9. Secure Mobile Computing
10. Cloud Security
11. Introduction to Blockchain and Bitcoin
12. Network Science
13. Cyberspace and International Security
14. Introduction to the Art of Cryptography

APPENDIX C: SELECTED GRADUATE DEGREE PROGRAMS IN CYBERSECURITY

Universities offering Bachelor degrees in cybersecurity

- Penn State University
- Bellevue University
- Colorado Technical University
- Strayer University
- University of Maryland
- Utica College
- Walden University

Universities offering Master's degree in cybersecurity

- Concordia University
- University of Arizona
- Bellevue University
- Berkeley
- Drexel
- Florida Institute of Technology
- Johns Hopkins
- New York University
- Pennsylvania State University
- Syracuse University
- University of San Diego
- University of Southern California

12/13/2018

Subject: **Support Letter for McGill University's Cybersecurity Online Graduate Certificate Program**

Bell

It is my pleasure to support McGill University's initiative of developing an online graduate certificate program in cybersecurity.

Bell Canada is the largest Canadian telecommunications company, providing mobile phone, television, high speed and wireless Internet, and residential home phone services. As the Internet has become the backbone for linking up the critical infrastructures of the society, we recognize the importance of securing the cyberspace of Canada. To achieve this objective, we have developed internal cyber-security practises and innovative services to serve our own organization and several other Canadian corporations. In order to keep those services at top-notch quality and to respond to the high demand of the market, having access to high-quality cybersecurity professionals plays an important role.

The shortage of high-quality professional ends up favouring the cybercriminals. They are doing all that they can to exploit understaffed firms that have little capacity to identify, recognize and reacts to attacks. These organizations are at high danger of enduring an information breach that may take a very long time to recuperate from. Thus, the proposed online certificate program addresses the need of cybersecurity professionals and technicians in the job market.

The proposed certificate program consists of five courses, covering a spectrum of cybersecurity topics, from network to mobile security, from application security to database security, from basic cryptography to operating systems security, and information security management. The proposed certificate program will contribute the industries a new generation of cybersecurity professionals equipped with the latest skills and techniques to secure the cyberspace of Canada.

Thank you.

Martin Labonté
Director – Security Operations Centre

Martin Labonté
Director – Security Operations Centre
E: martin.labonte1@bell.ca
T: 514-870-1043

Université de Montréal

Faculté des arts et des sciences
École de bibliothéconomie
et des sciences de l'information

Bureau du directeur

Montréal,
January 25, 2019

To Whom it May Concern,

I am writing in support of the McGill School of Information Studies, for the creation of their new program in Cybersecurity. I currently hold the position of Interim Head of Department at the École de bibliothéconomie et des sciences de l'information (EBSI) at the Université de Montréal, and this topic has been discussed at our most recent departmental assembly, where it prompted a good deal of interest.
We recognize that their proposed program, the Online Graduate Certificate in Cybersecurity, addresses a need to train professionals in the risks to IT infrastructure and the tools used to recognize and minimize threats to information contained in those cyberinfrastructures.

These concerns are not covered in their entirety by any of our programs. Students who successfully complete the certificate would be welcome to apply to EBSI (provided of course they meet our admission requirements); their knowledge of cybersecurity would be an asset to their overall training in our Masters in Information Science. Also, we will be happy to collaborate in the future if the opportunity should arise, namely by helping to promote the program and recommending it to some of our own students.

Yours truly,

Lyne Da Sylva, Associate Professor
Interim Director of École de bibliothéconomie et des sciences de l'information

C.P. 6128, succursale Centre-ville, Montréal QC H3C 3J7

Mickael Gardoni, Professeur
École de technologie supérieure
Département de génie production automatisée
1100, rue Notre-Dame Ouest, Montréal (Qc) Canada, H3C 1K3
Tél.: 514 396-8411, Télécopieur: 514 396-8595, Bureau A-3588, www.etsmtl.ca

Montréal, 11th of December, 2018

Object: Letter of support for a proposal for new self-funded proposal for new self-funded Graduate Certificate in Cybersecurity

To whom it may concern,

I am writing this reference at the request of Pr. Kimiz Dalkir who is applying to develop a new online Graduate Certificate in Cybersecurity.

As a Pr. Mickael Gardoni, I totally agree with one the statement of the proposal for new self-funded Graduate Certificate in Cybersecurity : The increasing prevalence of cyber-attacks on the critical IT infrastructure of our society emphasizes the need for a new generation of cybersecurity professionals with the latest knowledge and techniques to protect an organization's information. And I think that this program of five courses during 8 weeks each is one the answer because it covers a large spectrum of cybersecurity topics, from network to operating systems security, from application security to database security, from basic cryptography to advanced secure protocols, and the management of information security.

In conclusion, I would highly support this proposal for new self-funded Graduate Certificate in Cybersecurity. If you would need any additional information, feel you free to contact me by email at mickael.gardoni@etsmtl.ca.

Sincerely,

Mickaël Gardoni

SAMSUNG RESEARCH AMERICA
665 Clyde Avenue
Mountain View, CA 94043

Samsung Research America
665 Clyde Avenue
Mountain View, CA 94043

November 26, 2018

Re: Letter of Support – Online Certificate Program on Cybersecurity

To Whom It May Concern:

I am writing to support McGill University to develop an online certificate program in cybersecurity.

As the Head of Data Science at Samsung Research America, I am leading a team to develop production-scale deep/machine learning platforms and algorithms for real-world applications, including personalized recommendation, natural language understanding, user profiling, data-driven user growth strategies, and privacy-preserving data management. Data security and privacy protection are of utmost importance in developing nowadays IT products. Yet, it is very difficult to find quality staff in this area. The online certificate proposed by McGill University is a timely training program to fulfil the demand of the industries. Since the proposed program is online, it removes the constraint of requiring students to physically attend the lectures in a specific location at a specific time. The online program will provide the IT professionals around the world an excellent opportunity to further strengthen their knowledge and management skills in cybersecurity.

I would appreciate it if you can please keep me updated of the certificate program deployment schedule. I will encourage some of our staff to take the program. Should you require further information and feedback, please do not hesitate to contact me.

Thank you.

Yours sincerely,

Rui Chen, *Ph.D.*
Head of Data Science, Senior Staff Research Scientist
Samsung Research America
Email: rui.chen1@samsung.com

McGill University,
Montreal, QC,
Canada

Mascouche, November 25th, 2018

Subject: Support for McGill University online graduate certificate program in cybersecurity

To Whom It May Concern:

This letter is to express Secure Logika's strong support for the McGill University online graduate certificate program in cybersecurity.

Secure Logika is a Quebec-based security company specializing in software assurance, cyber-security services consulting and the development of secure software solutions. Before founding Secure Logika, I have been the Research and Development Director at Hitachi Systems Security. I have accumulated over 20 years of experience in the area of IT cybersecurity, so I am confident to comment on the new online graduate certificate program in cybersecurity.

I wish I could have had the opportunity to attend such a graduate certificate program to learn in a systematic way the foundation of cybersecurity. The proposed certificate program includes five online courses, covering the major topics in cybersecurity:

- The first course is an introductory course.
- The second course focuses on analyzing various security issues of binary executables and web application. I am particularly impressed by the fact that the course covers reverse engineering, which is an important topic in cybersecurity, but often neglected in many cybersecurity training programs.
- The third and the fourth courses covers network security and operating system security, forming the foundational technical knowledge in cybersecurity.
- The fifth course is on information security management, training students to manage and respond to information security threats and incidents. The capstone project provides a nice wrap up the entire certificate program. In general, the certificate program is well designed and covers all the essential topics in the area.

With such an offering, I am convinced that students in computer science, system administrators and network engineers alike will obtain enough materials to widen their security skills.

As a Founder and Senior Technical Director of a Quebec-based security company, I welcome McGill University to create a new certificate program that meets the challenges of the cyber security industry. Should you need further contribution on my end, please feel free to contact me.

Sincerely,

Michel-Ange Zamor
Founder and Senior Technical Director
Secure Logika

UNIVERSITY OF MANITOBA

Noman Mohammed
Assistant Professor
Department of Computer Science
University of Manitoba
Winnipeg, MB, R3T 2N2
Phone: +1 (204) 474-8391
E-mail: noman@cs.umanitoba.ca
http://www.cs.umanitoba.ca/~noman

December 12th, 2018

To Whom It May Concern:

I am writing this letter to support the development of a new online graduate certificate program in Cyber Security at McGill University.

I am an Assistant Professor in the Department of Computer Science at the University of Manitoba, where I lead the Data Security & Privacy (DSP) laboratory. Prior to joining UofM, I was an NSERC postdoctoral fellow in the School of Computer Science at McGill University and a member of the Cryptography, Security, & Privacy (CrySP) Research Group at the University of Waterloo. I completed my M.A.Sc. in Information Systems Security and Ph.D. in Computer Science at Concordia University in 2008 and 2012, respectively. My research interests include private data sharing, secure distributed systems, and applied cryptography. At the DSP laboratory, I along with my students have designed and implemented a number of secure data management systems for various application scenarios such as secure genome computing, private data sharing, and private image processing for social networks. We also have received a number of awards including the Best Student Paper Award in ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (2009) and the Critical Assessment of Data Privacy and Protection Award in iDash Privacy and Security Workshop (2014).

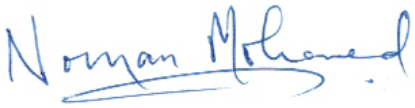
In recent years, there is a boom in cybersecurity jobs globally. A recent report from Deloitte discusses the rapidly growing need for security professionals in Canada and predicts that the demand for cybersecurity professional is growing by seven percent annually. The report also alerts that the lack of qualified professionals could slow down the pace of technology innovation. The aim of the proposed online graduate certificate program is to address this need by producing trained professionals for the cybersecurity industry. This is a very timely move by the McGill University, and I am confident that this online graduate certificate program will allow professionals to develop the required skillsets and thus solve the skill mismatch problem of the current job market. The program being online will also attract many national and international students.

I have seen the proposed curriculum of the program, and it covers all the essential topics in cybersecurity including cryptography, network security, malicious software, and cybersecurity standards. Given my experience of teaching three security-related courses at UofM, I can assure

that the proposed curriculum will also prepare students for pursuing further research and academic studies. If this program is approved, I will consider recruiting graduates from the certificate program to be graduate students at the University of Manitoba. I will also seek local and international collaborations to facilitate internship opportunities for the students.

Finally, I believe that this proposed online graduate program is a timely initiative by the McGill University, and I strongly support this program.

Yours sincerely,



Noman Mohammed

جامعة زايد
ZAYED UNIVERSITY

ZUCTI
كلية الابتكار التقني
COLLEGE OF TECHNOLOGICAL INNOVATION

December 18, 2018.

To Whom It May Concern:

I am writing to support McGill University to develop an online graduate certificate program in Cyber Security. I hold the position of Associate Professor in the College of Technological Innovation, Zayed University, United Arab Emirates. My research interests include information security, digital forensics, data science, and privacy and trust.

As the severity and frequency of cyber attacks continue to grow, there is a pressing need of cyber security professionals and technicians in the international job market, spanning across multiple sectors including telecommunications, finance, healthcare, transportations, government agencies, etc. I have reviewed the proposal of the certificate program. It consists of five cyber security courses that cover the security issues in each layer of a typical information system. The program is suitable for IT professionals who would like to further strengthen their knowledge and skills in the cyber security. The proposed program is on the right tack to address the need of cyber security professionals and technicians in the job market.

Should you require further information, I can be reached at Farkhund.Iqbal@zu.ac.ae.

Thank you.

Yours sincerely,

Farkhund Iqbal
Associate Professor, College of Technological Innovation
Zayed University, UAE