Are you looking for a Career in Cybersecurity?

Digital technologies are now an integral part of our daily lives, however, their use also opens us up to various threats as large amounts of confidential information is being collected and processed in organizations, governments, financial institutions, universities, the transportation sector, the energy sector and, in other businesses and industries. With persistent hackings, data breaches, and cyber-attacks on industries globally, the demand for cybersecurity expertise is on the rise across all industries. Better understanding of security and appropriate strategies are required to protect and reduce financial and reputation losses as these pose threats to Canada’s economic well-being and that of the world at large. There will therefore be a critical need for qualified individuals trained in cybersecurity to protect digital assets and guard intellectual property. The New York Times and other sources report that there will be approximately 3.5 million unfilled cybersecurity jobs globally by 2021. Research from Deloitte shows a lack of talent is being felt across corporate Canada, and they expect that organizations across Canada will need to fill an estimated 8,000 additional cybersecurity positions by 2021. This undergraduate Certificate program is designed to address the industry's increasing and urgent demand for well-educated security professionals in both the public and private sector.

This online program is designed to develop the skillset and competencies necessary for cybersecurity personnel. These include a solid foundation in theory and practical experience in IT networking and secure network infrastructures designed to anticipate and protect against cyber threats, fraud, data breaches and other vulnerabilities. The program provides students with a strong background in cybersecurity and prepares them for the designation of Security Certified Practitioner (SSCP), Certified Information Systems Security Professional (CISSP), and Certified Information Security Manager (CISM), provided that students meet the work experience requirement and pass the examination(s) offered by the corresponding designation organization.

Typical career opportunities include:

- Computer Security Specialist
- Cyber Security Consultant
- Security System Administrator
- Cyber Security Analyst
- Web Security Specialist
- Information Security Officer
- Cyber Security Investigator
- Penetration tester
- Incident Response Analyst
- Security Operations Centre Analyst
- I.T. Risk Analyst
- Incident and Threat Analyst
- Network Security Specialist
- I.T. Security Consultant
- Vulnerability Assessment Analyst
- Operations and Security Management Specialist
The Program

The Certificate in Applied Cybersecurity is a 30-credit program which consists of 10 required courses.

Classes are offered once a week for 13 weeks and are generally from 6 p.m. to 9 p.m. during the week. Courses can be taken in the Fall, Winter, and Summer sessions. Not all courses are offered every semester.

The certificate’s program requirements are:

10 Required courses (30 credits):

CCCS 300 Programming Techniques 1
CCCS 321 Operating Systems Administration
CCCS 431 Networking Fundamentals
CCCS 450 Access Control and Defence Methods
CCCS 451 Communication and Network Security
CCCS 452 Security Program Architecture and Engineering
CCCS 453 Security Risk Management and Governance
CCCS 454 Security Incident Response and Recovery
CCCS 455 Intrusion Testing and Security Assessment
CMIS 422 Information Systems Security

Learning Outcomes:
The Certificate in Applied Cybersecurity provides the theory and competencies required:

- To have a thorough technical review of cybersecurity issues
- To gain hands-on experience in tackling common threats
- To identify data threats and attacks
- To implement and administer security measures for organizations
- To apply protective measures with tools and techniques to a company’s technology and business operations
- To cover the critical knowledge domains required for examinations for the following security designations:
  - Certified Information Systems Security Professional (CISSP)
  - Systems Security Certified Practitioner (SSCP)
  - Certified Information Security Manager (CISM)
Course Sequence

Certificate in Applied Cybersecurity

- CCCS 300 Programming Techniques 1
  - Prerequisite: CCCS 431 Networking Fundamentals
  - Corequisite: CMIS 422 Information System Security

- CCCS 321 Operating Systems Administration
  - Prerequisite: CCCS 450 Access Control and Defence Methods
  - Corequisite: CCCS 451 Communication and Network Security

- CCCS 450 Access Control and Defence Methods

- CCCS 451 Communication and Network Security

- CCCS 452 Security Program Architecture and Engineering

- CCCS 453 Security Risk Management and Governance

- CCCS 454 Security Incident Response and Recovery

- CCCS 455 Intrusion Testing and Security Assessment

Note:
- \[\rightarrow\] Prerequisite for courses
- \[\bullet\bullet\] Corequisite for courses
## Course Descriptions

**CCCS 300 Programming Techniques 1**  
(3 credits)  
Pre-requisite: None  
Fundamental programming techniques, concepts, and data structures, including modularization and maintainability. Emphasis on facilitating communication and understanding between systems analysts and programmers to support decision-making.

**CCCS 321 Operating Systems Administration**  
(3 credits)  
Pre-requisite: None  
Operating systems such as Windows and LINUX/UNIX environments, administration of computer servers, usage of script languages and in various operating systems, back up procedures and remote access, communication protocol used among different systems, managing information, and system security.

**CCCS 431 Networking Fundamentals**  
(3 credits)  
Co-requisite: CCCS 300  
Fundamental concepts and practices of network principles, technical and managerial aspects of data communications, overview of local area and wide-area networks, network topology, network protocols, Internet/intranet, client/server communication and file sharing.

**CCCS 450 Access Control and Defence Methods**  
(3 credits)  
Pre-requisites: CCCS 300, CCCS 321, CCCS 431, CMIS 422  
Covers different authentication methods, identifies management, access controls implementation, attackers’ tactics and strategies, anomalous traffic detection, various types of hacking tools and prevention systems against attacks.

**CCCS 451 Communication and Network Security**  
(3 credits)  
Pre-requisites: CCCS 300, CCCS 321, CCCS 431, CMIS 422  
Provides an introduction to modern wireless communication and networking technology. Covers different approaches to secure the wireless networks, with necessary tools to adapt to the revolutionary change in mobile communications and networking.

**CCCS 452 Security Program Architecture and Engineering**  
(3 credits)  
Pre-requisites: CCCS 300, CCCS 321, CCCS 431, CMIS 422  
Covers the information security concepts of security models, engineering processes using secure design principles, assessing and mitigating vulnerabilities in systems, designing and implementing physical security.
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCCS 453</td>
<td>Security Risk Management and Governance</td>
<td>(3 credits)</td>
</tr>
<tr>
<td></td>
<td>Pre-requisites: CCCS 300, CCCS 321, CCCS 431, CMIS 422</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Covers ethical, legal and regulatory issues surrounding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cyber security so as to design networks and policies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>for security and compliance. Examine and manage cyber</td>
<td></td>
</tr>
<tr>
<td></td>
<td>security risks, threats, opportunities and vulnerabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>at the strategic and operational levels.</td>
<td></td>
</tr>
<tr>
<td>CCCS 454</td>
<td>Security Incident Response and Recovery</td>
<td>(3 credits)</td>
</tr>
<tr>
<td></td>
<td>Pre-requisites: CCCS 300, CCCS 321, CCCS 431, CMIS 422</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Covers the incident lifecycle, incident management plans,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>business continuity plans, disaster recovery plans that</td>
<td></td>
</tr>
<tr>
<td></td>
<td>are in place to identify, analyze and respond to attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and threats.</td>
<td></td>
</tr>
<tr>
<td>CCCS 455</td>
<td>Intrusion Testing and Security Assessment</td>
<td>(3 credits)</td>
</tr>
<tr>
<td></td>
<td>Pre-requisites: CCCS 300, CCCS 321, CCCS 431, CMIS 422</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Covers the fundamentals and tool set needed to discover</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and exploit system vulnerabilities, penetrate organization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>infrastructure; tools and hacking techniques used in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cyber-attacks, and planning intrusion tests.</td>
<td></td>
</tr>
<tr>
<td>CMIS 422</td>
<td>Information Systems Security</td>
<td>(3 credits)</td>
</tr>
<tr>
<td></td>
<td>Co-requisite: CCCS 300</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fundamental concepts relating to the design of secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>information systems. Identification and assessment of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>security risks and the application, network, and physical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>levels. Use of cryptography and other techniques to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>provide necessary level of security.</td>
<td></td>
</tr>
</tbody>
</table>
Admission Requirements

To be admitted to an Undergraduate Certificate in Applied Cybersecurity:

- Applicants must hold a CEGEP diploma (DCS, DEC or equivalent) OR
- Applicants who do not have the normal academic background for admission but are 21 years of age and older may be admitted as mature students OR
- Applicants between 18 and 21 years of age who do not have a CEGEP diploma but have at least a high school leaving certificate may be accepted into a qualifying program (a copy of the certificate must be provided).
Admission Procedures

STEP 1: PREPARE
1. Choose the program (certificate, diploma, graduate certificate or graduate diploma) you would like to apply to.
2. Verify the Application Deadlines to ensure that you submit your application in time.
3. Ensure you have a valid email address and credit card on hand to pay for the application fee (Visa, Master Card or America Express).
4. From the list of programs, click on the program you would like to apply to.
5. Review the admission requirements for the program to ensure you meet the criteria.
6. Ensure you have all necessary documentations required for your application as indicated in the “Documents Required” section.

STEP 2: APPLY
1. Click “Apply Now” at the top of the program page or go to https://mcgill.ca/x/4Um and click “Apply Now”.
2. If you have a Login ID and PIN, enter them now, or if not, create one and log in.
3. Click on “Begin New”.
4. Enter the information requested and click “Continue”.
5. When asked, “What are you applying for at McGill?”, click on “Continuing Studies”.
6. On the next page, select the program you would like to apply to.
7. Complete the rest of the application with all required information and submit.
8. You will receive a confirmation email providing you with a McGill ID number and a PIN. Within 24-48 hours, you will be able to log in to Minerva (www.mcgill.ca/minerva).

STEP 3: UPLOAD SUPPORTING DOCUMENTS
Once you have access to Minerva, upload your supporting documentation as per the admission requirements of your chosen program.

- Uploading your documents will speed up your application process and is strongly recommended.

- For instructions on how to proceed, please go to: https://mcgill.ca/continuingstudies/legal-documents.

(If you are unable to upload the documents, you can send them by regular mail or bring them in person to our Client Services office at the address below).

- Sending official transcripts: All transcripts received via the upload process are considered unofficial. If transcripts are required for your application, you will also need to have any official transcripts sent directly to McGill University by mail, in a sealed envelope by the educational institution(s) where you studied.

STEP 4: VERIFY ADMISSION STATUS
Once a decision has been made, admitted students will receive a “Letter of Admission” along with registration instructions.

Difficulty Applying Online?
If you have any problems with your online application, or if you have questions regarding admission requirement and procedures, contact Client Services (https://www.mcgill.ca/continuingstudies/client-services).
Helpful Tips for Applying

What is an Official Transcript?
If you have studied at an institution:
- In Canada or the United States – you will need to request a copy of your official transcripts (your marks) from that institution which the institution will mail to the address below in a sealed envelope with the official institution’s logo.
- Outside of Canada or the United States, - you will need to request a copy of your official transcripts (your marks) from that institution which the institution will mail to the address below in a sealed envelope with the official institution’s logo.
- Note: In cases where the language of instruction at the institution is not English or French, you must also send an official translation of the official transcript certified by a representative from the Ordre des traducteurs, terminologues et interprètes agréés du Québec (OTTIAQ - http://ottiaq.org/).
- You need to request official transcripts as soon as possible once your application has been submitted to the School of Continuing Studies. Your Educational Institution must then mail these directly to the appropriate office below:

Client Services c/o Admissions
McGill University – School of Continuing Studies
688 Sherbrooke Street West, Room 1125
Montreal, QC H3A 3R1
Canada

• Important: You must make sure you apply by the application deadline. However, if you have any outstanding supporting documents at the time of your application, you may upload them as they become available or forward them directly to the School of Continuing Studies as soon as possible. Your admission application will only be completed once the University has received all of the required documents.

• Note: All required documents received by McGill University’s School of Continuing Studies become the property of the university. Official documents and/or transcripts will not be returned to the applicant.

• Note: Transcripts received by McGill University’s School of Continuing Studies cannot be transferred to any other department or program as it would constitute submitting a new application. Therefore, you must submit a new sealed envelope of your official transcripts for each application made to McGill University’s School of Continuing Studies.
Language Requirements

- The language of instruction for most courses and programs at McGill University is English; however, students may submit any written work that is to be graded in English or French, except in cases where knowledge of the language is one of the objectives of the course.

- Applicants must demonstrate an adequate level of proficiency in English prior to admission, regardless of citizenship status or country of origin. McGill University has this language requirement in place to ensure that all students are provided with the opportunity to succeed in their chosen program.

- In all cases, the University reserves the right to require proof of English proficiency if it is deemed necessary. For additional information, please click on the link below.

https://www.mcgill.ca/continuingstudies/language-policy

Exemption by Examination

Students admitted to a Certificate, Diploma, Graduate Certificate or Graduate Diploma program requiring a pre-requisite or co-requisite course, must provide proof that they have taken and successfully passed an equivalent 3-credit course, with the requisite grade as per McGill University’s requirements, at the appropriate level at another approved institution or have successfully completed the Exemption by Examination test.

- The Exemption by Examination test is not applicable to required or complementary course(s) within a program.

- You cannot take the Exemption by Examination test if you have already attempted the course (a grade of W is considered as have attempted the course).

- If you are unsuccessful in the Exemption by Examination test(s) you will not be permitted to repeat the test(s) and must instead enroll in the course(s) for which the particular test(s) was taken.

To be eligible to write the Exemption by Examination test, you must have applied to or been admitted into a program. (The test is optional).

For more information visit: https://www.mcgill.ca/continuingstudies/recognition-prior-learning
Student Awards and Financial Aid

**McGill University’s School of Continuing Studies Bursaries**
The School of Continuing Studies will post the application form and eligibility requirements for the active term on its website. Please refer to link below for further information.


**McGill University’s School of Continuing Studies Scholarships**
For a list of McGill University Scholarships, please consult McGill University’s School of Continuing Studies website by clicking on the link below.


**McGill University’s School of Continuing Studies Graduating Prizes**
For a list of McGill SCS Graduating Prizes, please consult McGill University’s School of Continuing Studies website by clicking on the link below.

[https://www.mcgill.ca/continuingstudies/graduating-students](https://www.mcgill.ca/continuingstudies/graduating-students)

**Aide financière aux études (AFE)**
As a credit-bearing program, this program is eligible for financial aid through the Quebec Government.

[https://www.quebec.ca/education/aide-financiere-aux-etudes/](https://www.quebec.ca/education/aide-financiere-aux-etudes/)

Note: The amount and number of McGill University’s School of Continuing Studies Bursaries, Scholarships, and Graduating Prizes issued varies from year to year, depending on funds received and their specifications.

Contact

McGill University
School of Continuing Studies

688, Sherbrooke St. West, Suite 1140
Montreal, QC, H3A 3R1

**Program information**

Tel. 514-398-6200
Fax: 514-398-2650

[info.conted@mcgill.ca](mailto:info.conted@mcgill.ca)