Cybersecurity

PROGRAM INFORMATION

Academic Year	2024 – 2025
Credential	Graduate Certificate
Program Delivery	Full - Time
Length	4 Semesters
Program Code	T200 – Timmins Campus

DESCRIPTION

This program is currently open to International Students only.

This 2-year Ontario College Graduate Certificate in Cybersecurity prepares graduates to take on exciting and challenging positions within organizations that increasingly have realized their need to secure information. This program takes a hands-on approach through lab activities, project work, and case study analysis.

The program combines technical skill-building on topics that include ethical hacking, network security, incident response, forensics, and cloud security.

This curriculum will further broaden students' leadership skills in the areas of risk analysis, vulnerability management, and cybersecurity law and ethics. Students will also gain real-world experience through a co-operative education work term.

Upon completion of the program, students will be able to efficiently manage security in an organization through the application of cybersecurity controls designed to identify, protect, detect, respond, and recover. Graduates will also be prepared to attain certifications including CompTIA Security+ and PenTest+, (ISC)² SSCP, and EC-Council's CEH.

CAREER OPPORTUNITIES

- Cybersecurity specialist
- Employed in IT consulting firms and IT units in the private and public sectors.

VOCATIONAL LEARNING OUTCOMES

1. Identify cybersecurity risks based on organizational strategies to manage risk assessment processes.
2. Plan and implement vulnerability and penetration testing to identify, exploit, and correct weaknesses in an organization's infrastructure.
3. Recommend security controls for the maintenance and deployment of cyber security solutions to protect systems and information.
4. Implement technical measures to identify cybersecurity incidents and their potential impact to verify that appropriate protections are in place.
5. Plan, implement, and evaluate cybersecurity policies and procedures to improve the effectiveness of an organizational information security program.

6. Design and develop effective cybersecurity awareness and training resources for employees to reduce risk of a breach or other cyber incidents.
7. Communicate cybersecurity policies and risk management expectations to internal and external stakeholders in order to support business objectives.
8. Plan and conduct disaster recovery, forensic investigations, and incident responses to support organizational business continuity.
9. Use project management tools to implement information security strategies within scope and within timelines.

PROGRAM COURSES

The following reflects the planned course sequence for full-time offerings of the program. Programs at Northern College are delivered using a variety of instruction modes. Courses may be offered in the classroom or lab, entirely online, or in a hybrid mode which combines classroom sessions with virtual learning activities.

Semester 1		**Hours**
CS1004	Windows Server Fundamentals	56
CS1014	Information Security Fundamentals	56
CS1024	Linux Server Fundamentals	56
CS1034	Networking Fundamentals	56
CS1044	Scripting Fundamentals	56
Semester 2		
CS2004	Cloud Security	56
CS2014	Cybersecurity Risk Management	56
CS2024	Ethical Hacking	56
CS2034	Digital Forensics	56
CS2044	Intrusion Detection and Prevention	56
Semester 3		
CS3003	Work Experience Preparation	42
CS3004	Cybersecurity Law and Ethics	56
CS3014	Vulnerability Management Fundamentals	56
CS3024	Network Forensics and Incident Response	56
CS3034	Network Security Fundamentals	56
CS3044	Security Operations Centre Fundamentals	56
Semester 4		
CS4008	Cybersecurity Work Term/Capstone	392

Cybersecurity

PROGRAM PROGRESSION

The following reflects the planned progression for full-time offerings of the program.

Fall Intake
Sem 1: Fall 2024
Sem 2: Winter 2025

WORK INTEGRATED LEARNING OPPORTUNITIES

N/A

ARTICULATION/TRANSFER AGREEMENTS

A number of articulation agreements have been negotiated with universities and other institutions across Canada, North America and internationally. These agreements are assessed, revised and updated on a regular basis. Please contact the program coordinator for specific details if you are interested in pursuing such an option. Additional information can be found at Articulation Agreements.

ADDITIONAL INFORMATION

N/A

PROGRAM SPECIFIC INFORMATION

N/A

ADMISSION REQUIREMENTS

Ontario College Diploma, Ontario College Advanced Diploma, Degree, or equivalent in Information Technology or Computer Studies.

Additional Requirements for International Students

In addition to the general admission requirements, international students must have proof of English Proficiency and meet the requirements below.

English Proficiency (we will require one of the following):

Applicants possessing degrees/diplomas from institutions where the language of instruction was not English will be required to provide test scores as evidence of their English language proficiency.

- IELTS Academic International English Language Testing System: a minimum overall score of 6.0 must be achieved with no individual band score under 6.0.

- TOEFL (Test of English as a Foreign Language) – Internet Based Test (iBT) overall minimum score of 80+
- PTE (Pearson Test of English) Academic – Graduate Diploma: 60+

All educational documents must be submitted in English and will be dependent on the country of citizenship. For more information, please contact admissions@northern.on.ca.

GRADUATION REQUIREMENTS

17 Program Courses

GRADUATION ELIGIBILITY

To graduate from this program, a student must attain a minimum of 60% or a letter grade of CR (Credit) in each course in each semester unless otherwise stated on the course outline. Students should consult departmental policies and manuals for additional detail and exceptions.

GRADUATION WINDOW

Students unable to adhere to the program duration of two years (as stated above) may take a maximum of four years to complete their credential. After this time, students must be re-admitted into the program, and follow the curriculum in place at the time of re-admission.

CONTACT INFORMATION

For questions about being admitted into the program, please contact Northern College Admissions at admissions@northern.on.ca or by phone at 705-235-3211 ext. 7222. For questions about the content of the program, contact the Program Coordinator.

David Goldstein, Program Coordinator
Email: goldsteind@northern.on.ca

Cybersecurity

COURSE DESCRIPTIONS

Semester 1

CS1004 – Windows Server Fundamentals
Students will learn about the installation, storage requirements, and features and functionality of Windows Server, including server administration.

CS1014 – Information Security Fundamentals
Students will explore contemporary risks and threats within a Canadian context to an organization's sensitive data and strategies to use to safeguard these assets. Successful completion of this course will prepare students for an optional CompTIA Security+ certification.

CS1024 – Linux Server Fundamentals
In this course, students will learn fundamental concepts of system administration using modern Linux operating system implementations. Successful completion of the course will prepare students for an optional CompTIA Linux+ certification.

CS1034 – Networking Fundamentals
Students will explore computer and communication technologies within Canada including transmission concepts, network hardware and software, and standards and protocols. The course relates these concepts to other areas of information technology and prepares students for the optional CompTIA Network+ certification.

CS1044 – Scripting Fundamentals
In this course, students will be provided with an introduction to scripting languages, such as Python, including data types, control structures, and regular expressions in the context of cybersecurity applications.

Semester 2

CS2004 Cloud Security
This course introduces students to the concepts of cloud security, including security governance using cloud technologies, security principles and controls, and secure cloud architecture.

CS2014 Cybersecurity Risk Management
This course covers the management of information security risks, including assessing and analyzing threats to the organization. Students will learn how to use a risk registrar and develop and implement a risk treatment plan.

CS2024 Ethical Hacking
Students will examine the methodology used within a Canadian framework for ethical hacking using a practical application of security tools. Mitigation strategies are also covered, including countermeasures to reduce the risk of an attack.

CS2034 Digital Forensics
In this course, students will learn the technical aspects of digital forensics, including forensic procedures, imaging, hashing, file recovery and reporting. Digital forensic software tools are also introduced so students can learn how to conduct forensic examinations for themselves.

CS2044 Intrusion Detection and Prevention
In this course, students will learn how to design, implement, and administer intrusion detection and prevention systems. Various attack signatures and network traffic are analyzed to better understand threats to the organization.

Semester 3

CS3003 Work Experience Preparation
The purpose of this course is for students to enhance their career planning skills and apply these skills to prepare for work placement effectively. Skills like cover letter and resume development, job search, researching, networking, letter writing and interviewing will be developed and practiced. Additionally, students will focus on ‘‘soft” skills such as self-awareness, goal setting, interpersonal communication, personal presentation, and business etiquette. Active participation will be required as students learn experientially, collaboratively, and cooperatively in class and online.

CS3004 Cybersecurity Law and Ethics
Students will explore the issues of Canadian law and ethics of the Internet, including regulations of online behaviour, intellectual property, hacking and ethical behaviour. Practical examples of laws concerning security breaches and corresponding responses to these reaches will be discussed.

CS3014 Vulnerability Management Fundamentals
In this course, students will learn about information security vulnerability assessment fundamentals, practical analyses of threat intelligence, and automation and modeling with the overall goal of implementing successful organizational security vulnerability assessment programs within a Canadian context.

CS3024 Network Forensics and Incident Response
In this course, students will learn about security incidents, how to identify and categorize them, appropriate incident responses, and how to work with security information and event management systems (SIEMs).

CS3034 Network Security Fundamentals
In this course, students will learn the security principles needed to secure a network including developing a network infrastructure, understanding core security concepts, managing secure access, VPN, cryptography, firewalls, web and email content security, and endpoint security.

CS3044 Security Operations Centre Fundamentals
This course introduces students to security operation centres (SOCs) within Canada and the various roles and responsibilities required to support these centres. Students will learn fundamental requirements of SOCs, including how to map networks, scan systems for vulnerabilities, and monitor infrastructure for signs of an attack.

Cybersecurity

Semester 4

CS4008 Cybersecurity Work Term/Capstone
In this semester, students will apply their skills in cybersecurity in a Canadian work environment or complete an applied capstone project. The applied project will enable students to work on Canadian industry-relevant challenges to further demonstrate their skills and knowledge in cybersecurity and prepare for employment.