OntarioTech UNIVERSITY

**Academic Council**
**Graduate Studies Committee**
October 22, 2024
9:00 a.m. – 11:00 a.m.

Via Google Meet
Join: https://meet.google.com/cqx-oqam-fad
Or dial: (CA) +1 778-746-8746 PIN: 209 917 155#

**All Meeting Materials :**
**Graduate Studies Committee Agenda and Minutes 2024-2025**

## AGENDA

**Call to Order and Land Acknowledgement**

1. **Approval of the Agenda** — **C. Cesaroni**

2. **Approval of the Minutes of the Meeting of September 24, 2024*(M)** — **C. Cesaroni**

3. **Business Arising from the Minutes** — **C. Cesaroni**

4. **Comments from the Chair** — **C. Cesaroni**

5. **New Program Proposal – Faculty of Business and IT, PhD Cybersecurity* (M)** — **S. Heydari /C. McGregor**

6. **Faculty Reports**
   a) **Faculty Reports**
   b) **Graduate Student Report**
   c) **Library Report**

7. **For Information:**

   **7.1 2024-2025 Revisions to the Graduate Academic Schedule***
   **7.2 2024-2025 Draft GSC Work Plan***
   **7.3 Associate Graduate faculty: Appointments**

- Materials Science, Rachel Wortis, Faculty of Science
- Materials Science, Aaron Slepkov, Faculty of Science
- Materials Science, Balaji Subramanian, Faculty of Science
- Materials Science, Andrew Vregenhil, Faculty of Science
- Materials Science, Carlo Bradac, Faculty of Science
- Materials Science, Rayf Shiell, Faculty of Science
- Materials Science, Bill Atkinson, Faculty of Science
- Applied Bioscience, Peter Lewis, Faculty of Business and Information Technology
- Computer Science, Eric Rapos, Faculty of Science
- Computer Science, Nicholas Provart, Faculty of Science

8. **Call for Volunteer for Land Acknowledgement for November Meeting**

9. **Termination**

10. **Colleagues Exchange**
    - Thesis-Based Admission
    - Mental Health Support Seminar – November. 7, 2024

**Academic Council Graduate Studies Committee**
**Tuesday, September 24, 2024**
**9:00 a.m. – 10:27 a.m.**

Via Google Meet

All Meeting Materials
GSC Agenda – September 24, 2024

**MINUTES**

**Present**: P. Mirza Babei, (Chair), J. Abbas Dick, J. Arcand, R, Bailey, D. Bonetta, C. Cesaroni, A. Cooper, C. Davidson, K. Elgazzar, F. Gaspari, L. Harkins, S. Jackson, H. MacPherson, O. Marques, D. Papke, F. Quereshi, A. Tokuhiro, R. Van Oostveen, N. Wattie, K. Wilson, A. Wingate

**Staff & Guests**: K. Ayotte (secretary), S. Baglay, N. Crow, M. Heslip, A. Kassaris, K. McCartney, S. Windsor,

**Regrets:** K. Clarke, A. Kiani, L. Livingston, S. Marsh, A. Slane, J. Stokes,

**Chair P. Mirza Babaei called the meeting to order at 9:00am.**
S. Windsor read aloud the Land Acknowledgement.

1. **Approval of the Agenda**
   *Upon a motion duly made by F. Gaspari and seconded by J. Arcand, the agenda was approved as presented.*

2. **Approval of the minutes of the Meeting of June 25, 2024**
   *Upon a motion duly made by L. Harkins and seconded by C. Cesaroni, the Minutes were approved as presented.*

3. **Business Arising from the Minutes**
   None.

4. **Comments from the Chair**
   P. Mirza-Babaei welcomed returning and new committee members, including Nicola Crow, Amanda Cooper, Ken Wilson, Krystina Clarke, and Acting Dean Joe Stokes, and expressed gratitude to former Dean Ted Christou. He noted that GSC Charing responsibilities will be shared between the SGPS Associate Deans during the transition. He then highlighted key items from his written report, including approximately 1,000 graduate students with 300 new students, as well as the September orientation attended by 250 students. He mentioned the upcoming Research Poster Showcase in November and C. Cesaroni added that the showcase will be hosted by the Downtown Campus aiming to help students develop presentation skills and encourage participation.
   S. Windsor and C. Cesaroni also discussed an upcoming panel from the Supervisor Series that

will focus on mental health and wellness. It will address common concerns raised by supervisors and faculty, creating an interactive session that discusses mental health, emphasizing self-care and wellness strategies that will go beyond generic data, and focus on real-life case studies involving student scenarios. The goal  is to provide practical guidance, identifying when to seek support and understanding boundaries for faculty involvement. Additional communication will be provided shortly.

Responding to a question regarding changing the date for the Research Poster Showcase, C. Cesaroni acknowledged the timing, but indicated that no matter what date was considered, there was a conflict.

P. Mirza-Babaei announced tuition deposit waivers for International research students are now being processed manually, with integration into the admissions system pending. H. MacPherson added that typically, students are required to pay a $2000.00 non-refundable deposit when accepting their offer. However, this fee can be waived for research-funded students or course-based students with visa issues preventing their arrival for their intake semester, but the request must be submitted manually to SGPS for now. She noted that further information will be available on the SGPS website once available.

P. Mirza-Babaei also noted upcoming changes to Government policies on International student admissions, with further information pending from the Federal Government. In response to questions regarding the 10% change and International caps, P. Mirza-Babaei reiterated that the information from the Government is pending, and the University will update once more information received.

P. Mirza-Babaei concluded the Chair's Comments by expressing his gratitude to SGPS team the program directors and coordinators across all faculties for their dedication in supporting both our students and colleagues.

## 5. Major Program Modification

### 5.1 Faculty of Health Science – Master of Health Science (M)

N. Wattie presented the Master of Health Science Major Program Modification noting that the changes stem from the recent cyclical program review and faculty consultations aimed at modernizing the curriculum and attracting a broader student base. Key modifications include removing redundant core courses, adjusting the number of required electives, and introducing new core courses. Additionally, the independent project-based option will transition to a capstone course format within a broader course-based option for each field. These updates are intended to enhance the program's appeal and increase enrollment, particularly in the Kinesiology and Public Health fields.

He confirmed that there will be no changes to the total credit hours required for the Community Public Health field, but there will be a reduction in credit hours for the Kinesiology and Health field aligning with recommendations also stemming from the cyclical review and environmental scan of similar programs in Ontario.

In response to a question, N. Wattie confirmed that students starting in Fall 2024 can transition to the new program map, and that the department will be communicating these changes.

**Motion:**
*Upon a motion duly made by J. Arcand and seconded by K. Elgazzar, the Governance & Nominations Committee hereby recommends to Academic Council the approval of the Major Program Modification to the Master of Health Science Program.*

6. **Academic Policy Instruments**

   **6.1 Duolingo Policy (M)**
   H. Macpherson presented a proposal to accept Duolingo English testing on a one-year trial basis as a recommendation rather than a full policy change. She proposed an amendment to correct the required scores for MBA, MITS, and MFDA programs to 120 instead of 130, noting Health Science and Education programs will keep the 130 requirements. She advised that the Duolingo test costs approximately $150 and provides results within 48 hours and is accepted by many Universities. Concerns were raised that other top institutions do not accept Duolingo, potentially harming the University's brand, and that the cost savings are minimal compared to overall student expenses. H. Macpherson emphasized that the use of Duolingo English testing was for a one year trial and provided an overview of the considerations taken into account in deciding on Duolingo English testing for this trial.

   Members suggested enhancing English proficiency requirements for TAs through workshops and testing, aligning with other Universities' practices. It was proposed to separate TA language proficiency from general admission requirements. There was also a suggestion to limit the one-year Duolingo trial to non-thesis or shorter-term students to reduce long-term impact if unsuccessful. Discussion also took place on how the trial would be evaluated.

   K. Elgazzar requested an amendment to ensure the trial is restricted to non-thesis-based students.

**Motion:**
*Upon a motion duly made by N. Wattie, and seconded by R. Bailey, the Graduate Studies Committee herby recommends to Academic Council, the approval of the Duolingo English Test from applicants of non-thesis-based programs as sufficient evidence of English language proficiency for a trial period of 2024-2025 admissions cycle, as amended.*

*The following are the recommended scores for Graduate Programs:*

- *Health Sciences (MHSc), Education (MA, Med, EdD) – Minimum score of 130*
- *All other graduate programs – Minimum score of 120*

7. **Reports**
   i. Faculty of Business and IT
      - Enrollment numbers saw an increase this year and an additional welcome session was scheduled.

   ii. Faculty of Engineering and Applied Science
      - Discussion regarding PhD applicants whose undergraduate degrees do not qualify for a corresponding master's program should be ineligible for admission, reflecting practices at other Canadian institutions.
      - Current minimum funding levels are insufficient to cover tuition costs, leading to poor academic performance. Ongoing discussions consider increasing funding to better support students, though no decisions have been made yet.

   iii. Mitch and Leslie Frazer Faculty of Education
      - Nothing to Report

   iv. Faculty of Health Science
      - Efforts are underway to enhance orientation and onboarding processes for MHSc and PhD students, including progress reports from day one and clear TA responsibilities.
      - Discussions in the initial stages about potentially introducing a new field in the MHSc program focused on Medical Laboratory Sciences, with a target launch of Fall 2026

v. Faculty of Science
   - The Materials Science program is currently undergoing a cyclical review, with the documentation nearly complete and setting up timelines for the external visit and presentation to Faculty Council. The goal is to present the review in October, but if delays occur, November will be the latest. This review is being conducted in collaboration with Trent University, which has added some additional time due to the coordination required between the two institutions.
   - Computer Science program reported 75 graduate students (61 full-time, 14 part-time) and 96 full-time faculty members, plus 81 Associates. The course offering challenges facing the program were noted with  and noting the challenges it faces with course offerings with only seven courses in the fall and five planned for winter, missing key areas like software design and IT security. The need for Senior Leadership support was stressed.
   - Applied Bioscience reported that they are currently in the process of conducting their program review as well as attempting to enhance the structure of student feedback reports to allow for more adequate communication from the faculty.

vi. Faculty of Social Science and Humanities
   - See submitted written report.

vii. Graduate Student Report
   - No update

viii. Library Report
   - See submitted written report.

## 8. For Information

**Associate Graduate Faculty**

- Health Sciences, Mary Chiu, Faculty of Health Science
- Health Sciences, Stephen Hwang, Faculty of Health Science
- Health Sciences, Stephanie Felder, Faculty of Health Science
- Health Sciences, Jim Potvin, Faculty of Health Science
- Health Sciences, Lavern Bourne, Faculty of Health Science
- Health Sciences, Silvano Mior, Faculty of Health Science
- Health Sciences, Edward Osborn, Faculty of Health Science
- Health Sciences, Alvaro Joffre Uribe Quevedo, Faculty of Business and Information Technology
- Applied Bioscience, Marc Adler, Faculty of Science
- Computer Science, David Chandross, Faculty of Business and Information Technology
- Computer Science, Abdulaziz Almehmadi, Faculty of Business and Information Technology
- Information Technology Security, Abdulaziz Almehmadi, Faculty of Business and Information Technology
- Information Technology Security, Bernadette Schell, Faculty of Business and Information Technology
- Electrical and Computer Engineering, Peter Lewis, Faculty of Business and Information Technology
- Software Engineering, Peter Lewis, Faculty of Business and Information Technology
- Education, Bill Walters, Faculty of Education
- Nuclear Engineering, Rami El-Emam, Faculty of Engineering and Applied Science

**Graduate Faculty**

- Computer Science, Cristiano Politowski, Faculty of Science

## 9. Other Business

H. Macpherson volunteered to provide the October Land Acknowledgement and C. Davidson volunteered to provide the November Land Acknowledgement.

K. Elgazzar proposed a topic for the next colleagues exchange to discuss faculty endorsements for each application before it goes to a supervisor to provide better insight and help prevent the hiring of unqualified candidates, especially for supervisors with less experience. He recommended that the Committee consider striking a sub-committee for this purpose.
L. Harkins inquired about the attendance of the Acting Dean at upcoming meetings. P. Mirza-Babaei confirmed that J. Stokes is invited to join, however, the current arrangement is for GSC Chairing to be done by SGPS Associate Deans, they will lead the discussions and provide updates to the Acting Dean. L. Harkins expressed concern about the indirect communication of issues, preferring direct involvement.

Termination

*There being no other business, upon a motion duly made by S. Jackson the meeting adjourned at 10:27 a.m.*

Kirstie Ayotte, Assistant University Secretary

# Graduate Studies Committee

## Report of the Dean
## School of Graduate and Postdoctoral Studies

## Land Acknowledgement

*Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.*

*We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.*

*This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.*

## Chair's Remarks – October 2024

## SGPS Updates and Events

### 2024 SGPS Research Poster Showcase

The School of Graduate and Postdoctoral Studies (SGPS) is excited to present the SGPS Research Poster Showcase, Ontario Tech's annual graduate student and postdoc research poster session. It provides all graduate students and postdoctoral fellows with an exciting opportunity to present their research or academic work to a broad audience in an engaging and visually impactful format. Participants will create and display posters that communicate their research findings, methodologies, and significance to a diverse group of judges and attendees. This competition encourages students to distill complex ideas into clear and accessible visual presentations, making their research understandable to both specialists and non-specialists alike.

The showcase event will be held on Wednesday, November 27 from 5-7 p.m. at Charles Hall.

The deadline for applications has been extended to October 24 and we have currently received 37 applications.

### Mental Health and Wellness: Resources for Graduate Faculty Seminar

In recognition of World Mental Health Day, the Supervisor Series is hosting a panel discussion in collaboration with the Student Mental Health Services and Wellness at Work teams.

Graduate students often juggle competing priorities, leading to complex situations that have the potential to affect their mental health. Our graduate faculty members have asked for guidance, tools, and resources to better support their students. This session will provide an opportunity for colleagues to share strategies for both student support and their own self-care.

The 90-minute virtual session will be held on Thursday, November 7, 2024, at 11 a.m., moderated by Shelly Windsor, Graduate Academic Affairs Specialist, School of Graduate and Postdoctoral Studies, and Dr. Carla Cesaroni, Associate Dean, School of Graduate and Postdoctoral Studies. Ways to support graduate student mental health, faculty self-care, and wellness strategies will be explored, followed by an opportunity for an open, in-depth discussion.

Register here for the virtual session.

### Graduate Studies Networking and Information Session

Current 3rd, 4th and 5th year undergrads with a GPA of 2.7 or higher have been invited to attend this event to learn about graduate programs, interact with faculty members and connect with current graduate student and the School of Graduate and Postdoctoral studies staff. Information will be provided on specific research opportunities, professional programs and application processes in an informal, supportive environment.

This session will be held on Wednesday, October 30 from 4:00 to 6:00 p.m., in the UB Mezzanine.

### Recruitment Discussions

Carla and Pejman will be scheduling meetings with faculty GPD's to discuss recruitment, what is currently being done, and how SGPS can support these initiatives.

## Scholarship Updates

**Vanier** nominations (1 NSERC and 1 SSHRC) are being put forward on October 30th.

**CGS-D Doctoral** nominations have been received and the selection process is underway.

## Grad Pro Skills and Graduate Engagement

### Grad Pro Skills

- Starting off Strong: Library Resources 101 (October 3rd)
- Networking with Professionalism (October 18)
- Paragraphing & Summarizing (October 23)
- Upgrade your Cover Letter & Resume (October 25)

### Graduate Engagement

- Hackathon/Ideathon for Fusion Energy with Brilliant Catalyst, the Strategic partnership office, and Canadian Nuclear Laboratory (October 9, 10, 11)

## Graduate Student and Postdoc Celebrations!

The following students submitted their final thesis packages and successfully completed their program during the past month:

Student: Manraj Ladhar
Program: MASc in Electrical and Computer Engineering

Thesis Title: Signal and Power Integrity Analysis of Bidirectional DC-DC Converters for Hybrid Energy Storage Systems with EMI/EMC Optimization
Supervisor: Sheldon Williamson
Faculty: Engineering and Applied Science
Completed: September 19, 2024

Student: Ahmed Jafri
Program: MASc in Mechanical Engineering
Thesis Title: Experimental Investigation of Building Envelope and Air Source Heat Pumps in Canadian Cold Climate
Supervisor: Martin Agelin-Chaab & Horia Hangan
Faculty: Engineering and Applied Science
Completed: September 19, 2024

Student: Suben Shiam
Program: MASc in Mechanical Engineering
Thesis Title: PRODUCING TRANSITION METAL OXIDES AS CATHODES FOR AQUEOUSZINC-ION BATTERIES VIA ULTRA-SHORT LASER PULSES FOR IN-SITUNANOSTRUCTURE GENERATION (ULPING) Generation (ULPING)
Supervisor: Amirkianoosh Kiani
Faculty: Engineering and Applied Science
Completed: September 20, 2024

Student: Volletta Peters
Program: PhD in Health Sciences
Thesis Title: Exploring the Lived Experience of Aging Among Older Adults Who Are Chronically Homeless
Supervisor: Winnie Sun
Faculty: Health Sciences
Completed: September 26, 2024

Student: Jeonggi Son
Program: MASc in Electrical and Computer Engineering
Thesis Title: Enhanced Wireless Power Transfer System Modeling Using Reflection Theory and Magnetic Circuit Analysis
Supervisor: Sheldon Williamson
Faculty: Engineering and Applied Science
Completed: September 26, 2024

Student: Amit Maraj
Program: PhD in Computer Science
Thesis Title: Contextual Topics: Advancing Text Segmentation Through Pre-Trained Models And Contextual Keywords
Supervisor: Miguel Vargas Martin & Masoud Makrehchi
Faculty: Science
Completed: September 27, 2024

Student: Peter Kokkoros
Program: MA in Criminology
Thesis Title: Mothers of Children with Autism: Current Challenges and Intricate Dynamics Influencing the Quality of life and Mental Health of Mothers Caring for Children with Autism

Supervisor: Shahid Alvi
Faculty: Social Science and Humanities
Completed: September 27, 2024

Student: Aida Vatankhah
Program: PhD in Electrical and Computer Engineering
Thesis Title: QoS-Aware Energy Efficient Time-Slotted Channel Schedule for Heterogeneous IoT Sensor Networks
Supervisor: Ramiro Liscano
Faculty: Engineering and Applied Science
Completed: September 30, 2024

Student: Xiaolong Liu
Program: MASc in Electrical and Computer Engineering
Thesis Title: Development of an AI-Driven Robotic Manipulation Framework
Supervisor: Jing Ren & Haoxiang Lang
Faculty: Engineering and Applied Science
Completed: September 30, 2024

Student: Leanne Elliott
Program: PhD in Health Sciences
Thesis Title: Optimizing Training Designs and Elevating Reporting Standards in Simulation-Based Medical Education
Supervisor: Nick Wattie
Faculty: Health Sciences
Completed: September 30, 2024

# GRADUATE STUDIES COMMITTEE REPORT

**ACTION REQUESTED:**

| | |
|---|---|
| **Recommendation** | ☒ |
| **Decision** | ☐ |
| **Discussion/Direction** | ☐ |
| **Information** | ☐ |

**DATE: 22 October 2024**

**FROM: Faculty of Business and Information Technology**

**SUBJECT: New Program Proposal – Doctor of Philosophy - Cybersecurity**

**COMMITTEE MANDATE:**
In accordance with the Graduate Studies Committee (GSC) Terms of Reference, GSC has the responsibility "to examine proposals for new graduate degree and diploma programs" and "to recommend their approval, as appropriate, to the Academic Council".

**MOTION FOR CONSIDERATION:**
That GSC hereby recommends to Academic Council the approval of the PhD in Cybersecurity program and the subsequent recommendation of the program to the Board.

**BACKGROUND/CONTEXT & RATIONALE:**
The proposed PhD in Cybersecurity provides the highest-level degree of expertise in the broad area of Cybersecurity and will be a multidisciplinary research-intensive program that would cover a broad range of themes related to cybersecurity; including technology, policy and governance, AI and human behaviour, aiming to attract students from a variety of backgrounds and prior education, including computer science, information technology, business and management, social and political science.

The importance and emergence of the field of cybersecurity in today's world cannot be overstated, and its impact is no longer limited to technical (e.g. IT) domain. Entire infrastructures, government operations, social connections, health services, and almost every business sector rely on facilities that are potentially vulnerable to cyberattacks. Governments and businesses are increasingly looking for experts who are equipped not only with technical knowledge of the field, but also a deep understanding of its impacts on various aspects of our society. With Ontario Tech's mandate for market-driven programs and the well-established reputation of its IT security programs, it is only natural to add this program to our current portfolio.

The proposed program fits into FBIT strategic research plan themes of Digital Economy, Data Analytics and Artificial Intelligence, and Digital Technologies. This new degree will complement and build upon FBIT's portfolio of programs in information security, which includes our highly reputed bachelor of information technology in networking and IT security (NITS), established in 2005, as well as our successful Master of IT Security program, which is offered with 3 distinct fields: IT security, Artificial Intelligence, and Cybersecurity governance. The proposed program will be housed at FBIT Institute on CyberSecurity and Resilient Systems (ICRS), a multi-disciplinary global centre for cybersecurity research, innovation, teaching, and outreach.

There is a great opportunity within Ontario Tech to establish interdisciplinary research and collaboration among faculties in this program. For instance, research on global impact of cybersecurity policies could be supported by FSSH political science researchers, while applications of machine learning in cybersecurity could be explored by FBIT and FSCI computer science researchers. Cybercrime research can be supported by researchers from both FSSH and FBIT, while FBIT and FEAS experts can collaborate on infrastructure and smart city cybersecurity.

The program includes a number of components that each may be delivered differently. While some courses may be delivered using in-person, online, hybrid or asynchronous modes, it is expected that the seminar and research components will take place mostly on-campus and/or in collaboration with external organizations, industry and government agencies.

To our knowledge, this program will be the first specialized Ph.D. program in Cybersecurity in Canada, and among a handful of elite programs in this area in the world. The cross-faculty and cross-disciplinary nature of this program provides additional strength and differentiates it from cybersecurity specializations at other universities which are typically offered under Computer Science programs.

**RESOURCES REQUIRED:**

It is expected that most courses will be taught by core faculty members, with occasional hiring of adjunct instructors from the industry for specialized courses, if needed.

Recent TTT hires at FBIT are in line with the requirements of this program. As recommended in the external reviewers' report, it is recommended that the university prioritize hiring or appointing research chairs (NSERC CRC, Industry chairs or university research chairs) in cybersecurity, particularly in  areas related to  social and business aspects of cybersecurity. This is an important area of growth in the faculty and a differentiating factor that would enhance the multidisciplinary nature of the program.

The administration of the program at the faculty level will be added to the role of the Graduate Program Director and Graduate Program Assistant for Master of IT Security (MITS).

No Additional or dedicated space is required for the new program. Classes will be shared with MITS and CS graduate programs, and research work will be conducted in supervisors' research labs.

**CONSULTATION AND APPROVAL:**

- ✓ Academic Resource Committee: 18 December 2023
- ✓ FBIT Faculty Council: 1 October 2024
- Graduate Studies Committee (Recommendation): 22 October 2024
- Academic Council (Approval and Recommendation):  26 November 2024

- Board of Governors (Approval): ProspectiveTarget Date - 28 November 2024

**NEXT STEPS:**

- Pending the recommendation of GSC, the changes will be presented to Academic Council for approval and recommendation to the Board. The proposal must proceed through the following external approval steps
  - Ontario Universities Council on Quality Assurance
  - Ontario Ministry of Colleges and Universities

The preferred date of implementation is in the Fall of 2025

**SUPPORTING REFERENCE MATERIALS:**

- New Program Proposal with Appendices
- Reports from External Review

# New Graduate Program Proposal

| | |
|---|---|
| **Name of proposed program (as it will appear on the student's transcript):** | Doctor of Philosophy in Cybersecurity |
| **Degree Designation/Credential (e.g. BA, BSc, BEng, etc.):** | Ph.D. |
| **Cost Recovery Program?** | ☐ Yes ☑No |
| **Professional Program?** | ☐ Yes ☑ No |
| **For Graduate Diplomas** | ☐ Type 2 ☐ Type 3 |
| **Faculty (where the program will be housed):** | Faculty of Business and Information Technology |
| **Collaborating Faculty (if applicable):** | |
| **Program Delivery Location:** | North Oshawa Campus |
| **Collaborating Institution(s) (if applicable):** | |
| **Proposed Program Start Date:** | September 2025 |
| **Proposal Contact:** | Michael Bliemel, Carolyn McGregor and Shahram S. Heydari |
| **Submission Date:** | |
| **Approved by Dean:** (signature and date) | |

For CIQE Use Only:

| | |
|---|---|
| **Date of Academic Council Approval:** | |
| **QAF Version Used:** | 2021 QAF |
| ☐External reviewers' report<br>☐Program's and Dean's response (with date)*<br>☐Summary of changes | ☐Final, revised proposal<br>☐CVs, course outlines, and other supporting material (as appendices) |

# Table of Contents

# 1 Introduction

## a) Program Abstract

*Please provide a brief overview of the proposed program, to be shared with the public, in 1000 characters or less, including:*

- *A clear statement of the purpose of the program*
- *Any program components, such as fields, pathways, or micro-credentials (note that fields, pathways, and microcredentials are not required)*
- *Any distinctive elements, including alternative modes of delivery (including online)*
- *Note that this statement is for external purposes; what do you want potential students/advisors to know about this program?*

The PhD in Cybersecurity program is a multidisciplinary research-intensive program that covers a broad range of themes related to cybersecurity; including technology, policy and governance, AI and human behaviour. This program aims to prepare specialized socio-technical academics who can perform leading-edge research and teaching in the academia or industry, and help governments in policymaking in the area of cybersecurity. The proposed PhD in Cybersecurity program is the first of its kind in Canada.

The objectives of the program are achieved through a combination of coursework, seminars and a research thesis. The PhD in Cybersecurity program includes  graduate-level courses, a seminar course, a thesis proposal and candidacy exam, a dissertation and final defence. Potential students could come from a broad range of backgrounds including computer science, information technology, business and management, social and political science.

## b) Background and Rationale

- *Identify what is being proposed, what are the program objectives, and provide an academic rationale for the proposed program*
- *Explain the appropriateness of the program name and degree nomenclature as they relate to the program objectives; list any program specializations, pathways, etc.* ***(QAF 2.1.2.1a/b)***
- *Describe the mode of delivery (in-class, hybrid, online) and how it will support students in achieving the Degree Level Expectations and learning objectives of the program* ***(QAF 2.1.2.2c)***
- *Describe the ways in which the program fits into the broader array of program offerings within the Faculty and the University*
- *Describe any unique curriculum or program innovations, creative components, or significant high impact practice*

The proposed PhD in Cybersecurity provides the highest-level degree of expertise in the broad area of Cybersecurity and will be a multidisciplinary research-intensive program that would cover a broad range of themes related to cybersecurity; including technology, policy and governance, AI and human behaviour, aiming to attract students from a variety of backgrounds and prior education, including computer science, information technology, business and management, social and political science.

The importance and emergence of the field of cybersecurity in today's world cannot be overstated, and its impact is no longer limited to technical (e.g. IT) domain. Entire infrastructures, government operations, social connections, health services, and almost every business sector rely on facilities that are potentially vulnerable to cyberattacks. Governments and businesses are increasingly looking for experts who are equipped not only with technical knowledge of the field, but also a deep understanding of its impacts on various aspects of our society. With Ontario Tech's mandate for market-driven programs and the well-established reputation of its IT security programs, it is only natural to add this program to our current portfolio.

The proposed program fits into FBIT strategic research plan themes of Digital Economy, Data Analytics and Artificial Intelligence, and Digital Technologies. This new degree will complement and build upon FBIT's portfolio of programs in information security, which includes our highly reputed bachelor of information technology in networking and IT security (NITS), established in 2005, as well as our successful Master of IT Security program, which is offered with 3 distinct fields: IT security, Artificial Intelligence, and Cybersecurity governance. The proposed program will be housed at FBIT Institute on CyberSecurity and Resilient Systems (ICRS), a multi-disciplinary global centre for cybersecurity research, innovation, teaching, and outreach.

There is a great opportunity within Ontario Tech to establish interdisciplinary research and collaboration among faculties in this program. For instance, research on global impact of cybersecurity policies could be supported by FSSH political science researchers, while applications of machine learning in cybersecurity could be explored by FBIT and FSCI computer science researchers. Cybercrime research can be supported by researchers from both FSSH and FBIT, while FBIT and FEAS experts can collaborate on infrastructure and smart city cybersecurity.

The program includes a number of components that each may be delivered differently. While some courses may be delivered using in-person, online, hybrid or asynchronous modes, it is expected that the seminar and research components will take place mostly on-campus and/or in collaboration with external organizations, industry and government agencies.

To our knowledge, this program will be the first specialized Ph.D. program in Cybersecurity in Canada, and among a handful of elite programs in this area in the world. The cross-faculty and cross-disciplinary nature of this program provides additional strength and differentiates it from cybersecurity specializations at other universities which are typically offered under Computer Science programs.

## c) Consistency of Program Objectives with University Mission, Vision, Integrated Academic and Research Plan, and Strategic Mandate Agreement (QAF 2.1.2.1c)

- *Describe how the program contributes to the University's Mission and Vision*
- *Explain how the program aligns with the goals and priorities outlined in the Faculty's(ies') and University's Integrated Plan. Identify how the program fits within one or more areas of strength or growth in Ontario Tech University's Strategic Mandate Agreement*

The proposed program is an embodiment of the university's main priority, "Tech with a conscience", to advance scientific and technical knowledge in a domain that affects not just the daily lives of people but also of the well-being of the world.

Through its affiliation with the Institute for Cybersecurity and Resilience Systems (ICRS), the proposed program will achieve the university's strategic priority of "partnership" by connecting researchers across different faculties with industry partners, government organizations and other research institutes outside the university.

The proposed program also aligns with the university's core values, in particular, intellectual resilience and innovation, through developing research expertise, intellectual properties and innovations in the emerging field of cybersecurity. The proposed program builds upon the successful Master of IT Security program at FBIT, which has been one of the fastest growing graduate programs at Ontario Tech University.

The PhD program in Cybersecurity fits into several areas of strengths/growth that were identified in the university's strategic mandate. In particular, it builds upon and grows our strength in digital technologies and artificial intelligence; and due to the multidisciplinary nature of cybersecurity, it also has the potential to expand our strength in crime, justice and forensic science, automotive and transportation systems; and community wellness. The proposed program is also relevant to the university's strategic research priority area of disruptive technology and new economy, as cybersecurity continues to become an increasingly important factor in most social, business and public decision-making processes.

### d) Student Demand

- *Provide evidence of student demand, including number of prospective student inquiries; applications and registrations for similar programs; results from surveys/focus groups of existing students, graduates, or professionals in the field*
- *Include information about domestic vs. international student interest*

Considering the rising interest in Cybersecurity programs at universities worldwide and the need for specialist academics to teach and conduct research in the field, we expect the number of applicants to be quite sufficient for our target student numbers. As confirmed by the University Registrar and AVP International, the university's international agent network has confirmed significant demand for cybersecurity among international students, pointing out that our Master of IT Security (MITS) has had as many as 800 applicants for 50-100 spots each year and this alone could likely stimulate a PhD program.

***Enrolment Information***

- *Please complete Table 1 and provide, in paragraph form, information regarding enrolment projections*
- *Please determine the academic year when the program enrollment will reach a steady-state and add an asterisk (*) in the corresponding box beside the number*

The following numbers indicate the anticipated enrollments per year, based on the typical number of applications to other PhD programs at Ontario Tech, and the number of faculty members who will accept students under this program. It is expected that the program will reach stability in year 5 (2028-2029) for a total number of 20 students.

## Table 1: Projected Enrollment by Academic and Program Year

| | Academic Year | | | | | |
|---|---|---|---|---|---|---|
| | 2024-2025 | 2025-2026 | 2026-2027 | 2027-2028 | 2028-2029 | 2029-2030 |
| **Level of Study** | | | | | | |
| **Ph.D. year 1** | 4 | 5 | 5 | 5 | 5 | 5 |
| **Ph.D. year 2** | | 4 | 5 | 5 | 5 | 5 |
| **Ph.D. year 3** | | | 4 | 5 | 5 | 5 |
| **Ph.D. year 4** | | | | 4 | 5 | 5 |
| **Total Enrolment** | 4 | 9 | 14 | 19 | 20* | 20* |

## e) Societal Need

- *Evidence of the need for graduates of the program and in which fields (within academic, public, and/or private sectors)*
- *Please indicate up to three occupations in which graduates from this proposed program may be employed using the Ontario Job Futures website; you may also wish to review the Durham Workforce Authority website and provide any relevant sector portfolio or local/community impact information*
- *For professional programs, a description of the program's congruence with current regulatory requirements*
- *Mention if any employers in the area support the need for this program and include a letter(s) of support as an additional appendix*

The number of cybersecurity job openings across the globe is expected to grow to 3.5 million unfilled positions through 2025 (Cybercrime magazine, Nov. 9, 2021). The Canadian federal government has stated that "due to a shortage of cyber security talent in Canada and worldwide, cyber security professionals are needed across government." and "Nearly all Canadian federal government departments have a need for cyber security professionals." Currently roughly 20% of the 130+ postings on the Association of Information Systems job portal are looking for Cybersecurity assistant professors across the English-speaking countries where most are in business schools. This market is relatively new as cybersecurity from a management and technical perspective gains importance globally as a consequence of the digital economy that has accelerated from the pandemic driven digital transformation in all industries.

Given the growing reliance of the society on cyberspace in almost all aspects of life, the need for cybersecurity professionals and services is projected to increase significantly. Consequently, we expect a growing need for highly-skilled experts who could contribute to training, research, policymaking, and consultation in cybersecurity for businesses and governments. Graduates of the proposed program may be employed as university and college professors, industry researchers, government researchers and specialists, policymakers and business consultants.

## f) Duplication

- *Describe how the program is distinct from other programs at Ontario Tech. Is it reasonable to anticipate this program might affect enrolment in other related programs? If so, how might this be addressed?*

The PhD program in cybersecurity will provide a venue for aspiring students in MITS (graduate), NITS (undergraduate) as well as graduates of Computer science (CS) and social science programs who want to specialize in the field of cybersecurity. Given that several FBIT faculty members participating in this program are also members of the CS graduate program, some CS grad applicants may choose this specialized Ph.D. program in

Cybersecurity over the general CS graduate program. However, we don’t expect these programs to compete with each other. Both programs are hosted or co-hosted by FBIT. These programs are intended to complement each other for broader attractions of research-focused graduate students to the university. The Ph.D. program in cybersecurity focuses on applications of information Technology, and has a significantly broader scope as it covers policy, governance, privacy and IT management issues that are not covered under the Computer Science program.

- *Identify similar or complementary programs offered elsewhere in Ontario in Table 2. Please be brief but specific in the table. Avoid value-based statements*

## Table 2: List of Similar Programs in Ontario

<table>
<tr><th>Institution Name</th><th>Credential Level and Program Name</th></tr>
<tr><td>Queen’s University</td><td>PhD, School of Computing</td></tr>
<tr><td colspan="2"><b>Link to Program Web Page:</b> https://cyber.cs.queensu.ca/program/</td></tr>
<tr><td colspan="2"><b>Brief Program Description:</b><br>The school of computing at Queen’s University offers a PhD program in Computing Science in which students can also specialize in Cybersecurity. The program was originally supported by a 2019 NSERC CREATE grant. This is the only PhD program in Ontario currently listed under Government of Canada’s Post-secondary cyber security related programs guide.</td></tr>
<tr><td colspan="2"><b>What differentiates the new program from this existing program:</b><br>Queen’s program is a standard computing science PhD by research, with only a condition that students must take two courses in Cybersecurity. The proposed program at Ontario Tech focuses entirely on Cybersecurity (including all coursework), and does it from a multidisciplinary view, allowing non-CS students also to specialize in social, political and governmental aspects of cybersecurity. Such level of breadth does not exist in Queen’s university program.</td></tr>
<tr><th>Institution Name</th><th>Credential Level and Program Name</th></tr>
<tr><td>Carleton University</td><td>PhD, School of Information Technology</td></tr>
<tr><td colspan="2"><b>Link to Program Web Page:</b> https://www.csit.carleton.ca/index.php?pageID=GradPHD</td></tr>
<tr><td colspan="2"><b>Brief Program Description:</b><br>Carleton’s School of Information technology (CSIT) offers a PhD program in Information Technology with a focus on applications of IT in various fields, including network security. This is one of the few PhD programs in IT (and distinguished from similar programs in Computer Science) in Canada.</td></tr>
</table>

**What differentiates the new program from this existing program:**
While students in Carleton's PhD in IT program may be able to conduct their research in the area of IT security, the proposed Ontario Tech program provides a broader multidisciplinary focus on cybersecurity. The coursework of our proposed program also covers various aspects of cybersecurity, which gives the graduates both deeper and broader knowledge in this field.

- *Provide additional overall comment on the justification for this duplication*

No similar PhD program with a focus and breadth in the field of cybersecurity currently exists in Ontario, which justifies the launching of this new program at Ontario Tech.

# 2 Program Requirements

## a) Admission Requirements (QAF 2.1.2.5)

- *Outline the formal admission requirements; explain how these are appropriate for the program objectives and program learning outcomes: How will they help to ensure students are successful? How do they align with the learning outcomes of the program? (*
- *Explain any additional requirements for admission to the program such as minimum grade point average, special language, portfolio, etc. (and how the program recognizes prior work or learning experience, if applicable) (*
- *Indicate the programs from which students may be drawn*

In addition to the general admission requirements for graduate studies, PhD in Cybersecurity applicants must meet the following program-specific requirements.

- Students would normally be expected to have completed a four-year undergraduate degree and a thesis-based Masters degree in a relevant field from a Canadian university, or its equivalent from a recognized institution, with an overall academic standing of at least 3.5 on a 4.0/4.3 scale or its equivalent in their last two years of study.

**MITS Pathway:** Graduates of Ontario Tech University Master of IT Security (MITS) program can apply to the Ph.D. program If they have completed the MITS program with an overall academic standing of at least 3.5/4.3.

- A minimum of two letters of reference from persons having direct knowledge of the applicant's academic competence. Academic references are preferred; however professional references will be accepted. Letters of reference should come from individuals under whom the applicant has worked closely or studied. The quality of the letters will be assessed by the Graduate Committee to make sure relevant requirements have been met.

- Proof of English proficiency is needed from those applicants whose first language is not English, as per university regulations.

- Applicants must find a prospective faculty supervisor from among the list of graduate faculty members of the PhD in Cybersecurity program and receive formal acceptance of the faculty member to supervise their research. No applicant will be accepted to the program without having an approved prospective supervisor in advance.

- As part of the application form, students are required to provide a minimum 3000-word long personal research statement, outlining their area of interest in cybersecurity, their proposed academic research plan, and identify the faculty supervisor who has agreed to supervise their research.

**b) Program Learning Outcomes and Assessment of Student Knowledge (QAF 2.1.2.2 a/b/d, 2.1.2.3, 2.1.2.4)**

- ***Connect with CIQE (cige@ontariotechu.ca) early in the program development to participate in learning outcome development sessions or arrange for assistance and review prior to the scheduling of the external site visit***
- *In Table 3 below, please describe what the student will know or be able to do (knowledge, methodologies, and skills) by the end of the program and indicate how that knowledge or skill will be demonstrated*
- *An example has been provided in purple in the first row and should be removed.*

*Degree Level Expectations are set by the Quality Council of Ontario and should not be modified. For the list of and more information on these expectations, including a detailed description, visit their website.*

## Table 3: Program Learning Outcomes

| Program Learning Outcomes By the end of the program, students graduating will be able to… (normally 6-8 outcomes per program with 12 being the maximum) | Degree Level Expectations (list all that apply; you must align with each expectation at least once) | Relevant courses (provide course code and course title) | Assessment of Learning Outcomes (e.g. test, rubric, self-assessment, etc.) |
|---|---|---|---|
| Demonstrate a thorough understanding and detailed knowledge of the state of the art in threats and attacks against computing systems, | • Depth & Breadth of Knowledge<br>• Research & Scholarship | INFR5010G<br>INFR7100G<br>INFR7200G | Course Exam, Candidacy Defence, Thesis Defence |

| | | | |
|---|---|---|---|
| cyber-physical systems and social networks | | | |
| Analyze, plan and apply various techniques for vulnerability assessment, protection, detection, mitigation and response to cyberattacks | • Research & Scholarship<br>• Application of Knowledge<br>• Awareness of limits of Knowledge<br>• Autonomy and Professional Capacity | INFR5010G<br>INFR6020G<br>INFR7100G<br>INFR7200G | Course Exam, Candidacy Defence, Thesis Defence |
| Develop and evaluate information security and risk management practices, policies, and procedures that comply with the current standards, federal, provincial and international laws, agreements and policies on issues related to cybersecurity, ethical hacking and data privacy. | • Application of Knowledge<br>• Awareness of limits of Knowledge<br>• Autonomy and Professional Capacity | MITS5100G<br>INFR5600G | Course Exam |
| Demonstrate a thorough understanding and detailed knowledge of the economic, social and business drivers of cybersecurity and related technologies | • Depth & Breadth of Knowledge<br>• Research & Scholarship<br>• Application of Knowledge | INFR6020G<br>MITS6900G | Course Exam |
| Demonstrate a thorough understanding and detailed knowledge of the state of the art in applications of Artificial Intelligence to cybersecurity, attack detection and mitigation. | • Depth & Breadth of Knowledge<br>• Research & Scholarship<br>• Application of Knowledge | INFR6010G<br>INFR7100G<br>INFR7200G | Course Exam, Candidacy Defence, Thesis Defence |
| Evaluate, analyze and criticize limitations of cybersecurity and Artificial Intelligence tools in terms of privacy protection, algorithmic and data biases, sociopolitical | • Awareness of limits of Knowledge<br>• Autonomy and Professional Capacity | MITS5100G<br>INFR6010G<br>INFR6020G<br>INFR6030G | Course Exam |

| | | | |
|---|---|---|---|
| impact and other potential problems | | | |
| Communicate effectively and accurately to the public and in professional circles about various aspects of cybersecurity | • Communication Skills | INFR7000G<br>INFR7100G<br>INFR7200G | Seminar Evaluations, Candidacy Defence, Thesis Defence |

- *Selecting a few examples from above, and with assistance from CIQE (ciqe@ontariotechu.ca), please provide further details on:*
  - *Appropriateness of the program's structure and the requirements to meet its objectives and program learning outcomes; Guidance on program objectives and program-level learning outcomes, including examples, is available here*
  - *Appropriateness of the proposed methods for the assessment of student achievement of the intended program learning outcomes and Degree Level Expectations (How will students demonstrate they have learned and can do what we expect them to by the end of the program?); and*
  - *Completeness and appropriateness of plans for monitoring and assessing:*
    - *The overall quality of the program*
    - *Whether the program is achieving in practice its proposed objectives;*
    - *Whether the students are achieving the program learning outcomes; and*
    - *How the resulting information will be documented and subsequently used to inform continuous program improvement*

  *Please see Guidance on Assessment of Teaching and Learning for advice on how to satisfy these criteria.*

The following includes examples that illustrate the connections between learning outcomes, program elements and structure, and assessment methods. We also describe our plan for monitoring and assessing program quality, objectives and learning outcomes.

*Program Learning Outcome: Demonstrate a thorough understanding and detailed knowledge of the state of the art in threats and attacks against computing systems, cyber-physical systems and social networks.*

The PhD in Cybersecurity program provides a comprehensive theoretical understanding of the state-of-the art in information security through a foundation course in cybersecurity, INFR5010G. This course is designed particularly for those who enter the program without a deep theoretical knowledge of the field, and includes learning modules in cryptography, principles of network security, system vulnerabilities, malware, and a review of hacker tools and methods. The learning outcomes of this course will be assessed through individual module tests. The students will further enhance their knowledge of the field through developing a PhD research proposal which must be evaluated and defended in front of a committee of examiners, and subsequently write and defend their PhD thesis, which must include sufficient review of state-of-the art and elements of novel contributions to the field.

*Program Learning Outcome: Analyze, plan and apply various techniques for vulnerability assessment, protection, detection, mitigation and response to cyberattacks*

The PhD in Cybersecurity program provides a thorough understanding of the state-of-the art in cybersecurity defense through a foundation course in cybersecurity, INFR5010G. This course is designed particularly for those who enter the program without a applied knowledge of the field, and includes learning modules in design principles for secure systems, trusted computing base, security models, authentication, authorization and accounting (AAA), identity and access control, logging and auditing, intrusion detection, and information security management. The learning outcomes of this course will be assessed through individual module tests. The students will further enhance their knowledge of the field through developing a PhD research proposal which must be evaluated and defended in front of a committee of examiners, and subsequently write and defend their PhD thesis, which must include sufficient review of state-of-the art and elements of novel contributions to the field.

*Program Learning Outcome: Develop and evaluate information security and risk management practices, policies, and procedures that comply with the current standards, federal, provincial and international laws, agreements and policies on issues related to cybersecurity, ethical hacking and data privacy.*

The PhD in Cybersecurity program includes two courses that contribute toward this outcome. The MITS5100G – Law and Ethics of IT Security is a prerequisite program course which provides an overview of the laws and professional ethics that information security professionals must understand and apply. This course includes reviews of the current laws on e-contracts, regulations, online crime, intellectual property, privacy and data breach liability. Students will be assessed through research assignments to demonstrate their knowledge of the laws and standards. The INFR5600G – security policies and risk management, is a multidisciplinary course where students will learn about how to develop strong security policies and procedures, conduct risk management and identify vulnerabilities in security policies. The course includes lecture classes and lab exercises, and students will be assessed through quizzes and presentations.

*Program Learning Outcome: Demonstrate a thorough understanding and detailed knowledge of the state of the art in applications of Artificial Intelligence to cybersecurity, attack detection and mitigation.*

The PhD in Cybersecurity Program offers a course in AI in Cybersecurity – INFR6010G, along with a number of elective courses in this field from the MITS program. This course empowers students with knowledge about how AI can be used by attackers as well as in defence systems, and techniques to mitigate such attacks using machine learning programming. The learning outcomes of this course is assessed through assignments and projects. The students will have further opportunities to enhance their knowledge in this area through developing a relevant PhD research proposal which must be evaluated and defended in front of a committee of examiners, and subsequently write and defend their PhD thesis, which must include sufficient review of state-of-the art and elements of novel contributions to the field.

*Program Learning Outcome: Evaluate, analyze and criticize limitations of cybersecurity and Artificial Intelligence tools in terms of privacy protection, algorithmic and data biases, sociopolitical impact and other potential problems*

The PhD in Cybersecurity program addresses this important learning outcome in a number of courses that focus on potential issues arising from cybersecurity. The IT Security Law and Ethics – MITS5100G course discusses the issue of privacy from legal and technical standpoints. The AI in Cybersecurity – INFR6010G course includes discussions of algorithmic bias in AI. The Information Trust – INFR6030G course includes discussions of trust in computing and data, and how cybersecurity techniques and policies should be built around this issue. All courses provide assessment of the learning outcomes through student assignments, presentations and course projects.

*Program Learning Outcome: Communicate effectively and accurately to the public and in professional circles about various aspects of cybersecurity*

The PhD in Cybersecurity program includes several elements to prepare students for effective communication of cybersecurity ideas and solutions. Students are required to register in and participate in a zero-credit seminar course every semester. Each student must present at least two seminars throughout their program: one seminar before the candidacy exam, and one exit seminar before their thesis defence. Additionally, each student must present and defend their research proposal in an open session for an examining committee and public audience, and do the same for defending their thesis. Many of program courses also include student presentations as part of the assessment.

In general, learning outcomes overall are assessed on an ongoing basis by each student's supervisory committee. Student progress reports are submitted each term by the committee to the Graduate Program Director and School of Graduate and Postdoctoral Studies (SGPS) for assessment.

- *Describe the requirements and structure of the program. Is it full-time/part-time? Is this an online or partially online/hybrid program? What are the unique curriculum or program innovations or creative components in this program?*
- *Address how the program's structure, requirements, and program-level learning outcomes are appropriate in meeting the Degree Level Expectations.*
  - *Please attach, as an Appendix, the Program Learning Outcome Alignment Map to Degree Level Expectations*
  - *If the program is to be accredited, include with the above information about the accreditation requirements and add the accreditation tables, if available, as an Appendix.*
- *Provide evidence that each graduate student is required to take a minimum of two-thirds of the course requirements from among graduate-level courses*
- *What is the program length? Provide a rationale for the length that ensures the program learning outcomes and requirements can be reasonably completed*

The Ph.D. program in Cybersecurity is a full-time and includes graduate-level courses, a seminar course, a thesis proposal and candidacy exam, a dissertation and final defence. All coursework is at graduate level.

The course requirements of the program may include a variety of delivery options, including in-person, online or hybrid, depending on the course. The research portion of the program is normally conducted on campus and/or in a research facility.

The Ph.D. program in Cybersecurity is unique in Canada in terms of the scope, breadth and area of focus. It is a multidisciplinary research-intensive program that covers a broad range of themes related to cybersecurity; including technology, policy and governance, AI and human behaviour. No program with such scope currently exists in Canada. Cybersecurity research in other universities is either provided under computer science programs and limited to technical issues, or under political science and governance programs and limited to policy issues. There is a lack of a multidisciplinary program whose graduates are provide opportunities to gain a reasonable grasp of both angles, and the proposed program aims to fill this gap. Additionally, this program will provide a unique opportunity to graduates of Computer Science programs to gain expertise in policy and governance issues of cybersecurity, and to graduates of social policy and governance programs to learn about technical aspects of cybersecurity.

The program follows a traditional model for doctoral studies in North America. Similar to other doctoral programs at Ontario Tech university, students should be able to complete all requirements within four years of full-time study. Students are expected to complete course requirements and pass the candidacy exams within 18-24 months after starting the program, and complete and defend their research thesis within 48 months after starting the program.

Only graduate-level courses are accepted for fulfilling the requirements of this program. That includes both mandatory and elective courses.

- *Describe the ways in which the curriculum addresses the current state of the discipline (QAF 2.1.4a)*
- *For researched-focused graduate programs, provide a clear indication of the nature and suitability of the major research requirements for degree completion*

The proposed curriculum includes common elements of most other PhD by research program at Ontario Tech as well as other Ontario Universities. Those include coursework to prepare students for development of a research proposal; a candidacy exam where faculty experts examine the proposal and provide guidelines and critique to the student with regards to the nature and suitability of the research proposal; and a final thesis defence in front of internal and external arm-length experts to evaluate the quality of research work. Students are supported throughout this process by continuous guidance and feedback from their supervisors as well as regular meeting with their supervisory committee. Regular progress reports will be submitted every semester to SGPS.

- *Is there an experiential learning component (e.g. workplace learning, co-op, internship, field placements, service learning, mandatory professional practice) to the program? If yes, please describe this component in 2500 words or less. Include confirmed partners, duration of the experiential learning component(s), and projected number of placements (where applicable)*

Select students may have the opportunity to work on applied industry sponsored research through the Institute for Cybersecurity and Resilient Systems as part of their dissertation.

- *Describe how the principles of Equity, Diversity, Inclusion, and Decolonization have been considered:*
    - *Does the program contain concepts, materials, or resources from scholars/professionals who are part of one or more historically marginalized groups?*
    - *Are multiple perspectives represented in the program, such as those offered by those who are Indigenous, Black, Persons of Colour, and/or 2SLGBTQIA+?*

- o *How has accessibility been considered? More specifically, have the needs of students with disabilities been integrated into the program design (e.g., the ways that students are asked to demonstrate their learning)?*
- o *Will this program provide space to allow for the discussion of other viewpoints outside the "dominant, Western narrative"?*
- o *Have the principles of Universal Design been considered?*

- *Describe how the potential need to provide accessibility accommodations has been considered in the development of this program; please provide information beyond the services offered by Student Accessibility Services*

The Faculty of Business and IT (FBIT) is among the most diverse and inclusive faculties at Ontario Tech university in terms of racial, religious and gender diversity in faculty members and students. It is expected that the new PhD program in cybersecurity will also follow those standards. In particular, this program will help diversify the extreme gender imbalance in CyberSecurity by looking to recruit from our diverse pool of Master of IT Security students. Training and mentorship of the next generation of female and minority researchers and educators in the field of cybersecurity would also create a pool of role models for historically marginalized groups in this field.

The program also includes areas of research related to marginalized and indigenous communities where such students will have many opportunities to apply their learning back into their own communities through already established research projects and partnerships with communities and organizations. Examples include: cybersecurity policies and their impact on marginalized communities; algorithmic and data biases in cybersecurity; inclusion of marginalized communities and their well-being in cybersecurity decision-making process; and global cybersecurity issues. As part of this proposal, a special scholarship is proposed for indigenous students who intend to complete the Ph.D. program in cybersecurity.

EDI metrics will be evaluated during regular program reviews.

Similar to other graduate programs at Ontario Tech University, this program will also follow the Procedures for Academic Accommodation for Students with Disabilities https://usgc.ontariotechu.ca/policy/policy-library/policies/legal,-compliance-and-governance/procedures-for-academic-accommodation-for-students-with-disabilities.php

## c) Calendar Copy with Program Map(s)

- *Provide, as an Appendix using the template provided, a clear and full calendar copy. The template ensures consistency across all programs in the Academic Calendar*

- *Provide, as an Appendix, a full list of the all courses included in the program including course numbers, titles, and descriptions. Please indicate clearly whether they are new/existing. Include full course proposals for new courses, and the most recent course syllabi for existing courses. If you are making changes to existing courses, include instead a course change form. In an appendix noted below, you will note which faculty members are expected to teach in the program and who is responsible for developing any new courses.*

Please see Appendix for proposed calendar copy and a full list of courses in the program. ***Please note that all new courses were previously approved for offer in relation to the MITS program during the process of development of this proposal and are active in the 2024-2025 Academic Calendar.**

# 3 Consultation

- *Describe the expected impact of the new program on the nature and quality of other programs delivered by the home and collaborating Faculty(ies) and any expected impact on programs offered by other Faculties*
- *Outline the process of consultation with the Deans of Faculties that will be implicated or affected by the creation of the proposed program*
- *Provide letters of support for the program from Deans at Ontario Tech and/or from other institutions/partners*
- *Describe any consultation undertaken with regard to the principles of Equity, Diversity, Inclusion, and Decolonization*

The Ph.D. program in cybersecurity would create a new interdisciplinary venue for collaboration between Faculty of Business and IT (FBIT) and Faculty of Social Science and Humanities (FSSH), with additional areas of potential collaborations with Faculty of Science (FSCI) and Faculty of Engineering and Applied Science (FEAS) too. It is expected that some members from the aforementioned faculties would join this graduate program as associate or full members.

The program has currently been discussed and received support and feedback at FBIT at the current levels:

- Dean
- Academic Resource Committee approval of NOI and feedback (Feb 23, 2023)
- Faculty Council – information and feedback (June 20, 2023)
- Individual feedback from the networking and IT Security area (May-July 2023)
- FBIT Graduate Education Committee Approval (Nov 15, 2023)

Consultation with SGPS – Sep 6, 2023, October 25, 2023
Consultation with FSCI and FEAS faculty members – Sep 13, 2023
Request for comments from IEAC – Nov 10, 2023

| |
|---|
| Consultation with CIQE and TLC– Nov 10, 2023<br>External Review (site visit) – June 25/26, 2024 |
| |

Does this Program contain any Indigenous content? □ Yes ☒ No □ Unsure

*For more information on how Indigenous content is defined at Ontario Tech University and how to consult with the Indigenous Education Advisory Circle (IEAC), please refer to the Protocol for Consultation with the Indigenous Education Advisory Circle.*

Has the IEAC been contacted □ Yes ☒ No

If yes, when?

| |
|---|
| |

What was the advice you received from the IEAC, and how has it been included in your proposal?

| |
|---|
| |

Did the IEAC ask you to return the proposal to them for review? □ Yes ☒ No

If yes, have they completed their review? □ Yes □ No ☒ N/A

# 4 Resource Requirements (QAF 2.1.2.6, 2.1.2.7, 2.1.2.8 a)

## a) General Resource Considerations

- *Note here if this new program may impact enrolment agreements with other institutions/external partners that exist with the Faculty/Provost's office*
- *Indicate if the new program will require changes to any existing agreements with other institutions, or will require the creation of a new agreement. Please consult*

*with CIQE (cige@ontariotechu.ca) regarding any implications to existing or new agreements.*

There are no impacts on enrollment agreements or agreements with other institutions.

**b) Faculty Members - Current and New Faculty Requirements**

- *Complete as an Appendix, using the Faculty Information templates provided, charts chart detailing the list of faculty committed to the program and provide any additional details, in paragraph form below; the information in the Appendix or additional information must include clear evidence that faculty have the recent research or professional/clinical expertise needed to sustain the program, promote innovation, and foster an appropriate intellectual climate. This should also demonstrate how supervisory loads are distributed in light of qualifications and appointment status; if necessary, include this information below*
- *Include a brief statement to provide evidence of the participation of a sufficient number and quality of faculty who will actively participate in the delivery of the program and achieve the goals of the program and foster the appropriate academic environment, contribute substantively to the program, and commit to student mentoring*
- *Describe the role of any sessional/part-time faculty; provide an approximate percentage used in the delivery of the program and the plans to ensure the sustainability of the program and quality of the student experience*
- *Explain the provision of supervision of any experiential learning opportunities; how will supervisory loads be distributed?*
- ***If new faculty resources are needed, describe the plan and commitment to provide these resources to support the program and the rationale in section 4h)***

Recent TTT hires at FBIT are in line with the requirements of this program. As recommended in the external reviewers report, it is recommended that the university prioritize hiring or appointing research chairs (NSERC CRC, Industry chairs or university research chairs) in cybersecurity, particularly in areas related to social and business aspects of cybersecurity. This is an important area of growth in the faculty and a differentiating factor that would enhance the multidisciplinary nature of the program.

**c) Additional academic and non-academic human resources**

- *Give details regarding the nature and level of Sessional Instructor and TA support required by the program, the level of administrative and academic advising support, etc.*
- ***If new resources are needed, describe the plan and commitment to provide these resources to support the program and the rationale in section 4h)***

We expect that most courses will be taught by core faculty members, with occasional hiring of adjunct instructors from the industry for specialized courses, if needed.
The administration of the program at the faculty level will be added to the role of the Graduate Program Director and Graduate Program Assistant for Master of IT Security (MITS).

## d) Supporting information for online and hybrid programs

- *Describe the adequacy of the technological platform to be used for online delivery*
- *Describe how the quality of education will be maintained*
- *Describe how the program objectives will be met*
- *Describe how the program learning outcomes will be met*
- *Describe the support services and training for teaching staff that will be made available*
- *Describe the sufficiency and type of supports that will be available to students*
  - *How has accessibility been considered?*
  - *What strategies have been considered to accommodate students with disabilities?*
  - *Have the principles of Universal Design been considered?*
  - *Will course content be offered in both written and audible forms (e.g., closed captioning, transcriptions)?*
  - *Is course content designed logically and is it easy to follow with limited instruction?*
  - *Are assignment expectations clear (i.e., a rubric)?*
  - *Have the needs of students with limited or unreliable access to wi-fi been considered (e.g., breaking down pre-recorded lectures into maximum 10-minute videos)?*

Not Applicable.

## e) Existing non-financial student supports

### <u>School of Graduate and Post-Doctoral Studies</u>

Quality graduate and postdoctoral education combines teaching, research, professional development, disciplinary community involvement and personal growth. It is by nature a shared responsibility between students, faculty members, the programs and a large number of support units, with overarching administration being provided by the School of Graduate and Postdoctoral Studies.

The School of Graduate and Postdoctoral Studies (SGPS) at Ontario Tech University is the main point of contact for our postgraduates, facilitating support and offering guidance for our growing graduate community of students, postdoctoral fellows and graduate faculty members. The SGPS Graduate Academic Affairs Specialist works to identify and provide advice to solutions for graduate students based on graduate policies, resources and working with faculty partners. The SGPS assists students in areas such as: student-supervisor relationships; personal or academic barriers to progression; research progression; and navigating academic regulations. The SGPS works closely with campus partners to refer students to other helpful resources and supports across our campus community.

The SGPS Graduate Engagement Team coordinates a range of programs such as Graduate Pro Skills and the Three Minute Thesis.  SGPS' most recent initiative, Base Camp, represents foundational programming that provides our graduate students and postdoctoral fellows with specific skills necessary to succeed as global citizens in the workplace and beyond. Centered around four pillars: Achieve, Empower, Ascend, Inspire, Base Camp builds on the aptitudes and lived experiences of our graduate students and postdoctoral fellows, propelling them forward to new heights. The SGPS team supports prospective, new and returning graduate students from the start of their journey beginning with recruitment and admissions, through registration, funding and scholarships, to then join us at orientation, professional development workshops and a range of events, ultimately supporting our graduates through to successful degree conferral.

## **Faculty-Specific Support**

### ***Academic Advising***

Graduate students will receive academic advice and support at FBIT through the office of Graduate program Director (GPD). A dedicated graduate program assistant provides support for all graduate programs at FBIT.

## **Student Life**

Ontario Tech University, as a relatively small campus community, has a centralized delivery model for many student supports. All undergraduate students have access to an extensive support system that ensures a quality student experience. Each Faculty may provide additional, Faculty- or program-specific supports. In addition to the outlined services below, students may also take advantage of the Campus Bookstore, Housing and Living Resources as well as the Ontario Tech Student Union. Further information can be found at: http://studentlife.ontariotechu.ca/.

### ***Student Learning Centre***

Ontario Tech University fosters a high level of academic excellence by working with students, undergraduate and graduate, to achieve educational success. Faculty specific academic resources are available online and include tip sheets and videos. Academic specialists offer one-on-one support services in mathematics, writing, study skills, ESL and physics. With the additional support of peer tutors and workshops, the

Student Learning Centre can also accommodate the needs of a specific course or program.

### ***Student Accessibility Services***

Ontario Tech University ensures that students with disabilities have equal opportunities for academic success. Student Accessibility Services operates under the Ontario Human Rights Code and the Accessibility for Ontarians with Disabilities Act. Services and accommodation support are provided for students with documented disabilities and include:

- Adaptive technology training
- Alternate format course material
- Learning skills support
- Testing support
- Transition support for incoming students

Student Accessibility Services also provides inclusive peer spaces, support groups, and skills workshops for students.

### ***Career Readiness***

Ontario Tech University offers comprehensive career service assistance, co-op and internship support and a variety of valuable resources to help students along their career paths, including:

- Assistance with creating effective job-search documents
- Career counselling
- Co-op and internships
- Interview preparation
- Job market information
- Job search strategies

The Career Centre hosts a variety of events during the academic year including employer information and networking sessions, job fairs and interviews conducted by leading employers.

### ***Student Engagement, Equity and Inclusion***, and ***Indigenous Education and Cultural Services***

The university supports students' successful transition and provides opportunities to develop leadership and professional skills throughout their university career. Services provided include:

- Equity and inclusivity programming and support groups
- Indigenous Education and Cultural Services provides space and supports for students to connect with Indigenous culture and resources

- Opportunities to grow and develop leadership skills through the Ambassador and Peer Mentorship program
- Orientation and events through first year
- Peer mentoring
- Services and supports for international and exchange students
- Specialized programming for first-generation, graduate, Indigenous, international, mature, online, transfer and diploma-to-degree pathways students

### ***Student Mental Health Services***

Student Mental Health Services helps students learn how to better manage the pressures of student life. Students can:

- Access short term counselling and therapy services
- Access tools and resources online to learn about mental health and how to maintain good health and wellness
- Attend drop-in sessions
- Participate in events, activities or support groups that promote positive health and well-being
- Work with a mental health professional to address concerns

Students in distress will also be provided with support and counselling as needed. There is no cost to students and services are confidential. For those who need long-term counselling support or specialized mental health services, Ontario Tech University will provide referrals to assist the student in accessing resources in the local community or in the student's home community.

### ***Athletics and Recreation Facilities***

Ontario Tech University offers a number of recreation facilities and fitness opportunities to meet all lifestyles and needs. On-campus facilities include the state-of-the-art FLEX Fitness Centre which overlooks Oshawa Creek, five gymnasiums, a 200-metre indoor track, two aerobic/dance studios, the Campus Ice Centre, Campus Fieldhouse, a soccer pitch, a fastball diamond, squash courts and an indoor golf training centre. Students are able to participate in varsity and intramural sports as well as group fitness classes and personal training sessions.

### **Campus Health Centre**

The Campus Health Centre provides assistance in numerous confidential health-care options including:

- A medical clinic with daily access to physician and nursing staff
- Treatment of disease, illness, and injury

- Allergy injections, immunizations, and influenza injections
- Complementary Health Services featuring acupuncture, chiropractic, custom orthotics, massage therapy, nutritional counselling, and physical therapy
- An on-site laboratory (blood work, STI testing, throat swabs, etc.)
- Gynaecological health-care and prescriptions

## Student Awards and Financial Aid

Student Awards and Financial Aid (SAFA) is dedicated to helping students understand the variety of options available to finance their education. Budgeting and financial planning are essential to their success and SAFA is on hand to help create the right financial plan. Financial assistance can be in the form of bursaries, employment (both on-campus and off), parental resources, scholarships, student lines of credit and the Ontario Student Assistance Program (OSAP).

## Information Technology Resources

Ontario Tech University is a leader among North American universities in implementing and using curriculum and industry specific software in a technology-enriched learning environment (TELE). Our unique environment is adapted to each discipline based on faculty requirements and input for optimal student learning. We are committed to providing the greatest value for students' investment in education and technology while studying at Ontario Tech University.

One of the greatest advantages of Ontario Tech University's approach to TELE is that all students have equal access to the same technology, resources and services. Whether you are inside or outside of the classroom, your course-specific software allows you to work on your own or with others and enjoy seamless access to all Ontario Tech online resources. TELE supports Bring-your-own-device (BYOD) which provides you with laptop standards when acquiring the right laptop for your program and software support services onsite and online. An annual fee for TELE covers a wide range of program-specific software, technical software support, exam support and virus protection.

IT Services strives to provide quality services to students at Ontario Tech. To support these objectives, the following components are included:

### *Wireless network*

Wireless internet connection is available in public areas and open-air locations around the Ontario Tech campus where students congregate (North Oshawa and Downtown locations).

### *Wired network*

To ensure the success of the technology-enriched learning environment, a comprehensive data network has been installed on campus. This includes network drops in lecture halls and designated areas as well as network drops for each residence suite.

Ontario Tech students benefit from networked classrooms and learning spaces. Each ergonomically-designed space has data network connection access and electrical connections to ensure battery regeneration. In addition, classrooms include electronic projection equipment and full multimedia support.

### *Exam support services*

IT Services provide hardware, software and technical support during examinations. IT team will be equipped with loaner laptops in the event of major technical issues.

### *Laptop repairs*

IT Services provide on campus repairs on eligible laptop models.

### *IT Service Desk*

The IT Service Desk is equipped with certified technicians and experienced IT professionals offering technical support services on a drop-in, call-in or email basis.

### *General Use Workstations (GUWs)*

Ontario Tech undergraduate students are able to use general workstations available at the library and have access to Bring Your Own Device Technology-Enriched Learning Environment (BYOD TELE) model course-specific software.

### *Software Support*

Software Support specialists are available to students on-site and online to assist in downloading/installing University software and support any other software related issues.

### *Printing services*

Printing services are available to students in the following areas: labs, classrooms, study common areas, the Learning Commons and the Library. All Ontario Tech students receive print credits every year, more Printpacks can be purchased through the Campus Bookstore if students require additional printing services.

## Teaching & Learning Centre

The mission of the Teaching and Learning Centre (TLC) at Ontario Tech University is to empower faculty to reach their potential as educators and to create a culture where effective teaching is valued. We champion the scholarship of teaching and implementation of pedagogy.  We create valuable teaching and learning professional development experiences.  We move Ontario Tech University towards being a leader in teaching excellence, ultimately leading to greater student success.

The TLC provides faculty with a range of tools and facilities to assist them in providing a rich learning experience for students. Experts at the TLC provide support in various areas including curriculum development, multimedia design, learning technology and in the overall improvement of teaching practice.

In addition, the TLC funds teaching-related projects from the Teaching Innovation Fund (TIF) for proposals by faculty members aimed at developing new methods in teaching and learning. The TLC facilitates teaching awards at the University and supports faculty in their application for external awards and funding opportunities that focus on teaching and learning.

### f) Graduate student financial support

- *Provide evidence that financial assistance will be sufficient to ensure quality and numbers of students*
- *Provide the teaching assistant hours and capacity within the Faculty*

Full time students in the program will receive guaranteed financial support from the following sources:

1. Graduate Research Assistantship from their supervisors, for the amount set by SGPS and guaranteed for four years of full-time study (subject to satisfactory standing).
2. Graduate Teaching Assistantship from the faculty, for 270 hours of TA work in a year at the rate determined by the university, and guaranteed for four years of full-time study (subject to satisfactory standing).
3. International student tuition scholarship for international students, equivalent to the difference between international and domestic tuition fees, subject to SGPS rules and availability.
4. A special graduate scholarship (funded by SGPS) for indigenous students in the program.

Part-time students in the program will not be guaranteed any financial support.

### g) Physical resource requirements

- *Please attach a report, as an Appendix, from the Library regarding existing library holdings and support for student learning; please contact your Subject Librarian as you begin your proposal to request a 'Library statement for new program proposal'*
- *Address any space/infrastructure requirements including information technology, laboratory space, equipment, etc.* ***If new space is required, please complete Table 4 (examples in purple); otherwise, please remove this Table***
- *Ideally, please provide information on the change in the number of faculty, students, administrative staff, etc. as well as information on changes in equipment and activities (additional space; the renovation of existing space; or will the current space allocation accommodate the new program)*

- ***If new resources are needed, d the plan and commitment to provide these resources to support the program and the rationale in section 4h)***

No Additional or dedicated space is required for the new program. Classes will be shared with MITS and CS graduate programs, and research work will be conducted in supervisors' research labs.

## Table 4: Additional Space Requirements

| Space Type | Number Required | Space Requirements (sq. ft) |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

### h) Resource Summary

*Provide a brief statement of the funding requirements and the rationale.*

**<u>Human Resource Requirements</u>**

Are additional faculty required to be able to offer this program? ☒ Yes ☐ No

If yes, what year will the faculty hire be required, and are there additional criteria associated with the hiring requirement (e.g. enrolment levels)?

A new TTT hire with expertise in the area of cybersecurity has already been hired for the program.

Are additional staff required to be able to offer this program? ☐ Yes ☒ No

If yes, please outline what year the staff hire will be required and any additional criteria associated with the hiring requirement:

**<u>Space Requirements</u>**

Are there additional space requirements specific to being able to successfully launch this program? □ Yes ☒ No

If yes, please provide additional details:

**Technology Requirements**

Are there additional technology requirements specific to being able to successfully launch this program? □ Yes ☒ No

If yes, please provide additional details:

**Additional Resource Requirements**

Are there additional resource requirements not specified above that are required to successfully launch this program? If so, please outline them below:

***The resource requirements outlined above have been reviewed and approved by the Academic Resource Committee (ARC):*** ________________________________

*(date of review)*

# 5 Closing Statements Regarding Program Quality (QAF 2.1.2.8)

- *Please describe any additional evidence of the quality of the faculty (e.g. qualifications, funding, honours, awards, research, innovation and scholarly record) not already discussed*
- *Please provide any other evidence that the program and faculty will ensure the intellectual quality of the student experience*

# APPENDICES

*Please include at minimum the below. Additional Appendices may be added, as appropriate. Appendices should ultimately be listed, attached, and labelled (A, B, C, etc.) in the order in which they first are mentioned in the document.*

Program Learning Outcome Alignment Map to DLEs
Accreditation tables (if applicable)
Calendar Copy with Program Maps (please use template)
List of Program Courses, New Course Proposals, Required Course Changes, Course Syllabi for Existing Courses (can each be attached as separate appendices)
Detailed Listing of Faculty Committed to the Program (please use template)
Library Report

## Items to be separate documents sent to CIQE:

New Program Funding and Tuition form (for CIQE use only)
Budget Spreadsheet (for ARC use only)
CVs for all faculty committed to the program (to be provided to the external reviewers)

# Appendix A: Full Doctoral GDLE Mapping

| | Demonstrate a thorough understanding and detailed knowledge of the state of the art in threats and attacks against computing systems, cyber-physical systems and social networks | Analyze, plan and apply various techniques for vulnerability assessment, protection, detection, mitigation and response to cyberattacks | Develop and evaluate information security and risk management practices, policies, and procedures that comply with the current standards, federal, provincial and international laws, agreements and policies on issues related to cybersecurity, ethical hacking and data privacy. | Demonstrate a thorough understanding and detailed knowledge of the economic, social and business drivers of cybersecurity and related technologies | Demonstrate a thorough understanding and detailed knowledge of the state of the art in applications of Artificial Intelligence to cybersecurity, attack detection and mitigation. | Evaluate, analyze and criticize limitations of cybersecurity and Artificial Intelligence tools in terms of privacy protection, algorithmic and data biases, sociopolitical impact and other potential problems | Communicate effectively and accurately to the public and in professional circles about various aspects of cybersecurity |
|---|---|---|---|---|---|---|---|
| **Depth and Breadth of Knowledge** | X | | | X | X | | |
| A thorough understanding of a substantial body of knowledge that is at the forefront of their academic discipline or area of professional practice including, where appropriate, relevant knowledge outside the field and/or discipline. | X | | | X | X | | |
| **Research and scholarship** | X | X | | X | X | | |
| a) The ability to conceptualize, design, and implement research for the generation of new knowledge, applications, or understanding at the forefront of the discipline, and to adjust the research design or methodology in the light of unforeseen problems; | X | X | | X | X | | |
| b) The ability to make informed judgments on complex issues in specialist fields, sometimes requiring new methods; and | X | X | | X | X | | |
| c) The ability to produce original research, or other advanced scholarship, of a quality to satisfy peer review, and to merit publication. | X | X | | X | X | | |
| **Level of Application of Knowledge- The capacity to:** | | X | X | X | X | | |
| a) undertake pure and/or applied research at an advanced level; and | | X | X | X | X | | |
| b) contribute to the development of academic or professional skills, techniques, tools, practices, ideas, theories, approaches, and/or materials. | | X | X | X | X | | |
| **Communication Skills** | | | | | | | X |
| The ability to communicate complex and/or ambiguous ideas, issues and conclusions clearly and effectively. | | | | | | | X |
| **Awareness of limits of knowledge** | | X | X | | | X | |
| An appreciation of the limitations of one's own work and discipline, of the complexity of knowledge, and of the potential contributions of other interpretations, methods, and disciplines. | | X | X | | | X | |
| **Autonomy/Professional capacity** | | X | X | | | X | |
| a) The qualities and transferable skills necessary for employment requiring the exercise of personal responsibility and largely autonomous initiative in complex situations; | | X | X | | | X | |
| b) The intellectual independence to be academically and professionally engaged and current; | | X | X | | | X | |
| c) The ethical behaviour consistent with academic integrity and the use of appropriate guidelines and procedures for responsible conduct of research; and | | X | X | | | X | |
| d) The ability to evaluate the broader implications of applying knowledge to particular contexts. | | X | X | | | X | |

## Appendix B – Calendar Copy

### Contact Information

Faculty of Business and Information Technology
Ontario Tech University
2000 Simcoe Street North
Oshawa, ON L1G 0C5
T: 905.721.8668
E: fbit@ontariotechu.ca

### Program

Ph.D. in CyberSecurity

### Program General information

The PhD in Cybersecurity program is a multidisciplinary research-intensive program that covers a broad range of themes related to cybersecurity; including technology, business, policy and governance, AI and human behaviour. This program aims to prepare specialized socio-technical academics who can perform leading edge research and teaching in Academia or in Industry and help governments in policymaking in the area of cybersecurity. The objectives of the program are achieved through a combination of coursework, seminars and a research thesis. Students will gain comprehensive knowledge of theory and technologies of cybersecurity, legal and ethical issues around cybersecurity and privacy, and cybersecurity policies, as well as proficiency in cybersecurity research methodology and state-of-the art research topics. The Ph.D. in cybersecurity program is hosted at Ontario Tech Faculty of Business and Information Technology and affiliated with the Institute for Cybersecurity and Resilient Systems (ICSR), a multi-disciplinary, global centre for cybersecurity research, innovation, teaching, and outreach at Ontario Tech University.

### Admission requirements

In addition to the general admission requirements for graduate studies, PhD in Cybersecurity applicants must meet the following program-specific requirements.

- Students would normally be expected to have completed a four-year undergraduate degree and a thesis-based Masters degree in a relevant field from a Canadian university, or its equivalent from a recognized institution, with an overall academic standing of at least 3.5 on a 4.0/4.3 scale or its equivalent in their last two years of study.

**MITS Pathway:** Graduates of Ontario Tech University Master of IT Security (MITS) program can apply to the Ph.D. program If they have completed the MITS program with an overall academic standing of at least 3.5/4.3.

- A minimum of two letters of reference from persons having direct knowledge of the applicant's academic competence. Academic references are preferred; however professional references will be accepted. Letters of reference should come from individuals under whom the applicant has worked closely or studied. The quality of the letters will be assessed by the Graduate Committee to make sure relevant requirements have been met.

- Proof of English proficiency is needed from those applicants whose first language is not English, as per university regulations.

- Applicants must find a prospective faculty supervisor from among the list of graduate faculty members of the PhD in Cybersecurity program and receive formal acceptance of the faculty member to supervise their research. No applicant will be accepted to the program without having an approved prospective supervisor in advance.

- As part of the application form, students are required to provide a minimum 3000-word long personal research statement, outlining their area of interest in cybersecurity, their proposed academic research plan, and identify the faculty supervisor who has agreed to supervise their research.

## Part-time studies

The PhD in Cybersecurity program is intended to be a full-time program.

## Degree requirements

a. **Coursework component**

Students in the program must demonstrate their broad proficiency in the area of cybersecurity through evidence of completing or having completed graduate-level coursework in the fields of theory, applications, legal and governance issues of cybersecurity. The coursework component of the program includes prerequisite and specialized courses, a seminar, a thesis proposal and a final thesis.

Students are required to complete or demonstrate proficiency in the following prerequisites:

1. Cybersecurity: The following courses are required for students who do not have prior background in IT security.

   - INFR 5010G - Fundamentals of IT security (6 Credits)
   - MITS 5100G - Law and Ethics of IT Security (3 Credits)

2. Research methods: The following prerequisite is required for students who have not completed a thesis-based Master's program in a relevant field prior to starting the PhD in Cybersecurity.

   - CSCI 5010G – Survey of Computer Science Research Topics and Methods (3 Credits)

Note: Students who demonstrate sufficient proficiency through prior graduate-level coursework or extensive related work experience, can request a waiver for the corresponding prerequisite course from the Graduate Program Director. Waiver requests are not guaranteed and will be considered on a case-by-case basis.

**Specialized Courses**

Students in the PhD program in Cybersecurity must take three specialized courses with the approval of their supervisory committee. These courses must be completed prior to the thesis candidacy proposal examination. The specialized courses for each year will be announced at the time of registration for that academic year, and may vary from year to year based on instructor availability. Some examples of specialized course topics are as following:

- INFR 6010G - Artificial Intelligence in Cybersecurity
- INFR 6020G - Usable Security
- INFR 6030G - Information Trust
- INFR 6040G - Cybersecurity in Critical Infrastructure
  INFR 6050G – Advanced Topics in Cybersecurity
- INFR 6110G - Global Cybersecurity Threats
- INFR 6120G - Cybersecurity Leadership
- INFR 6130G - CyberCrime
- MITS 6900G - Blockchain Fundamentals and Technologies

Note: Students may take up to two relevant MITS or CSCI 5xxx/6xxx-level courses as specialized courses (If not taken in a previous degree) with the approval of their supervisory committee and the Graduate Program Director.

**Seminar/Proposal/Thesis Courses**

Students must register in the following zero-credit courses for their seminar, proposal and thesis work:

- INFR 7000G - PhD Cybersecurity Seminar
- INFR 7100G - PhD thesis proposal and candidacy Exam
- INFR 7200G - PhD Dissertation

### b. Research component

Students who successfully complete their coursework will then enter the thesis phase of the program. At this stage, students must prepare a thesis proposal under the supervision of their supervising committee, and then defend their proposal in an oral candidacy exam. After successful defence of their proposal, they will be considered PhD candidates. It is strongly recommended that students complete their coursework and candidacy exam within 24 months after entering the program on a full-time basis.

All PhD Candidates must defend their final thesis in an oral session in front of a committee of internal and external examiners, as per university regulations. Upon successful defence of their thesis and subject to completion of all other requirements of the program, a degree of PhD in Cybersecurity will be conferred upon them.

### c. Seminars

All /students in the PhD in Cybersecurity program must register in and participate in a zero-credit seminar course every semester. Each student must present at least two seminars throughout their program: one seminar before the candidacy exam, and one exit seminar before their thesis defence.

# Appendix C - New Courses

**Please note that all courses were formally approved during the 2023-2024 academic year in relation to the MITS program and are active in the 2024-2025 Academic Calendar.**

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT

**Fundamentals of Cybersecurity**

**2024-25**

## 1. Course Details & Important Dates*

| Term | Course Type | Day | Time | Location | CRN# |
|---|---|---|---|---|---|
| 2024-25 | Online | | | | |

| Classes Start | Classes End | **Last day to drop course without academic consequence** | Final Exam Period |
|---|---|---|---|
| | | | |

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

## 2. Instructor Contact Information

| Instructor Name | Office | Phone | Email |
|---|---|---|---|
| Stephen Marsh | | | Canvas Email |
| Office Hours: by appointment | | | |

| Laboratory/Teaching Assistant Name | Office | Phone | Email |
|---|---|---|---|
| | | | |
| Office Hours: by appointment | | | |

## 3. Course Description

This course introduces a concise review of the foundations of IT Security. It is designed as a collection of six modules using asynchronous online delivery method, covering the following topics:

Module 1: Fundamentals of Networking
Module 2: Foundations of Cryptography
Module 3: Authentication and Identity Management
Module 4: Network attacks and malicious codes
Module 5: Intrusion Detection and Protection
Module 6: IT Forensics

Each module includes approximately 8-10 hours of video lectures and reading material, and is expected to be completed over four weeks.

## 4. Learning Outcomes

On successful completion of the course, students will be able to:

- Describe the architecture of today's Internet; identify and differentiate TCP/IP layers and protocols; and analyze various communication technologies.
- Explain the basic concepts and theoretical underpinnings of symmetric cryptography, public-key cryptography and hash functions.
- Explain the basic concepts of authentication and access control, and differentiate various techniques.
- Describe different types of malicious software, and explain how OS and software vulnerabilities can be exploited by malware and network attacks.
- Understand Intrusion Detection Systems (IDSs), Anomaly Detection and Behavior Analysis, Security Information and Event Management Systems and Deception Technologies.
- Describe how to implement a computer forensics incident-response strategy, and how to conduct proper IT forensics and investigation.

## 5. Course Design

The course will be modular, with 6 modules over two semesters, each focusing on a different aspect of cybersecurity. Each module has its own assessment and a grade of 70% per module is required to pass the entire course. The course is delivered entirely online, with recorded lectures, extensive office hours available per week, an online synchronous (1.5 hour) exam per module, and readings in the form of academic papers and an Open Educational Resource.

Students requiring assistance are encouraged to speak to their instructor during class or during office hours. Should you wish to meet with the instructor outside of office hours, please email first to make an appointment. Students should get into the habit of making and keeping business appointments. Should you fail to attend or cancel the appointment at least 24 hours in advance, you will lose the right to book another appointment.

Email is commonly used by students to communicate with their instructor. However, it does limit the effectiveness of the communications and may not be the best way for instructors to answer student questions, especially those requiring an explanation of concepts covered in this course or some personal concerns. Therefore, the instructor may request a telephone call or personal/online meeting. *Your instructor will inform you as to their expectations about emails.*

## 6. Outline of Topics in the Course

### Tentative Course Schedule, Fall 2024 and Winter 2025

| Module/Week # | Date | Topics | Material Covered |
|---|---|---|---|
| 1/1 | | Fundamentals of Networking | Data communication Fundamentals |
| 1/2 | | | Network models and architectures |
| 1/3 | | | Emerging trends in networking |
| 1/4 | | | |
| | | | Module assessment |
| 2/1 | | Foundations of Cryptography | Random bit generation and stream ciphers |
| 2/2 | | | Advanced Encryption Standard |
| 2/3 | | | Secure Hash Algorithm (SHA-2) |
| 2/4 | | | Message Authentication Codes<br>Public-Key Certificates |
| | | | Module assessment |
| 3/1 | | | User Authentication |
| 3/2 | | Authentication and Identity Management | Access control |
| 3/3 | | | OS Security (Windows, Linux)<br>Mobile Authentication and Zero Trust |
| 3/4 | | | Audits and logs |
| | | | Module assessment |
| Semester Break | | | |
| 4/1 | | | Denial of Service Attacks and Botnets |
| 4/2 | | | Malicious Software |
| 4/3 | | | |
| 4/4 | | | Disaster Recovery |
| | | | Module assessment |
| 5/1 | | Intrusion Detection and Prevention | Intrusion Detection Systems |
| 5/2 | | | Firewalls and Network Security |
| 5/3 | | | |
| 5/4 | | | AI and IDS/IDP |
| | | | Module assessment |
| 6/1 | | IT Forensics | Introduction to Digital Forensics<br>Digital Investigation Fundamentals |
| 6/2 | | | Volume Analysis<br>File System Analysis |

| | | | |
|---|---|---|---|
| 6/3 | | | Operating System Forensics |
| | | | |
| 6/4 | | | Mobile forensics |
| | | | Module assessment |
| | | | Final presentation (online, recorded) |

***Important Notes:*** *Adjustment of scheduled lectures might be made in accordance with any unforeseen circumstances during the semester.*

## 7. Required Readings

An Open Educational Resource is available for the course which contains the reading material for each module.

*Additional readings may be assigned or recommended during the course.*

## 8. Evaluation Method

Each module will have a final assessment in its fourth (4th) week, which usually takes the form of an exam. To pass the course, each assessment must be passed with at least 70% in the assessment. The final grade is an average of each of the modules amounting to 90% of the final grade of the course, with an additional 10% for an online recorded final presentation and engagement, due date end of final module.

A within-exam grade of 70% (10.5/15) or higher is necessary **in each module** in order to pass the entire course.

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found under Academic Regulations at: Ontario Tech's Academic regulations

## 9. Assignments and Tests

Each module has a final online assessment (usually in the form of an exam) of one hour which is worth 15% of the final grade for the course. In order to pass the course it is necessary to achieve a grade of 70% (or 10.5 out of 15) in each of these exams. The assessment will normally be held during an online synchronous session in the final week of each module.

### Missed In-Term Course Work

A request for consideration for missed course work worth 20% or less of the final grade must be documented and reported to the instructor in writing within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. Course work includes, but is not limited to: quizzes, written assignments (problem set), participation, case studies, etc. If missed coursework totals more than 20% of the final grade, the request for consideration must be submitted to the Faculty of Business and IT Advising Office and to the course instructor in writing using the Academic Consideration Form, along with supporting documentation. The request must be submitted within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. If approved, the extended deadline of the missed course component will be granted. If a student misses coursework and does not follow the procedure above, they will receive a score of zero on the missed component.

All forms can also be found through MyOntarioTech or on the Ontario Tech University website.

For information on how missed/late assignments and medical excuses are managed, please refer to the university's revised ***Procedures for Consideration of Missed In-Term Course Work and Examinations***

## 10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

## 11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.
Disclaimer: "The content you are about to view contains sensitive subject matter that may be considered offensive and/or disturbing to some viewers. By viewing and/or interacting with the content you acknowledge and agree that it is your decision to view and interact with the content and to take the risk that you will experience a negative emotional response or reaction to the nature of the content."

## 12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

## 13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

## 14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code. Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

## 15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

## 16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

## 17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

## 18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

## 19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English  when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration*  Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

## 20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

**Notice of Collection and Use of Personal Information**
Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Internet and Webcam.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

**By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.**

## 21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g. during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

## 22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

## 23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University.  The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

## 24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

## 25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT

# INFR 6020: Usable Security
# Course outline for Fall 2024

## 1. Course Details & Important Dates*

| Term | Course Type | Day | Time | Location | CRN# |
|---|---|---|---|---|---|
| FALL 2024 | Lecture | TBA | TBA | TBA | TBA |

| Classes Start | Classes End | **Last day to drop course without academic consequence** | Final Exam Period |
|---|---|---|---|
| TBA, 2024 | TBA, 2024 | TBA | TBA |

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

**Important Note – Final Exams**

The final exam for this course will be run ON CAMPUS during the regular final exam period. If a student cannot attend due to COVID-19 related international travel restrictions you **must email your course instructor ASAP** (as soon as possible) regarding the possibility of alternate arrangements.

## 2. Instructor Contact Information

| Instructor Name | Office | Phone | Email |
|---|---|---|---|
| Dr. Julie Thorpe | UB2016 | | Julie.thorpe@ontariotechu.ca |
| Office Hours: TBA | | | |

| Laboratory/Teaching Assistant Name | Office | Phone | Email |
|---|---|---|---|
| | | | |
| Office Hours: | | | |

## 3. Course Description

The security offered by a system can be dramatically influenced by its user interface. This effect has been observed across many cybersecurity applications that aim to help users in tasks such as secure authentication, encryption, system administration, and secure software development. The user interfaces for such applications require not only good usability, but also need to assist users in understanding risks and making decisions, typically in environments and situations where cybersecurity is not their primary concern. This course provides foundational knowledge on general HCI, usable security, and user interface techniques that have been proposed for cybersecurity applications. The course also discusses a set of cybersecurity problems whereby usable security approaches have been proposed.

## 4. Learning Outcomes

On successful completion of the course, students will be able to:

- Explain the challenges of usable security
- Describe, review, and critique recent literature in usable security
- Compare the strengths and weaknesses of usable security solutions, from both a usability perspective and a cybersecurity perspective
- Propose solutions to current problems in usable security
- Design user studies and analyze their results

## 5. Course Design

Each lecture period reviews and discusses the materials of that week. There will be in-class paper presentations and related activities. Assignments and quizzes will reinforce the weekly topics. Understanding of course concepts will be demonstrated through a final project. The scheduled topics and readings are detailed below.

## 6. Outline of Topics in the Course

| Week # | Date | Topics | Readings (papers may vary slightly based on most recent research at the time of offering) |
|---|---|---|---|
| 1 | | Introduction to Usable Security | • Garfinkel Chapters 1 and 2 |
| 2 | | Experimental Research and Design | • Lazar Chapters 2 and 3 |
| 3 | | Authentication | • Garfinkel Chapters 3.1 and 5.1 |
| 4 | | Statistical Analysis in HCI Research | • Lazar Chapter 4 |
| 5 | | Social Engineering and Phishing | • Garfinkel Chapters 3.3 and 4 |
| 6 | | Nudging and Cybersecurity Decisions | • A. Caraban et al. “23 Ways to Nudge: A Review of Technology-Mediated Nudging in Human-Computer Interaction”. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019.<br>• V. Zimmermann and K. Renaud. “The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions.” ACM Trans. Comput.-Hum. Interact. 28, 1, Article 7 (2021). |
| 7 | | Designing Surveys | • Lazar Chapter 5<br>• E. Redmiles et al. “A Summary of Survey Methodology Best Practices for Security and Privacy Researchers.” University of Maryland CS-TR-5055, 2017. |
| 8 | | Usability Testing and Working with Human Subjects | • Lazar Chapters 10 and 15<br>• Schechter, Stuart. "Common pitfalls in writing about security and privacy human subjects experiments, and how to avoid them." Microsoft, 2013, URL: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/commonpitfalls.pdf |
| 9 | | Mental Models and User Education in Cybersecurity | • Jampen, D., Gür, G., Sutter, T. et al. Don’t Click: Towards an Effective Anti-Phishing Training. A Comparative Literature Review. Hum. Cent. Comput. Inf. Sci. 10, 33 (2020).<br>• Elissa M. Redmiles et al., A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web, In Proceedings of the 29th USENIX Security Symposium, 2020. |

| | | | |
|---|---|---|---|
| 10 | | Usable Encryption | • Garfinkel Chapter 3.2<br>• Scott Ruoti, Nathan Kim, Ben Burgon, Timothy van der Horst, and Kent Seamons. 2013. Confused Johnny: when automatic encryption leads to confusion and mistakes. In Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS), 2013.<br>• C. Stransky et al. On the Limited Impact of Visualizing Encryption: Perceptions of E2E Messaging Security. In Proceedings of SOUPS, 2021.<br>• C. Stransky, O. Wiese, V. Roth, Y. Acar and S. Fahl. 27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University. In Proceedings of the IEEE Symposium on Security and Privacy, 2022. |
| 11 | | Usability for Secure Software Development | • M. Green and M. Smith, "Developers are Not the Enemy!: The Need for Usable Security APIs," in IEEE Security & Privacy, vol. 14, no. 5, pp. 40-46, Sept.-Oct. 2016.<br>• D. Votipka et al. “Understanding security mistakes developers make: Qualitative analysis from Build It, Break It, Fix It.” In Proceedings of the USENIX Security Symposium, 2020.<br>• A. Krause et al. “Pushed by Accident: A Mixed-Methods Study on Strategies of Handling Secret Information in Source Code Repositories.” In Proceedings of the 32nd USENIX Security Symposium, 2023. |
| 12 | | Usability for Secure System Administration | • Garfinkel Chapters 3.10 and 5.3<br>• Schreuders, Z. Cliffe, Tanya McGill, and Christian Payne. "Empowering end users to confine their own applications: The results of a usability study comparing SELinux, AppArmor, and FBAC-LSM." ACM Transactions on Information and System Security (TISSEC) 14.2 (2011): 1-28. |

## 7. Required Texts/Readings

The following textbooks are mandatory for this course:

1. Garfinkel, Simson and Lipford, Heather Richter. *Usable Security: History, Themes, and Challenges.* Synthesis Lectures on Information Security, Privacy, and Trust, 2014.
2. Lazar, Jonathan, Jinjuan Heidi Feng, and Harry Hochheiser. *Research Methods in Human-Computer Interaction*. Morgan Kaufmann, 2017.

Additional readings may be assigned or recommended during the course.

## 8. Evaluation Method

- Paper presentation: 20%
- Final project: 40%
- Assignments: 20%
- Quizzes: 20%

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found under Academic Regulations at: Ontario Tech's Academic regulations

## 9. Assignments and Tests

- Week 1: Paper presentation sign-up.  Paper presentation will be in-class, the date will depend on the paper signed up for.
- Week 2: Assignment #1 released, due Week 4
- Week 3: Quiz #1
- Week 4: Assignment #2 released, due Week 6
- Week 6: Quiz #2
- Week 9: Quiz #3
- Week 12: Quiz #4
- Final Project: Due 1 week after last class

### Missed In-term Examination

Students who miss an in-term examination such as a midterm or a term test may submit a request for consideration to the Faculty of Business and IT Advising Office and to the course instructor in writing using the Academic Consideration Form, along with supporting documentation. The request must be submitted within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. If a midterm or term test is missed for approved reasons, the weight of the missed component will be added to the weight of the final exam (or another exam component). If a student misses an in-term examination and does not follow the procedure above, they will receive a score of zero on the missed component.

All forms can also be found through MyOntarioTech or on the Ontario Tech University website.

### Missed In-Term Course Work

A request for consideration for missed course work worth 20% or less of the final grade must be documented and reported to the instructor in writing within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. Course work includes, but is not limited to: quizzes, written assignments, participation, case studies, etc. If missed coursework totals more than 20% of the final grade, the request for consideration must be submitted to the Faculty of Business and IT Advising Office and to the course instructor in writing using the Academic Consideration Form, along with supporting documentation. The request must be submitted within the deadlines specified in the Procedures for Consideration of Missed In-Term

Course Work and Examinations. If approved, the weight of the missed course component will be added to the weight of the final project. If a student misses coursework and does not follow the procedure above, they will receive a score of zero on the missed component.

For information on how missed/late assignments and medical excuses are managed, please refer to the university's revised *Procedures for Consideration of Missed In-Term Course Work and Examinations*

## 10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

## 11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain e.g. graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.

## 12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

## 13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

## 14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code. Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday’s 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

## 15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected

to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one’s perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

## 16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University’s regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one’s own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

## 17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University’s use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

## 18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

## 19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English  when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration*  Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

## 20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

### Notice of Collection and Use of Personal Information

Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Turnitin.

  For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

**By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.**

## 21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone’s race or creed, ridiculing an individual’s disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one’s sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech’s Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g. during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

## 22. Freedom of Expression

Pursuant to Ontario Tech’s Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university’s legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using “chat” functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

## 23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University. The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

## 24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

## 25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT

**INFR 6030G: Information Trust**

**Course outline for ----**

## 1. Course Details & Important Dates*

| Term | Course Type | Day | Time | Location | CRN# |
|---|---|---|---|---|---|
| ---- | | | | ---- | |

| Classes Start | Classes End | **Last day to drop course without academic consequence** | Final Exam Period |
|---|---|---|---|
| ---- | ---- | ---- | ---- |

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

**Please Choose ONE of the following, *if applicable*:**

**Important Note – Final Exams**

There is no final exam for this course

## 2. Instructor Contact Information

| Instructor Name | Office | Phone | Email |
|---|---|---|---|
| | | | |
| Office Hours: | | | |

| Laboratory/Teaching Assistant Name | Office | Phone | Email |
|---|---|---|---|

| | | | |
|---|---|---|---|
| | | | |
| Office Hours: | | | |

## 3. Course Description

In this course, students examine trust, provenance, critical thinking and design thinking for information from first principles to action. How to measure and judge information quality is discussed, as well as the various ways in which trust can be attacked in the context of information. More specifically, we will also examine how to use information to make trustworthy decisions in different cybersecurity and other contexts.

## 4. Learning Outcomes

On the successful completion of the course, students will be able to:

- Compare and Contrast different philosophies and models of trust
- Apply Design Thinking and Critical Thinking to information trust and provenance problems
- Discuss different approaches for the protection of information as an object
- Construct learning materials to help others in the understanding of information trust problems
- Hypothesize on the ways in which information is useful and used in the context of trust and future technoloogies

## 5. Course Design

The course is an online discussion-based course with presentations from experts from industry and academia on the ways in which trust, information design, critical and design thinking come together to address the increasingly difficult provenance questions as they relate to information that can be used to inform decisions, justify actions and build worthwhile, trustworthy knowledge.

We will use lectures to discuss the fundamentals of the concepts, and case or paper-based student-led discussions about how real examples reflect the content of the course fundamentals. This is a student-driven course and students are expected to provide their own personal and/or professional examples of how information trust works (or doesn’t) for the class.

## 6. Outline of Topics in the Course

| Lecture # | Topics | Details of topics to be covered in the course, by unit or by week |
|---|---|---|
| 1 | What is trust? How can we even use it? | Trust fundamentals, computational trust, computing trust. |
| 2 | Trust in information, the basics | |
| 3 | Provenance | What it is, what is means, how it can be determined, what it means to trust |
| 4 | Building knowledge | How is knowledge built? What builds it? What links together? What are the problems? |
| 5 | Design Thinking | An introduction to design thinking and why it matters here |

| | | |
|---|---|---|
| 6 | Critical Design Thinking | Applying critical thinking to the design thinking problem and coming up with a new paradigm |
| 7 | Information Trust, tying it all together | A look at Atele-William's Information Trust models |
| 8 | Applying what was learned | How can what we have looked at help with things like provenance and knowledge bulding?<br>We will do our information trust problem this week. |
| 9 | Attacks on trust | Trust is fragile. How? Why? What can kill or damage it? |
| 10 | Attacks on information | Information has always been precious, and has always been attacked, to be stolen or (more relevant to us) weaponized. How, when and why? |
| 11 | Defences and panaceas | And how can we defend it, either by being pre-informed or by putting sensible checks and balances in place? |
| 12 | Wrapping up: a design for information trust for the LLM world and beyond | The world is changing. How can we best adapt and put in place a sensible way to think about what we see before us based on what we have learned? |

## 7. Required Texts/Readings

The course is reading and discussion-based. Some of the materials are expected to come from students themselves (related to their own experiences in the area) whilst some are drawn from sources that are either freely available or available through the library at no cost to the student. There is no textbook but as a reference we will be using the Open Educational Resource, "Trust Systems" (Marsh, 2022) which is available on the Ontario Open Library. Further open resources will be curated during the course by the students as part of their evaluated work.

The readings and cases will be assigned at the start of the course, and will include sections and papers related to:

- Design Thinking
- Critical Thinking
- Computational Trust
- Information Trust
- Decision-making
- Trust Attacks
- Provenance
- AI and LLMs
- Privacy

Additional readings may be assigned or recommended during the course.

## 8. Evaluation Method

Participation in classes is expected, attendance is mandatory (a maximum of 2 classes can be missed before the final grade becomes a zero). Participation is 30% of the final grade.

Presentation of case/papers (weekly, assigned at the start of the class): 25%

A recorded video presentation of one of the class topics will be required by students: 25%

Peer evaluation of recorded presentations: 10%

Worked problem example: 10% (this will use the skills developed in the course of the class in order to address information trust in a curated information sample).

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found under Academic Regulations at: Ontario Tech's Academic regulations

## 9. Assignments and Tests

**Missed In-Term Course Work**

A request for consideration for missed course work worth 20% or less of the final grade must be documented and reported to the instructor in writing within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. Course work includes, but is not limited to: quizzes, written assignments, participation, case studies, etc. If missed coursework totals more than 20% of the final grade, the request for consideration must be submitted to the Faculty of Business and IT Advising Office and to the course instructor in writing using the Academic Consideration Form, along with supporting documentation. The request must be submitted within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. If approved, the weight of the missed course component will be added to the weight of the final information trust problem.  If a student misses coursework and does not follow the procedure above, they will receive a score of zero on the missed component.

Attendance in the weekly classes is mandatory. Given the discussional nature of the course, students who miss more than 2 of the weekly sessions will receive an automatic zero for the course.

For information on how missed/late assignments and medical excuses are managed, please refer to the university's revised *Procedures for Consideration of Missed In-Term Course Work and Examinations*

## 10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

## 11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain Instructors should provide examples that are applicable to the course subject matter – e.g. graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content. Instructors should publish a warning statement in advance so as to give students adequate opportunity to make a choice to avoid any such matter. The following is a sample disclaimer: “The content you are about to view contains sensitive subject matter that may be considered offensive and/or disturbing to some viewers. By viewing and/or interacting with the content you acknowledge and agree that it is your decision to view and interact with the content and to take the risk that you will experience a negative emotional response or reaction to the nature of the content.”

## 12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

## 13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

## 14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code. Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

## 15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.

- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

## 16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application.  Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

## 17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

## 18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

## 19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English  when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration*  Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

## 20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

### Notice of Collection and Use of Personal Information

Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below: Instructors should edit this section according to the systems and technologies to be used in this specific course (e.g. If using Proctortrack, remove any reference to Respondus)

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Instructor to list all relevant components.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to:  Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

**By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.**

## 21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g.  during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

## 22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

## 23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University. The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

## 24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

## 25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT
**Cybersecurity in Critical Infrastructure**
**2024-25**

## 1. Course Details & Important Dates*

| Term | Course Type | Day | Time | Location | CRN# |
|---|---|---|---|---|---|
| 2024-25 | Online | | | | |

| Classes Start | Classes End | **Last day to drop course without academic consequence** | Final Exam Period |
|---|---|---|---|
| | | | |

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

## 2. Instructor Contact Information

| Instructor Name | Office | Phone | Email |
|---|---|---|---|
| Khalil El-Khatib | | | Canvas Email |
| Office Hours: by appointment | | | |

| Laboratory/Teaching Assistant Name | Office | Phone | Email |
|---|---|---|---|
| | | | |
| Office Hours: by appointment | | | |

## 3. Course Description

Today, every nation has identified several critical infrastructures that are essential for national and economic security. The Canadian National Strategy has identified 10 CI sectors including information and communication technology, energy and utilities, water, manufacturing, food, government, health, safety, finance, and transportation. Ensuring the security and resiliency of these infrastructure is a key priority for the Canadian government and for every government around the world. The course will teach students about identifying physical and cybersecurity threats that can affect the security of a critical infrastructure, and also understanding and developing integrated risk management strategies

## 4. Learning Outcomes

On successful completion of the course, students will be able to:

- Understand the key concepts in critical infrastructure protection,
- Understand the security requirements and considerations for critical infrastructure.
- Understand interdependencies among critical infrastructures.
- Perform risk analysis for critical infrastructure protection.
- Develop an integrated risk management strategies for critical infrastructure protection.

## 5. Course Design

The lectures for the course are designed to include a fair amount of discussion with the necessary theory to meet the level of a graduate course. Students are expected to attend all lectures. To succeed in this course, it is highly advisable that students:

1. Read the notes/textbook/papers prior to the lecture to have an idea of the new concept(s) that will be introduced that day.
2. During the lecture, make sure the new topic(s) being introduced is understood. Ask questions.
3. Pay attention to lectures.
4. After the lecture, review the material studied during that session.
5. See the professor during office hours or schedule extra consultation time, if necessary.
6. Assignments are designed to provide students with hands-on learning on the concepts studied in the course.
7. The Final Project is designed so that students will become very familiar with a specific topic, and will be able to write a survey paper on that area as well as articulate a presentation to the class.

## 6. Outline of Topics in the Course

| Week # | Date | Topics | Readings |
|---|---|---|---|
| 1 | | Introduction to Critical Infrastructure | • |
| 2 | | The convergence of Physical and cybersecurity | • |
| 3 | | Industrial Control Systems | • |

| | | | |
|---|---|---|---|
| 4 | | Critical Infrastructure Threats | • |
| 5 | | Energy and Utilities Sector | • |
| 6 | | finance and Government Sector | |
| 7 | | Risk Assessments | • |
| 8 | | Incident Response | • |
| 9 | | Policy & Governance | • |
| 10 | | Student Presentations | • |
| 11 | | Student Presentations | |
| 12 | | | |
| | | | |
| | | | |

***Important Notes:** Adjustment of scheduled lectures might be made in accordance with any unforeseen circumstances during the semester.*

## 7. Required Readings

Students will be assigned various up-to-date research papers to read on each topic. students might wish to read some of the following textbooks, including:

- Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, Scada, and Other Industrial Control Systems, by Eric D. Knapp and Joel Thomas Langill
- Critical Infrastructure Protection A Complete Guide, by Gerardus Blokdyk

*Additional readings may be assigned or recommended during the course.*

## 8. Evaluation Method

The course has only a final term paper and presentation. Students are encouraged to pick a topic related to critical infrastructure protection, do a literature review about the topic, present it to the whole class, and finally write a report about it.

## 9. Assignments and Tests

There are no tests in this course.

## 10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

## 11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.
Disclaimer: "The content you are about to view contains sensitive subject matter that may be considered offensive and/or disturbing to some viewers. By viewing and/or interacting with the content you acknowledge and agree that it is your decision to view and interact with the content and to take the risk that you will experience a negative emotional response or reaction to the nature of the content."

## 12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

## 13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

## 14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code.

Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

## 15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

## 16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application.  Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

## 17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

## 18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

## 19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English  when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration* Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

## 20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

**Notice of Collection and Use of Personal Information**

Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Internet and Webcam.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

**By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.**

## 21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g. during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

## 22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

## 23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University. The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

## 24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

## 25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

Revised August 2023

FACULTY OF BUSINESS AND IT

# INFR 6110G: Global Cybersecurity Threats

Course outline for **Fall 2023**

## 1. Course Details & Important Dates*

| Term | Course Type | Day | Time | Location | CRN # |
|---|---|---|---|---|---|
| FALL 2023 | | | | | |

| Classes Start | Classes End | **Last day to drop course without academic consequence** | Final Exam Period |
|---|---|---|---|
| September 5, 2023 | December 4, 2023 | October 2, 2023 | December 6 - 16, 2023 |

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

## 2. Instructor Contact Information

| Instructor Name | Office | Phone | Email |
|---|---|---|---|
| | | | |
| Office Hours: | | | |

| Laboratory/Teaching Assistant Name | Office | Phone | Email |
|---|---|---|---|
| | | | |
| Office Hours: | | | |

## 3. Course Description

In a hyper connected world, threat actors see no limits or boundaries to their targets, and cybersecurity incidents can have major effects on individuals, organizations, and governments around the world. Cybersecurity managers find themselves obliged to learn about the latest cyber threats to protect their digital assets. The objective of this course is to learn about the global power dynamics, conflicts and risk factors in cyberspace; cyber-based sabotage, espionage and subversion activities; and major and recent cyber incidents that have unfolded internationally and to evaluate their implications. Students will also go over recent threat reports from various security organizations to learn about how the global cyberthreat landscape is evolving.

## 3. Learning Outcomes

On the successful completion of the course, students will be able to:

- Describe the nature of cyber threats at the global level

- Understand how leading organizations, regulators and governments around the world analyze and prepare for global threats.
- Analyze various threat reports from various sources to understand the cyber threat Landscape and develop cybersecurity strategies.
- Analyze the intrigued world of global cybersecurity threats, opportunities, risks, and policies.
- Develop some actionable information on emerging global cybersecurity threats.

## 5. Course Design

The course will be structured to include a variety of pedagogy exercises including case studies, reports analysis, guest speakers, lectures, classroom discussions, and student presentations. Students are expected to participate in all discussions in the classroom. For some activities, teams maybe be formed by the instructors, with each team assigned different activities,

## 6. Outline of Topics in the Course

Given the dynamic nature of the course that focuses on state-of-the-art threats, the topics in the course are determined on a year-to-year basis. Some core topics are included in the table below:

| Lecture # | Date | Time | Topics | Details of topics to be covered in the course, by unit or by week |
|---|---|---|---|---|
| 1 | | | Fundamentals of Cyber warfare | |
| 2 | | | Global Cyber threats | |
| 3 | | | Analysis of cyber incidents | |
| 4 | | | Geopolitics and Cyber power | |
| | October 9, 2023 | | Thanksgiving Day, no scheduled academic activities. | |
| STUDY BREAK | October 10 to 15, 2023 | | Study Break, no scheduled academic activities. | |
| 5 | | | Hacktivism | |
| 6 | | | Cyber Deterrence and surveillance | |
| 7 | | | Global issues related to ethics and legality of cyber warfare | |
| | | | Student Presentations | |
| | | | Student Presentations | |
| | December 5, 2023 | | Study break, no scheduled academic activities. | |

## 7. Required Texts/Readings

There is no textbook required for this course.
Students will be assigned various articles on each topic, including the latest threat reports from various security organizations.
Students will also be assigned cases and students finding weekly news cybersecurity nuggets.

*Additional readings may be assigned or recommended during the course.*

## 8. Evaluation Method

Students will be evaluated based on their participation in the class.
Students will also be required to submit a cumulative "portfolio" assignment of "what happened in the 12 weeks during the term." Here is a tentative percentage for each work:

- Class participation: 50%
- Presentation: 30%
- Peer evaluation 20%

*Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found at: Ontario Tech's Academic regulations*

## 9. Assignments and Tests

[Provide a schedule of term assignments (format, description, length, due dates, submission requirements, etc.), tests and examinations. If collaborative group work is component of the course, include a statement that sets out the roles and roles and responsibilities of members for their own work and for the work of the other members of the group. Detail also how missed/late assignment and medical excuses will be managed in accordance with Faculty rules.]

**Step #1**: If you have midterms/term tests in your course, you **MUST** include the "Missed Term Test" paragraph below.

**Missed Term Test**
Students who miss a midterm or term test may submit a request for deferral using an Academic Consideration form, along with supporting documentation to the Faculty Advising offices within three (3) working days. We do not require students to submit Ontario Tech University Medical Statements at this time. If a midterm or term test is missed for approved reasons, the weight of the missed component will be added to the final (or select this sentence: a make-up test will be offered at a date set by the course instructor). If you miss the midterm or term test and do not follow the procedure above, you will receive a score of zero on the missed component.

All forms can also be found through MyOntarioTech or on the Ontario Tech University website.

**Step #2:** If you have no midterms/term tests in your course, however have coursework/ quizzes/ assignments you **MUST select** Option #1 OR Option #2 of the "Missed Course Work" paragraphs (below).

If you also have a coursework/quiz/assignment component in addition to midterms/term tests you **MUST** include the "Missed Term Test" paragraph (above) AND select Option #1 OR Option #2 of the "Missed Course Work" paragraphs(below).

**Select - Option #1: Missed Course Work**
Coursework missed for medical or serious personal reasons must be documented and reported to the instructor within three (3) working days of the missed work using an Academic Consideration form. Coursework includes, but is not limited to, quizzes; written assignments; participation; case

studies; etc… If missed coursework totals more than 25% of the final grade, this must be documented through the FBIT Academic Advising office. The weight of the missed course component will be reweighted to … (or select this sentence: the instructor will contact you regarding a make-up assignment) If you miss coursework and do not notify the instructor within the three (3) working day deadline, you will receive a score of zero on the missed component.

**Or Select - Option #2: Missed Course Work**
To cover any coursework missed due to unexpected absences, the lowest (out of xx) quizzes/assignments/journals/seminars/etc… will be dropped. Please note that this provision is not a free ticket to skip coursework as there will be no make-up quizzes/assignments/journals/seminars/etc for the missed ones.

(**REMOVE** this paragraph **after you have read**): The object of these paragraphs is to note that any missed assignment/quiz/coursework that is worth LESS than 25% of the final grade in the course will be **handled by the course instructor NOT** the FBIT Advising Office. As in the past, any missed final exam or test/assignment/midterm worth 25% or more of the final grade will be administered through the FBIT Advising Office.

## 10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

**By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.**

## 11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain [Instructors should provide examples that are applicable to the course subject matter – e.g. graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality]. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content. [Instructors should publish a warning statement in advance so as to give students adequate opportunity to make a choice to avoid any such matter. The following is a sample disclaimer: "The content you are about to view contains sensitive subject matter that may be considered offensive and/or disturbing to some viewers. By viewing and/or interacting with the content you acknowledge and agree that it is your decision to view and interact with the content and to take the risk that you will experience a negative emotional response or reaction to the nature of the content."]

## 12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

## 13. Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to a Support Worker, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. Support Workers can offer help and resolution options which can include safety plans, accommodations, mental health support, and more. To make an appointment with a Support Worker, call 905.721.3392 or email studentlife@ontariotechu.ca
- Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information

## 14. Students with Disabilities

Accommodating students with disabilities at Ontario Tech is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

**When on campus access is allowed,** students taking courses on North Oshawa campus can visit Student Accessibility Services in Shawenjigewining Hall.  Students taking courses on the **downtown Oshawa campus** can visit Student Accessibility Services in Charles Hall, Room 225.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm.  For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

**When on campus access is allowed**, students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes AT LEAST seven (7) days before the date of the test.

Students must register for final exams by the registration deadline, which is typically two (2) weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

## 15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so. (See Appendix A for more information about how students can raise concerns about academic matters.)
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

## 16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. This information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech's Student Learning Centre.

## 17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

## 18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

## 19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and **when on campus access is allowed,** may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their Student ID card (campus ID) when **in-person examinations are allowed.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit a Request for Accommodation for Religious Obligations to the Faculty concerned as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found at Ontario Tech's Procedures for Final Examinations.

## 20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of [Insert Faculty name] encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech

University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

**Notice of Collection and Use of Personal Information**
Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below: [Instructors should edit this section according to the systems and technologies to be used in this specific course (e.g. If using Proctortrack, remove any reference to Respondus)]

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: [Instructor to list all relevant components].

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech. Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

**By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.**

## 21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring a campus environment that is equitable and inclusive. Requirements to refrain from harassment and discrimination apply broadly to the classroom, including in lectures, labs and practicums, as well as through the use of sanctioned and unsanctioned technological tools that facilitate remote learning, e.g. class and other chat functions, video conferencing, electronic mail and texts, and social media content amongst or about University students, faculty and staff.

## 22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

## 23. Copyright Notice

All teaching materials provided by the instructor throughout the course, including, but not limited to, in whole or in part, recorded lectures, slides, videos, diagrams, case studies, assignments, quizzes, and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42. Teaching materials are owned by the faculty member, instructor or other third party who creates such works. The copyright owner(s) reserves all intellectual property rights in and to the teaching materials, including the sole right to copy, reproduce, distribute, and modify the teaching materials. Consistent with the university's Intellectual Property Policy, teaching materials are intended only for the educational use of Ontario Tech University students registered in the course that is the subject of this course outline. Any distribution or publishing of this material (e.g. uploading material to a third-party website) is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the Intellectual Property Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

## 24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

## University Response to COVID-19

The government response to the COVID-19 pandemic is continually evolving. As new information becomes available from federal and provincial public health authorities, the Province of Ontario and the Regional Municipality of Durham, Ontario Tech University will remain nimble and prepared to respond to government orders, directives, guidelines and changes in legislation to ensure the health and safety of all members of its campus community. In accordance with public health recommendations, the university may need to adjust the delivery of course instruction and the availability and delivery mode of campus services and co-curricular opportunities. Ontario Tech University appreciates the understanding and flexibility of our students, faculty and staff as we continue to navigate the pandemic and work together to demonstrate our strong commitment to academic, research and service excellence during these challenging and unprecedented times.

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

OntarioTech UNIVERSITY

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT

# INFR 6120G: Cybersecurity Leadership
# Course outline for XXX

## 1. Course Details & Important Dates*

| Term | Course Type | Day | Time | Location | CRN# |
|---|---|---|---|---|---|
| ---- | | | | Online | |

| Classes Start | Classes End | **Last day to drop course without academic consequence** | Final Exam Period |
|---|---|---|---|
| ---- | ---- | ---- | ---- |

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

**Important Note – Final Exams**

There is no final exam for this course

## 2. Instructor Contact Information

| Instructor Name | Office | Phone | Email |
|---|---|---|---|
| | | | |
| Office Hours: | | | |

| Laboratory/Teaching Assistant Name | Office | Phone | Email |
|---|---|---|---|
| | | | |
| Office Hours: | | | |

## 3. Course Description

This course examines the concept of leadership, how it works and specifically how it may be applied to the specific needs of cybersecurity. This includes leadership in times of normalcy, crisis and continuance. The course includes case discussions, roleplaying exercises and input as available from external cybersecurity experts. The course will be held in a hybrid format, with online and face to face discussions and exercises according to the availability of students.

## 4. Learning Outcomes

On the successful completion of the course, students will be able to:

- Analyze different leadership styles in the context of cybersecurity
- Construct and justify different actions in response to cybersecurity activities and events
- Demonstrate how leadership makes a difference in cybersecurity events
- Debate the strengths and weaknesses of different leadership styles in context

## 5. Course Design

This course is largely discussion-based, with a few lectures on the concepts of leadership and how it is different or similar in different cybersecurity concepts. We will use a case-based and discussion method to tease out the ways in which different leadership styles and the actions of leaders have led to different outcomes. There may well be visiting presenters who will share their expertise of how and when the different styles and requirements of leadership make sense, in ‘normal’, crisis and post-crisis settings. There will be ample opportunity to discuss the governance and leadership issues associated with the cases, as well as in a final ‘war game’ scenario and subsequent debriefing in which students will participate.

## 6. Outline of Topics in the Course

| Week # | Topics | Details of topics to be covered in the course, by unit or by week |
|---|---|---|
| 1 | What do we mean by leadership? From philosophy to sociology through psychology. From stoicism to authoritarianism and beyond. | The Romans, the Greeks, “Great Man” Theory, military leadership, civilian leadership. |
| 2 | Leadership rules. Leadership actions. Leadership versus management. | Leadership styles, how leadership works in context. |
| 3 | Why cybersecurity needs leadership. What is different about cybersecurity? | The different timescales of cybersecurity. The different people and tools of cybersecurity. The similarities between cybersecurity and other areas. |
| 4 | Communication | How, why, when and again, how. |

| | | |
|---|---|---|
| 5 | Normalcy | How to lead in uncertain and normal times, in different kinds of environment. |
| 6 | Crisis | The requirements of a crisis: pro-action, reaction, availability, communication, understanding. |
| 7 | Post-crisis and return to normalcy | What happens next? Who knows? |
| 8 | Legal concerns | The law in Canada and elsewhere as it relates to cybersecurity and why it impacts leadership requirements. |
| 9 | Recognizing and building new leaders in our field and work | Coaching and encouraging. |
| 10 | Incompetency and worse:<br>There is no I in team | How to fail. How to spot failing. Self-assessment and self-regulation. |
| 11 | “War game” | |
| 12 | Debriefing | |

## 7. Required Texts/Readings

There is no specific text assigned for the course. Cases will be assigned on a weekly basis to help discuss the concepts presented. Readings from different texts and articles will be required. All of these will be available in or through the university library (no purchase of texts will be required.)

Additional readings may be assigned or recommended during the course.

## 8. Evaluation Method

This is a course that requires people to participate.

There are weekly case discussions. Students will be expected to prepare and present a case assigned to them at some point during the semester. The presentation and analysis is worth 25% of the final grade for the course.

The ‘war game’ will be a **full day** session in which all students are expected to take part in different roles – it is a reactive simulation that is designed to examine the different ways in which leadership makes a difference in various situations. A report on what transpired is required per student and participation in the debrief session is also required.

War game participation and activity: 20%
Report: 15%
Debrief: 15%

Participation in the weekly sessions/discussions is worth up to 15% of the final grade.

Contribution to the ongoing course educational resource (an OER created and maintained by the class) is worth up to 15% of the final grade and opportunities to contribute will present themselves throughout the course.

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found under Academic Regulations at: Ontario Tech's Academic regulations

## 9. Assignments and Tests

Weekly cases (at least one per student group).
Online and in class discussions (generally, topics will be assigned but can be requested).
OER contributions (to be discussed in class, due by end of semester).

Attendance at the weekly sessions/discussions is therefore mandatory. Up to two may be missed for personal or other reasons without penalty, but given the unique nature of what we are discussing and how, further absences will result in the student being unable to complete the course.

For information on how missed/late assignments and medical excuses are managed, please refer to the university's revised ***Procedures for Consideration of Missed In-Term Course Work and Examinations***

## 10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

## 11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content

## 12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

## 13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

## 14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code. Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

## 15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

## 16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

## 17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

## 18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

## 19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English  when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration*  Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

## 20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

**Notice of Collection and Use of Personal Information**
Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: pressbooks, mentimeter.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

**By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.**

## 21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g. during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

## 22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

## 23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University.  The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

## 24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

## 25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

FACULTY OF BUSINESS AND IT

# INFR6130G: Cybercrime

Course outline for **** 20**

## 1. Course Details & Important Dates*

| Term | Course Type | Day | Time | Location | CRN # |
|---|---|---|---|---|---|
| - | Lecture | - | 3 hours | - | - |

| Classes Start | Classes End | **Last day to drop course without academic consequence** | Final Exam Period |
|---|---|---|---|
| - | - | - | - |

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

**Important Note – Final Exams**
The final exam for this course will be run ON CAMPUS during the regular final exam period. If a student cannot attend due to COVID-19 related international travel restrictions you **must email your course instructor ASAP** (as soon as possible) regarding the possibility of alternate arrangements.

## 2. Instructor Contact Information

| Instructor Name | Office | Phone | Email |
|---|---|---|---|
| Dr. Fletcher Lu | UB3062 | 905-721-8668 ext. 3761 | fletcher.lu@ontariotechu.ca |
| Office Hours: TBA* | | | |

| Teaching Assistant Name | Office | Phone | Email |
|---|---|---|---|
| | | | |
| | | | |

*TBA = To Be Announced

## 3. Course Description

This course covers different manifestations of cybercrime including hacking, viruses and other forms of malicious software. It presents technical and social issues of cybercrime, covers the origins and extent of the cybercrime problem, ethical and legal issues as well as analytical techniques to detect cybercrime.

## 4. Learning Outcomes

On the successful completion of the course, students will be able to:

1. Identify and describe techniques for cyber-fraud, online deception and scams,

2. Distinguish between criminal hacking, and non-criminal hacking.
3. Describe how computer technologies have altered the ways in which theft, terrorism, ransoming, fraud, and identity crimes are committed.
4. Identify and distinguish the various types of viruses and malicious code.
5. Identify and define the primary security technologies used to protect information.
6. Explain the conflicting roles within law enforcement pertaining to investigation vs. intelligence gathering.
7. Identify the legal issues related to various cybercrime activities both domestically and internationally.
8. Describe social issues related to cybercrime including cyberbullying and harassment.

## 5. Course Design

Many of the topics covered in this course are contemporary in nature and not adequately covered by any single textbook. Due to this contemporary nature, extensive online reading and material are required. Students are strongly recommended to attend lectures as not all material necessary for exams and assignments may appear on printed lecture notes, but instead are drawn from articles and postings that are cited and discussed during lectures. Thus, students will need to take comprehensive notes during lectures or be prepared to obtain another student's notes for any missed lectures. For missed lectures, it is the responsibility of the student to obtain such notes from another student and NOT from the instructor.

Online interactive computer tools will be used during lectures, thus students must bring their laptop with them to lectures and it is strongly encouraged to bring an internet cable to help reduce lag time due to the slower wireless transfer speeds.

## 6. Outline of Topics in the Course

| Week # | Date | Time | Topics* |
|---|---|---|---|
| 1 | - | - | 1. Introduction and Overview<br>• Introduction to course<br>• Overview of assignments, grading<br>• Defining cybercrime<br>• Current events, issues |
| 2 | - | - | 2. Online fraud, email spam and scams<br>• Peer to peer network dangers<br>• Who is tracking your online activities<br>• Phishing, Pharming, Spams and scams<br>• Misinformation, Deception & Deep Fakes |
| 3 | - | - | 3. Analytics for Crime Detection<br>• Modeling methods<br>• Probabilistic Association Rules<br>• Training & outlier techniques |
| 4 | - | - | 4. Computer viruses, spyware and attacks<br>• Approaches, techniques and medium<br>• Protection methods and mechanisms<br>• DOS attacks |
| 5 | - | - | 5. Theft, piracy and security issues<br>• Theft and protections of identity and data<br>• Approaches to commit identity and data theft |

| | | | |
|---|---|---|---|
| | | | • Legal and technological protections<br>• Smartphone and WiFi issues<br>• Midterm Review |
| 6 | - | - | Midterm |
| 7 | - | - | 6. Online Surveillance<br>• Surveillance through mobile and computer devices<br>• Government, individual and business surveillance tactics<br>• Tracking systems |
| 8 | - | - | 7. Bullying, pornography and sex crimes<br>• Stalking, bullying and harassment<br>• Definitions, laws and protections<br>• Sexual predators<br>• Security measures<br>• Protections |
| 9 | - | - | 8. Advanced Techniques<br>• Misinformation, DeepFakes and AI in cybercrime<br>• Techniques for detection and prevention |
| 10 | - | - | Project Presentations |
| 11 | - | - | Project Presentations |
| 12 | - | - | Final Exam |

*topic schedule subject to change

## 7. Required Texts/Readings

There is no required textbook, however additional readings are assigned or recommended during the course.

## 8. Evaluation Method

| | Due Date[1] | Percentage of Final Grade* |
|---|---|---|
| **Assignment 1** | - | 15% |
| **Midterm** | - | 15% |
| **Assignment 2** | - | 15% |
| **Term Project** | *Written Report portion*:<br>- | 20% |
| | *Oral Presentation portion:*<br>- | 20% |
| **Final Exam** | - | 15% |

1. Due dates are subject to change, be sure to check the course Canvas account for updates/changes.
2. TBD = to be determined

**Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found at: Ontario Tech's Academic regulations*

## 9. Assignments and Tests

All assignments must be submitted on or before the due date and time. No late submissions will be accepted unless accompanied by an acceptable excuse (medical or compassionate with supporting documentation) that has been approved by the instructor. All late submissions without an approved excuse by the instructor will receive a mark of zero. Note: technical difficulties due to such issues as a slow or dropped connection, lag on server, etc. are NOT approvable excuses. Students are strongly encouraged to avoid such difficulties by following a principle of submitting both early and often before the due date/time. The principle behind ‘early and often’ submission is that as soon as you have some work done such as part of one question, submit it so you always avoid getting a zero due to a missed or late assignment as you will have at least something submitted. And then keep resubmitting as you complete more of the assignment material.

Assignments will be posted on the Canvas system with submissions handed in electronically through Canvas. The term project has both a written and oral presentation component. The written component is due all on the same due date. For the project, students will work in groups and each group will be randomly assigned to a presentation date. Each group member is required to participate in the oral presentation. It is the responsibility of the group members to ensure that work is equitably shared among the group’s members.

**Missed Term Test**
Students who miss a midterm or term test may submit a request for deferral using an Academic Consideration form, along with supporting documentation to the Faculty Advising offices within three (3) working days. We do not require students to submit Ontario Tech University Medical Statements at this time. If a midterm or term test is missed for approved reasons, the weight of the missed component will be added to the final. If you miss the midterm or term test and do not follow the procedure above, you will receive a score of zero on the missed component.

All forms can also be found through MyOntarioTech or on the Ontario Tech University website.

**Missed Course Work**
Coursework missed for medical or serious personal reasons must be documented and reported to the instructor within three (3) working days of the missed work using an Academic Consideration form. Coursework includes, but is not limited to, quizzes; written assignments; participation; case studies; etc… If missed coursework totals more than 25% of the final grade, this must be documented through the FBIT Academic Advising office. The weight of the missed course component will be reweighted to the final exam. If you miss coursework and do not notify the instructor within the three (3) working day deadline, you will receive a score of zero on the missed component.

## 10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech’s Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

**By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.**

## 11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.

## 12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

## 13. Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to a Support Worker, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. Support Workers can offer help and resolution options which can include safety plans, accommodations, mental health support, and more. To make an appointment with a Support Worker, call 905.721.3392 or email studentlife@ontariotechu.ca
- Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information

## 14. Students with Disabilities

Accommodating students with disabilities at Ontario Tech is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

**When on campus access is allowed,** students taking courses on North Oshawa campus can visit Student Accessibility Services in Shawenjigewining Hall. Students taking courses on the **downtown Oshawa campus** can visit Student Accessibility Services in Charles Hall, Room 225.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

**When on campus access is allowed**, students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes AT LEAST seven (7) days before the date of the test.

Students must register for final exams by the registration deadline, which is typically two (2) weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

## 15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so. (See Appendix A for more information about how students can raise concerns about academic matters.)
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

## 16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. This information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech's Student Learning Centre.

## 17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

## 18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

## 19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and **when on campus access is allowed,** may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their Student ID card (campus ID) when **in-person examinations are allowed.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit a Request for Accommodation for Religious Obligations to the Faculty concerned as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found at Ontario Tech's Procedures for Final Examinations.

## 20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of [Insert Faculty name] encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

**Notice of Collection and Use of Personal Information**

Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Mentimeter (www.menti.com) for participation polling.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech. Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

**By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.**

## 21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring a campus environment that is equitable and inclusive. Requirements to refrain from harassment and discrimination apply broadly to the classroom, including in lectures, labs and practicums, as well as through the use of sanctioned and unsanctioned technological tools that facilitate remote learning, e.g. class and other chat functions, video conferencing, electronic mail and texts, and social media content amongst or about University students, faculty and staff.

## 22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

## 23. Copyright Notice

All teaching materials provided by the instructor throughout the course, including, but not limited to, in whole or in part, recorded lectures, slides, videos, diagrams, case studies, assignments, quizzes, and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42. Teaching materials are owned by the faculty member, instructor or other third party who creates such works. The copyright owner(s) reserves all intellectual property rights in and to the teaching materials, including the sole right to copy, reproduce, distribute, and modify the teaching materials. Consistent with the university's Intellectual Property Policy, teaching materials are intended only for the educational use of Ontario Tech University students registered in the course that is the subject of this course outline. Any distribution or publishing of this material (e.g. uploading material to a third-party website) is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the Intellectual Property Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

## 24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

## University Response to COVID-19

The government response to the COVID-19 pandemic is continually evolving. As new information becomes available from federal and provincial public health authorities, the Province of Ontario and the Regional Municipality of Durham, Ontario Tech University will remain nimble and prepared to respond to government orders, directives, guidelines and changes in legislation to ensure the health and safety of all members of its campus community. In accordance with public health recommendations, the university may need to adjust the delivery of course instruction and the availability and delivery mode of campus services and co-curricular opportunities. Ontario Tech University appreciates the understanding and flexibility of our students, faculty and staff as we continue to navigate the pandemic and work together to demonstrate our strong commitment to academic, research and service excellence during these challenging and unprecedented times.

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT

# Financial Implications of Cyber Risk

**2024-25**

## 1. Course Details & Important Dates*

| Term | Course Type | Day | Time | Location | CRN# |
|---|---|---|---|---|---|
| 2024-25 | Lecture | | | | |

| Classes Start | Classes End | **Last day to drop course without academic consequence** | Final Exam Period |
|---|---|---|---|
| | | | |

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

## 2. Instructor Contact Information

| Instructor Name | Office | Phone | Email |
|---|---|---|---|
| Dr. Julia Zhu | UB3036 | | Canvas Email |
| Office Hours: by appointment | | | |

| Laboratory/Teaching Assistant Name | Office | Phone | Email |
|---|---|---|---|
| | | | |
| Office Hours: by appointment | | | |

## 3. Course Description

This course attempts to provide a comprehensive and integrated introduction to cyber risk. We use contemporary models in accounting, finance, and economics to analyze and understand financial costs and implications of cyber risk. The focus will be on various issues regarding the causes and determinants of data privacy breaches, and the adverse consequences of cyberattacks.

Prerequisite(s):

## 4. Learning Outcomes

On the successful completion of the course, students will be able to:

- Demonstrate financial costs and implications of cyber risk
- Identify causes and determinants of data privacy breaches
- Evaluate the adverse consequences resulting from cyberattacks
- Estimate economic importance and financial consequences of cyberattacks
- Improve communication, teamwork, analytical, academic writing skills

## 5. Course Design

The course will be presented in the format of lectures, discussions, case study, simulated research projects, presentations, and term papers. A good understanding of the research papers and contemporary academic concepts is necessary for successful completion of this course. Students are therefore urged to work conscientiously on all assigned problems, questions, and readings. The practical implications will be analyzed through case study.

Lectures focus on the material presented in the distributed academic papers and general discussion relating to the topic(s) outlined in the lecture schedule. Students are expected to read the assigned academic journal articles and readings before class, and be prepared for class discussion. *Your instructor may not necessarily cover all of the materials in the paper, but it is the responsibility of the student to understand the concepts presented in the paper and lectures. If you are unsure of any of the concepts, please take the initiative to ask the instructor during class.*

Students requiring assistance are encouraged to speak to their instructor during class or during office hours. Should you wish to meet with the instructor outside of office hours, please email first to make an appointment. Students should get into the habit of making and keeping business appointments. Should you fail to attend or cancel the appointment at least 24 hours in advance, you will lose the right to book another appointment.

Email is commonly used by students to communicate with their instructor. However, it does limit the effectiveness of the communications and may not be the best way for instructors to answer student questions, especially those requiring an explanation of concepts covered in this course or some personal concerns. Therefore, the instructor may request a telephone call or personal/online meeting. *Your instructor will inform you as to her expectations about emails.*

Any surfing of the Internet during lectures that is not directly related to the class discussion is distracting and strictly forbidden. Additionally, the use of any electronic devices (e.g., cellular phones, Blackberrys, iphones) for e-mailing, text-messaging, etc. is strictly prohibited. Please turn OFF your phone before the beginning of each lecture. The laptop is to be used in class for academic purposes only.

## 6. Outline of Topics in the Course

| Tentative Course Schedule, 2024-2025 | | | |
|---|---|---|---|
| **Lecture #** | **Date** | **Topics** | **Material Covered** |
| Lecture 1 | | Overview | Course Outline |
| | | Introduction | Freeze, 2019;<br>Bank of Canada, 2019 |
| Lecture 2 | | Cyber Risk in Accounting and Finance | Deloitte, 2016;<br>Institute of Internal Auditors, 2018;<br>Interpol, 2020 |
| Lecture 3 | | Research methods in Finance | Amir et al., 2018;<br>Richardson et al., 2019 |
| Lecture 4 | | Data Breach Investigations Report and | AICPA, 2018;<br>PSC, 2018;<br>Verizon, 2019 |
| | | Case study | |
| Lecture 5 | | Accounting audits | Chichernea, Holder, Petkevich, and Robin, 2018 |
| Lecture 6 | | Trade secrets | Ettredge, Guo, and Li, 2018 |
| ***Family Day, no scheduled academic activities***<br>***Study Break, no scheduled academic activities*** | | | |
| Lecture 7 | | Board-level technology committees | Higgs, Pinkser, Smith, and Young, 2016 |
| Lecture 8 | | Financial Costs of Cyber Risk | Deloitte Development LLC, 2018;<br>Lloyd’s, 2017;<br>Rajgopal and Srinivasan, 2016 |
| | | Case study | |
| Lecture 9 | | Cyber risk disclosure | Amir et al., 2018;<br>Hilary et al., 2016 |
| Lecture 10 | | Financial reports and audit fees | Smith et al., 2019;<br>Lawrence et al., 2018 |
| Lecture 11 | | Mixed effects of cyberattacks on stock market | Gatzlaff and McCullough, 2010;<br>Richardson et al., 2019;<br>Spanos and Angelis, 2016 |
| Lecture 12 | | Private-sector firms | Gordon et al., 2015;<br>Gordon et al., 2018 |

***Important Notes:*** *Adjustment of scheduled lectures might be made in accordance with any unforeseen circumstances during the semester.*

## 7. Required Readings

1. AICPA (American Institute of Certified Public Accountants), 2018. Cybersecurity risk management reporting fact sheet. Available at: www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity-fact- sheet.pdf

2. Amir, E., Levi, S. and Livne, T., 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. Review of Accounting Studies 23, 1177-1206.

3. BoC (Bank of Canada), 2019. Cyber security strategy: Reducing Risk Promoting Resilience. Available at: https://www.bankofcanada.ca/wp-content/uploads/2019/06/cyber-security-strategy-2019-2021.pdf

4. Chichernea, D., Holder, A., Petkevich, A., and Robin, A., 2018. Better audits, better cybersecurity?
   Available at http://www.fmaconferences.org/SanDiego/SanDiegoProgram.htm.

5. Deloitte, 2016. Beneath the surface of a cyberattack: A deeper look at business impacts. Oakland, CA: Deloitte Development LLC.

6. Deloitte Development LLC. 2018. Black market ecosystem: Estimating the cost of ownership. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-black-marketecosystem.pdf.

7. Ettredge, M., Guo, F., and Li, Y., 2018. Trade secrets and cyber security breaches. Journal of Accounting and Public Policy 37, 564– 585.

8. Freeze, Di. 2019. Cybersecurity almanac: 100 facts, figures, predictions and statistics. Cisco/CybersecurityVentures 2019 Cybersecurity Almanac. Available at https://cybersecurityventures.com/cybersecurity-almanac-2019/

9. Gatzlaff, K.M., McCullough, K.A., 2010. The effect of data breaches on shareholder wealth. Risk Management and Insurance Review 13, 61-83.

10. Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L., 2015. Externalities and the magnitude of cybersecurity underinvestment by private sector firms: a modification of the Gordon-Loeb model. Journal of Information Security 6, 24-30.

11. Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. 2018. Empirical evidence on the determinants of cybersecurity investments in private sector firms. Journal of Information Security 9,133-153.

12. Higgs, J., Pinkser, R., Smith, T., and Young, G. 2016. The relationship between board-level technology committees and reported security breaches. Journal of Information Systems 30, 79–98.

13. Hilary, G., Segal, B., Zhang, M.H., 2016. Cyber-risk disclosure: Who cares? Unpublished working paper, Georgetown University.

14. IIA (Institute of Internal Auditors), 2018. The future of cybersecurity in internal audit. A joint research report by the internal audit foundation and crowe Horwath. Available at: https://bookstore.theiia.org/the-future-of-cybersecurity-in-internal-audit

15. Interpol, COVID-19 Cybercrime Analysis Report - August 2020.

16. Lawrence, A., Minutti-Meza, M., Vyas, D., 2018. Is operational control risk informative of financial reporting deficiencies? Auditing 37, 139-165.

17. Lloyd’s, 2017. Closing the gap. Insuring your business against evolving cyber threats, http://www.lloyds.com/lloyds/about-us/what-do-we-insure/what-lloyds-insures/cyber/cyber-riskinsight/closing-the-gap.

18. PSC (Public Safety of Canada), 2018. Canada’s vision for security and prosperity in the digital age. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

19. Rajgopal, S., Srinivasan, S., 2016. Why the market Yawned when Yahoo was hacked. The Wall Street Journal. Available at: https://www.wsj.com/articles/why-the-market-yawned-when-yahoo-washacked-1475537076.

20. Richardson, V.J., Smith, R.E., and Warson, M.W., 2019. Much ado about nothing: the (lack of) economic impact of data privacy breaches. Journal of Information System, 33 (3): 227–265.

21. Smith, T., Higgs, J.L. and Pinsker, R., 2019. Do auditors price breach risk in their audit fees?” Journal of Information Systems 33, 177-204.

22. Spanos, G. and Angelis, L., 2016. The impact of information security events to the stock market: a systematic literature review. Computers and Security 58, 216-229.

23. Verizon, 2019. Data Breach Investigations Report. Available at https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf.

*Additional readings may be assigned or recommended during the course.*

## 8. Evaluation Method

| **Evaluations** | **Weights** | **Due dates** |
|---|---|---|
| In class presentation | 15% | |
| Paper summary | 15% | |
| Simulated project 1 | 20% | |
| Simulated project 2 | 20% | |
| Term paper | 30% | |
| | 100% | |

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found under Academic Regulations at: Ontario Tech's Academic regulations

## 9. Assignments and Tests

### Paper Summary, Simulated Projects, and Term Papers:

Paper summary, simulated projects, and term papers are **individual** assignments.

Late submissions for above assignments will be accepted with a 20% **per day** penalty. Late submissions (penalty or not) are NOT accepted 2 days after the due date.

### Missed In-Term Course Work

A request for consideration for missed course work worth 20% or less of the final grade must be documented and reported to the instructor in writing within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. Course work includes, but is not limited to: quizzes, written assignments (problem set), participation, case studies, etc. If missed coursework totals more than 20% of the final grade, the request for consideration must be submitted to the Faculty of Business and IT Advising Office and to the course instructor in writing using the Academic Consideration Form, along with supporting documentation. The request must be submitted within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. If approved, the extended deadline of the missed course component will be granted. If a student misses coursework and does not follow the procedure above, they will receive a score of zero on the missed component.

All forms can also be found through MyOntarioTech or on the Ontario Tech University website.

For information on how missed/late assignments and medical excuses are managed, please refer to the university's revised *Procedures for Consideration of Missed In-Term Course Work and Examinations*

## 10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

## 11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.
Disclaimer: "The content you are about to view contains sensitive subject matter that may be considered offensive and/or disturbing to some viewers. By viewing and/or interacting with the content you acknowledge and agree that it is your decision to view and interact with the content and to take the risk that you will experience a negative emotional response or reaction to the nature of the content."

## 12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

## 13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

## 14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code. Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

## 15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

## 16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

## 17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

## 18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

## 19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration* Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

## 20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

**Notice of Collection and Use of Personal Information**
Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Internet and Webcam.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

**By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the**

**technologies and using your personal information for the purposes described in this course outline.**

## 21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g. during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

## 22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

## 23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University. The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

## 24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

## 25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

# Course Outline

## MITS 6810 - Adversarial Machine Learning

### Course Description

This course introduces adversarial attacks and defenses against machine learning models. Covered topics include evasion attacks against learning-based schemes, causative attacks by perturbing training datasets, and an introduction to robust statistics. Additionally, the course provides an overview of attacks against learning-based schemes utilized in some of the cybersecurity applications, such as *Spam Detection* and *Intrusion Detection*. The course provides the latest overview of state-of-the-art Adverserial Machine Learning (AML) schemes, such as *Generative Adversarial Networks* (GAN) and *Adversarial Active Learning*.

### Learning Outcomes

Upon successful completion of the course, students will be able to:

- Describe different categories of attacks against machine learning models.
- Outline different categories of defenses for the development of robust learning-based models.
- Identify vulnerabilities of adaptive learning-based schemes deployed in an adversarial environment.
- Explain the importance of robust statistics and the use of invariant features in developing robust learning-based schemes for different cybersecurity applications.

### Course Design

Course content will be presented to students during assigned lecture periods. Lecture slides will shall be posted on Canvas; however, the lecture slides may not cover some hands-on content, discussions and Q/A discussed in the class. Therefore, students are expected to attend assigned lectures, participate in class discussions as well as take notes to gain the most out of this course.

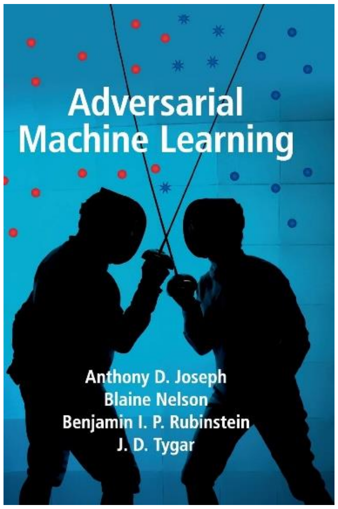
The two assignments and a final project constitute hands-on components and exercises related to the previously discussed topics during assigned lecture periods.

### Outline of Topics in the Course

| Week | Theme | Topics | Reading Assignments |
|---|---|---|---|
| 1 | A framework for Secure Learning | Overview of AML | Chapter 1 |
| 2 | | Characteristics of Adversarial Capabilities | Chapter 3 |
| 3 | | Exploratory vs. Causative Attacks | |
| 4 | | Poisoning Hypersphere Learners | Chapter 4 |

| | | | |
|---|---|---|---|
| 5 | Causative Attacks | Poisoning Retraining with Data Replacement | |
| 6 | | Feature Space Attack: Red herring | *Selection of Research Papers* |
| 7 | | Case Study – Causative Attack against Integrity and Availability | Chapter 5 and Chapter 6 |
| 8 | | Case Study – Active Learning and Malicious Labelers | *Selection of Research Papers* |
| 9 | Exploratory Attacks | Optimal Evasion Attacks | *Selection of Research Papers* |
| 10 | | Evasion of Convex Inducing Classifiers | Chapter 8 |
| 11 | Robust Learning | Robust Statistics for Learning | *Selection of Research Papers* |
| 12 | | Generative Adversarial Networks | *Selection of Research Papers* |
| 13 | | Randomized Classifiers (If time permits) | *Selection of Research Papers* |

## Required Texts/Readings



**Textbook:**

Title: Adversarial Machine Learning
Authors: Joseph, A., Rubinstein, B., Tygar, J.
ISBN-13: 9781107043466

**Example of Papers:**

- Brendel (2017) Decision-Based Adversarial Attacks: Reliable Attacks Against Black-Box Machine Learning Models
- Chen (2019) HopSkipJumpAttack: A Query-efficient Decision-based Adversarial Attack
- Guo (2019) Simple Black-box Adversarial Attacks
- Xiao (2018) Generating Adversarial Examples with Adversarial Networks
- Tramer (2018) Ensemble Adversarial Training: Attacks and Defenses
- Xu (2017) Feature Squeezing: Detecting Adversarial Examples in Deep Neural Networks
- Shafahi (2018) Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks
- Zhang (2019) Theoretically Principled Trade-off between Robustness and Accuracy
- Belle (2020) Principles and Practice of Explainable Machine Learning
- Miller (2014) Adversarial Active Learning.

** Additional readings may be assigned or recommended during the course.*

## Evaluation Method

| Item | Weight (%) |
|---|---|
| Assignment 1 – (Coding & Report) | 25% |
| Assignment 2 – (Coding & Report) | 25% |
| Final Project – Outline | 10% |

| | |
|---|---|
| Final Project – Report/Code | 25% |
| Final Project – Presentation | 15% |

## Assignments and Final Project

### Assignments #1 and #2

For the two assignments (25% each), students will implement studied “causative” and “exploratory” attacks, and defenses methods utilizing different cybersecurity datasets. The students must implement the assignments using Python programming language and document their work (i.e. in report form) on Jupyter notebooks and must use common ML libraries, such as sci-kit learn and TensorFlow. The students may use free Jupyter notebooks provided by Google Colab (as their development environment) or choose to run a local Jupiter instance on their own machines.

### Final Project

The students have the option to either: (a) select an AML research paper to implement or (b) define a learning-based application in cybersecurity that can be attacked/defended using the studied topics. Each student must prepare a project report explaining the selected problem statement, type of threats that selected learning-based scheme may face, demonstrate a successful attack, and present a viable defence. The report (25%) must be accompanied by a python implementation on the Juypyter notebook that can be shared with other students at the end of the term. Additionally, each student must prepare a presentation (15%) that shall be no more than 10 minutes long to discuss their project report with class.

# Appendix D - Existing Courses

UNIVERSITY OF ONTARIO
INSTITUTE OF TECHNOLOGY

Faculty of Business and Information Technology

MITS5100G
Law and Ethics of IT Security
Course outline for Fall 2017

## 1. Course Details & Important Dates*

| Term | Course Type | CRN | Day | Time | Room |
|---|---|---|---|---|---|
| Fall | Lecture | 42996 | Mon | 6:40 pm – 9:30 pm | UA3230 |

| Classes Start | Classes End | Last day to drop course without academic consequence | Final Exam Period |
|---|---|---|---|
| September 11th, 2017 | December 4th ,2017 | October 4th, 2017 | December 6-17th, 2017 |

* for other important dates go to: www.uoit.ca >Current Students >Important Dates and Deadlines

## 2. Instructor Contact Information

| Instructor Name | Office | Phone | Email |
|---|---|---|---|
| David Clark | TBA | 416.642.3688 | david.clark@uoit.ca |
| Office Hours: Before and after class, or by arrangement | | | |

## 3. Course Description

One year ago the big Tech story was Pokémon GO. Today the news is filled with US federal investigations into whether Russian hackers interfered with US federal elections through hacking and online social media manipulation, as well as stories about the surge in ransomware that threatens entire business sectors and even the governments of nation states. And legal issues figured heavily into both. While people wandering the streets playing games on their phones[1] seems to have little in common with cyber attacks on businesses and democratic institutions, both situations point out what happens when technology creates new ways for people to communicate and interact. That is to say, sometimes the law does not keep up very well.

[1] During the summer of 2016 there were many articles in the popular and IT industry media about: the game causing a danger to players and non-players; homeowners suing the publisher Niantic Inc. for trespass (even though no one from Niantic ever sets foot on those properties); calls to regulate the game or the players to remove them from sacred sites like cemeteries and memorials; and even comments that the selection of sites for PokéStops showed unintended racial biases justifying calls for a code of ethics for future programmers of location-based augmented reality games.

Why should we pay attention to this? Because both situations teach us a great deal about why technology, law and ethics sometimes clash. And they also help us understand where the law and technology can work well together.

Information technology in its many forms presents exciting new opportunities for enterprises of all kinds. With each innovation the doors are flung open for new business models to be born and for existing businesses to reinvent themselves. What they all have in common is the need to safeguard information. This is transforming IT departments and professionals into protectors of significant business assets, the custodians of official business records, and the wardens of customers' private information. Laws and the courts impose many of these duties. They also provide critical and effective tools to achieving success in protecting information and other intellectual property.

Yet the very characteristics of e-commerce and online activities that create great opportunities also present significant challenges for the law. And many times, laws are ultimately incapable of providing meaningful protection for computer systems and data. Therefore, as IT Security Professionals, you must understand this interplay between IT and the law. Only then can you anticipate how the law may best be used to achieve IT security in the face of new technologies, and when other tools may be required. Furthermore, when a breach of security actually occurs, you must know how to respond, and even this is shaped by laws and legal principles.

However, as IT Security Professionals responding to the challenges of new technologies, you will also find that the law sometimes fails to provide "real world" guidance about what security methods are acceptable. Moreover, news media are filled with stories about how governments which are are supposed to be protecting citizens are engaging in far-reaching and pervasive monitoring of their electronic communications. Some call these activities illegal. Others defend them and counter that the monitoring is permitted under the law. In these and other circumstances, behaviour that is legally permissible may nevertheless seem improper or ethically challenging. For such cases, you must also have a solid understanding of professional ethics developed by your professional community and peers.

This course will provide an overview of the laws and professional ethics that IT Security Professionals must understand. In the early weeks of the course, we will examine some of the basic ideas and dynamics that will help us analyze and discuss the interplay between technology, law and professional ethics. Later, we will examine one or two substantive areas of law each week, including: e-contracts; e-regulation; online crime; intellectual property; privacy; data breach liability; and we will conclude by examining the concept of ethical hacking, the "white hat" hacker vs. the "black hat" hacker, and those in between.

## 4. Learning Outcomes

On the successful completion of the course, students will be able to:

- Explain basic principles of substantive areas of law covered in the course;
- Demonstrate a basic understanding of the principles, dynamics and tools of computer law;
- Explain how and why online activities and e-business challenge traditional areas of law, and where the law is successful in regulating behavior;
- Demonstrate an understanding of common ethical systems and professional Codes of Ethics;

- Analyze novel situations to identify IT Security issues from the legal and ethical perspectives;
- Explain issues arising from hacking and ethical hacking.

## 5. Course Design

Course content will be delivered through a combination of lectures, discussions and assignments. Success in the course will require students to attend and participate in class. Reading assignments must be completed prior to each class in preparation for the more advanced discussions in the lecture.

The lectures and discussions will provide the core theory. Assignments will include short papers. There will also be a term project. These activities allow students to apply information from course theory and readings and to utilize problem solving and decision-making skills to analyze realistic scenarios.

Through written assignments, examination, and participation in class discussions, students will gain practice in the use of oral and written communication skills. There is a Blackboard course web page which includes a constantly updating calendar of course milestones, assignment and test dates, and so on. Students are expected to log on to the page regularly and to keep informed of course requirements. Items posted on the course site are deemed communicated to the class. Students are required to use the email tool attached to the Blackboard course website if they wish to communicate with the instructor by email.

[The rest of this page left blank intentionally.]

## 6. Outline of Topics in the Course

| Lecture # | Date | Topics |
|---|---|---|
| **Lecture 1** | Sept 11 | • Introduction to Law and Ethics<br>• What is "Law"?<br>• Computer Ethics |
| **Lecture 2** | Sept 18 | • Dynamics, Themes and Skill Sets of Computer Law<br>• Law of the Horse: Code as Law |
| **Lecture 3** | Sept 25 | • Jurisdiction in a Borderless World<br>• Is there a "there" there?<br>• Evidence Law |
| **Lecture 4** | Oct 2 | • e-Contracts<br>• Implied Click Consent & Express Click Consent |
| | Oct 9 | THANKSGIVING – NO CLASSES |
| **Lecture 5** | Oct 16 | • Computer Crime in Canada and the US<br>• Preventing Harmful Conduct |
| **Lecture 6** | Oct 23 | • Privacy Law in Canada, the EU and US<br>• Data Breach Regulation |
| **Lecture 7** | Oct 30 | • Intellectual Property: Part 1<br>• Patents<br>• Trade-mark Law |
| **Lecture 8** | Nov 6 | • Intellectual Property: Part 2<br>• Copyright<br>• Digital Rights Management (DRM)<br>• DMCA (US and others) |
| **Lecture 9** | Nov 13 | • Self-Regulation and Indirect Regulation of Online Activities<br>• White House Cybersecurity Framework |
| **Lecture 10** | Nov 20 | • Regulating Social Media<br>• SPAM - CASL |
| **Lecture 11** | Nov 27 | • Cyberliability<br>• Privacy breach liability<br>• Cyber Insurance as Risk Management |
| **Lecture 12** | Dec 4 | • Ethical Hacking |

## 7. Required Texts/Readings

Fitzgerald, P., Wright, B., & Kazmierski, V., *Looking at Law – Canada's Legal System*, 6th Edition. Toronto: LexisNexis Canada, 2010.

Takach, George S., *Computer Law*, 2nd Edition, Toronto: Irwin Law, 2003.

(*Both textbooks are also available on three-hour reserve from the Reserve Desk at the UOIT Library*).

Each week, **additional mandatory readings** will be posted on the course website on Blackboard that **you will be responsible to prepare**.

## 8. Evaluation Method

The evaluation components and their respective weightings towards the final mark are shown below:

| **Course Component** | **Portion of Final Mark** | **Date Assigned*** | **Date Due*** |
|---|---|---|---|
| First Assignment | 5% | Sept 18 | Sept 25 |
| Second Assignment | 5% | TBA | TBA |
| Midterm Exam | 30% | Oct 16 | Oct 23 |
| Project / Paper | 20% | Oct 23 | Nov 20 |
| Final Exam | 40% | TBA | TBA |

*These dates are subject to change. Changes will be announced in class and on Blackboard.

More specific instructions and deadlines for submission will be provided for each Course Component. You are responsible to review and adhere to them.

*Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found in the Academic Regulations of the UOIT Academic Calendar.*

## 9. Assignments and Tests

All assignments, tests and examinations will be in a "take home" format. You are expected to adhere to the Academic Regulations contained in the UOIT Academic Calendar 2017/18, as well as all other Academic and Administrative Policies of UOIT.

There will be no make-up assignments or tests.

### Missed Term Test

Students who miss a midterm or term test for medical or compassionate grounds may submit a request for deferral along with supporting documentation to the Faculty Advising offices within three (3) working days. Medical deferrals will be comprised of a completed UOIT Medical

Statement form completed by the student and physician within 24 hours of the missed course work. These forms can be found on the UOIT website or the FBIT Announcement Board on Blackboard. If a midterm or term test is missed for approved reasons, the weight of the missed component will be added to the final.

**Missed Course Work**

Coursework missed for medical or serious personal reasons must be documented and reported to the instructor within three (3) working days of the missed work. Medical absences must be accompanied by a UOIT Medical Statement form completed by the student and physician within 24 hours of the missed course work. Coursework includes, but is not limited to, quizzes; written assignments; participation; case studies; etc… If missed coursework totals more than 20% of the final grade, this must be documented through the FBIT Academic Advising office. The weight of the missed course component will be reweighted to the final examination. If you miss coursework and do not notify the instructor within the three (3) working day deadline, you will receive a score of zero on the missed component.

*Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@uoit.ca for support.*

## 10. Accessibility

Accommodating students with disabilities at UOIT is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

Students taking courses on the North Campus Location can visit Student Accessibility Services in the U5 Building located in the Student Life Suite. Students taking courses on the Downtown Oshawa Campus Location can visit Student Accessibility Services in the 61 Charles St. Building, 2nd Floor, Room DTA 225 in the Student Life Suite.

Disability-related support and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Mon-Fri. For more information on services provided, you can visit the SAS website at http://uoit.ca/studentaccessibility

Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@uoit.ca

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here www.uoit.ca/SASexams. Students must sign up for tests, midterms or quizzes AT LEAST seven (7) days before the date of the test.

Students must register for final exams by the registration deadline, which is typically 2 weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

## 11. Academic Integrity

Students and faculty at UOIT share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by UOIT's regulations on Academic Conduct (Section 5.15 of the Academic Calendar) which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with UOIT's regulations on academic conduct does not constitute a defense against its application.

Further information about academic misconduct can be found in the Academic Integrity link on your laptop. Extra support services are available to all UOIT students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found in the Academic Calendar (Section 8).

## 12. Turnitin

UOIT and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents for five academic years. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to UOIT's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet:
http://www.uoit.ca/assets/Academic~Integrity~Site/Forms/Assignment%20Cover%20sheet.pdf

Further information about Turnitin can be found on the Academic Integrity link on your laptop.

## 13. Final Examinations

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. Student ID cards can be obtained at the Campus ID Services, in G1004 in the Campus Recreation and Wellness Centre.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit a Request for Accommodation for Religious Obligations to the Faculty concerned as soon as possible and no later than three week prior to the first day of the final examination period.

Further information on final examinations can be found in Section 5.25 of the Academic Calendar.

## 14. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes and other evaluative material in your courses in the Faculty of Business and Information Technology.

As you may know, UOIT is governed by the *Freedom of Information and Protection of Privacy Act* (“FIPPA”). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that UOIT not disclose the personal information of its students without their consent.

FIPPA’s definition of “personal information” includes, among other things, documents that contain both your name and your Banner ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Faculty of Business and Information Technology encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that UOIT will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@uoit.ca

## 15. Course Evaluations

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of UOIT's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Blackboard, Weekly News and signage around the campus.

## 16. Sexual Violence Policy

UOIT is committed to the prevention of sexual violence in all is forms. For *any* UOIT student who has experienced Sexual Violence, **UOIT can help**. UOIT will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to a Support Worker, who are specially trained individuals authorized to receive confidential disclosures about incidents of sexual violence. Support Workers can offer help and resolutions options which can include safety plans, accommodations, mental health support, and more. To make an appointment with a Support Worker, call 905.721.3392 or email supportworker@uoit.ca
- Learn more about your options at: www.uoit.ca/sexualviolence

## Appendix: Other Policies and Expectations for the Learning Environment

### 1. Effective Learning in the Classroom

The following are suggestions on how to carry out effective learning in your daily studying:

• Pre-Class Preparation:

Before you go to your classroom, you should allow enough time for commuting, and eat a healthy meal or snack. Also, you should ask yourself the following questions:

- Have you *previewed* the reading assignments?
- Have you noted down key insights and questions from your reading?

* *Rule of thumb*: for every hour lecture, you need approximately three hours of outside class studying to reinforce the material learnt in class.

• In-Class Attitude:

In order to get the most out of your lectures, you need to:

- Arrive to class On Time
- Concentrate (be curious and be motivated)
- Be Active:
  - in class discussion
  - in group activities
  - in creative and critical thinking

And you should also AVOID the following:

- Eating 'strong smelling' or 'noisy' food
- Getting involved in side conversations
- Sending signs that scheduled class time is up, i.e. closing up your laptop or standing
- Answering cellular phones in class

• After class:

- Review lecture notes; highlight key points
- Consult instructors or TA for unresolved questions
- Seek help when necessary
- Finish assignments on time

### 2. The use of your laptop in the classroom

The use of laptops often enhances the learning experience. However, there are circumstances when it can be obstructive. Instructors have the right and the responsibility to determine appropriate classroom protocols for student use of laptops. Students refusing to comply with such requests may be requested to remove themselves from the classroom. Students refusing to comply may also be considered to be in violation of our University code of conduct and disciplinary action may result.

- **Examples of appropriate use of laptops**:

- Taking lecture notes
- Course related computing
- Limited messaging for learning purposes
- Download course material from Blackboard

- **Examples of Inappropriate Use of Laptop**

- Watching movies
- Playing computer games
- Social messaging

### 3. Effective team management

The following are suggestions on how to effectively manage your teamwork:

Setting clear objectives
Signing the team contract
Meeting regularly
Conducting effective meetings

- Assigning roles to members
- Staying in touch: meeting; emails; phones
- Managing conflicts effectively

### 4. Managing  Conflict

The following are suggestions on how to resolve conflict that could possibly happen during your studying:

- Have a team contract to guide conflict resolution.
- The team "leader" might send an e-mail to the absent member, and copy all members, asking why he or she missed the meeting.
- Keep an attendance log and use this as part of your peer review process.
- Try to avoid making any decisions that are known to be an issue for an absent member until that person can be reached.

### 5. In the event of the illness

In the event of illness, you are suggested to:

- Please stay home so as not to spread it to others
- Contact your Academic Advisor by email or phone right away – not your instructor.

The Academic Advisors will organize any assignment, test or lab adjustments if needed.
You can find your academic advisor contact information at:
http://www.businessandit.uoit.ca/people/academic-advisors.php

- Also check the following website http://www.cdc.gov for further health and wellness information.

### 6. Academic Planning and General Information

Please follow the link below to view our academic resources and calendar.  This link will provide you with information pertaining to Grade point average (GPA), Academic Standing Requirements, Internship Programs, Graduation Information, etc.
https://uoit.ca/current-students/index.php

**Other links of interest include:**

http://www.businessandit.uoit.ca/undergraduate/index.php for information pertaining to **FBIT Undergraduate Programs**

http://www.gradstudies.uoit.ca/ for information on **Graduate Programs**

https://uoit.ca/current-students/campus-services/ for information on **Campus Services**

http://www.businessandit.uoit.ca/about/student-societies/index.php for information pertaining to **Student Societies**

July 2022

Faculty of Business and Information Technology

MITS6900G Blockchain Foundation and Technology

Course outline for **FALL 2022**

## 1. Course Details & Important Dates*

| Term | Course Type | Day | Time | Location | CRN # |
|---|---|---|---|---|---|
| FALL 2022 | Lecture | Tuesday | 5:10PM – 8:00PM | UA2120 | 44919 |

| Classes Start | Classes End | Last day to drop course without academic consequence | Final Exam Period |
|---|---|---|---|
| September 6, 2022 | December 5, 2022 | October 3, 2022 | December 7 – 16, 2022 |

* Visit https://ontariotechu.ca/current-students/academics/important-dates-and-deadlines.php

## 2. Instructor Contact Information

| Instructor Name | Office | Phone | Email |
|---|---|---|---|
| Sheikh Ahmed Munieb | UB2018 | 905.721.8668<br>Ext: 5361 | Ahmed.sheikh@ontariotechu.ca |
| Office Hours: By Appointment<br>Tuesday: 12PM – 1:00PM | | | |

| Laboratory/Teaching Assistant Name | Email |
|---|---|
| Divyesh Savani | divyeshlallubhai.savani@ontariotechu.net |

## 3. Course Description

This course introduces blockchains from a technical perspective. Students will learn: the fundamentals of blockchains, cryptocurrencies, and dApps; the key business and value drivers of blockchain services; application development fundamentals, best practices, and supportive technologies; economic drivers and bleeding-edge trends. This course includes the development and deployment of a custom blockchain using Python, followed by multiple smart contract implementations using Solidity.

## 4. Learning Outcomes

On the successful completion of the course, students will be able to:

- demonstrate and verbalize a deep understanding of blockchains and their technical underpinnings
- understand the economic and business drivers of blockchain and web 3.0
- compare and contrast blockchain technologies, their use cases, and emerging technologies
- architect, develop, and deploy basic blockchain solutions using industry-standard tools and languages

## 5. Course Design

Course content will be presented to students during the assigned lecture periods. Some lectures will include hands-on components and exercises. Lecture slides will be posted on Canvas, however some hands-on content and discussions or Q/A in the class may not be covered in the lecture slide. Students should plan to attend all lectures and take notes to get the most out of this course.

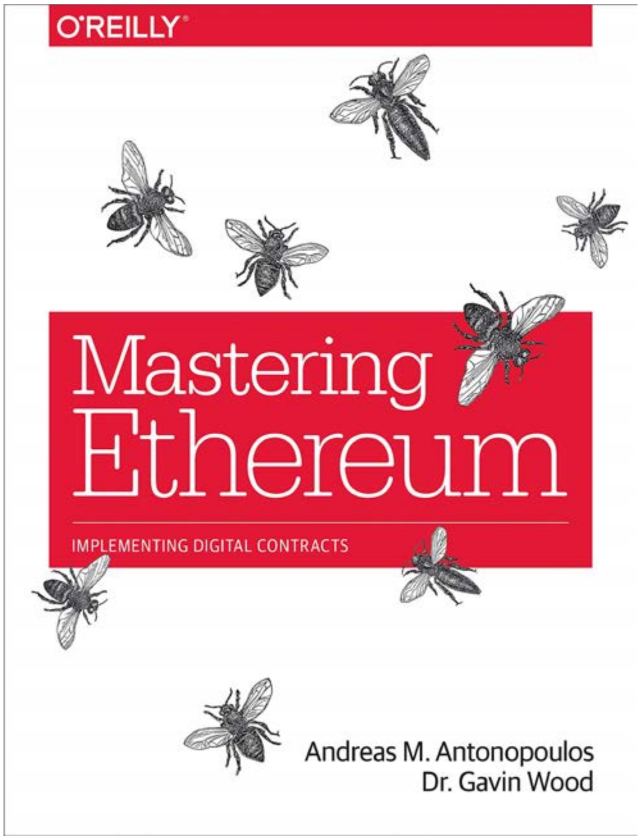
## 6. Outline of Topics in the Course

| Lecture # | Date | Time | Topics | Details of topics to be covered in the course, by unit or by week |
|---|---|---|---|---|
| 1 | September 6th ,2022 | 5:10PM – 8:00PM | Blockchain – Introduction | |
| 2 | September 13th ,2022 | 5:10PM – 8:00PM | Blockchain – Technical Deep-Dive | |
| 3 | September 20th ,2022 | 5:10PM – 8:00PM | Blockchain – Development (Python & Flask) | |
| 4 | September 27th, 2022 | 5:10PM – 8:00PM | Cryptocurrency – Bitcoin 1 | |
| 5 | October 4th, 2022 | 5:10PM – 8:00PM | Cryptocurrency – Bitcoin 2 | |
| | October 10, 2022 | | Thanksgiving Day, no scheduled academic activities. | |
| STUDY BREAK | October 11 to 16, 2022 | | Study Break, no scheduled academic activities | |

| | | | | |
|---|---|---|---|---|
| 6 | October 18th, 2022 | 5:10PM – 8:00PM | Cryptocurrency – Development (Python & Flask) | |
| 7 | October 25th, 2022 | 5:10PM – 8:00PM | Ethereum & Smart Contracts | |
| 8 | November 1st, 2022 | 5:10PM – 8:00PM | Alternative Cryptocurrencies | |
| 9 | November 8th, 2022 | 5:10PM – 8:00PM | Building Smart Contracts with Solidity – Part 1 | |
| 10 | November 15th, 2022 | 5:10PM – 8:00PM | Building Smart Contracts with Solidity – Part 2 | |
| 11 | November 22nd, 2022 | 5:10PM – 8:00PM | Building Smart Contracts with Solidity Part-3 / Final Project Presentations | |
| 12 | November 29th, 2022 | 5:10PM – 8:00PM | Final Project Presentations | |
| | December 6, 2022 | | Study break, no scheduled academic activities. | |

## 7. Required Texts/Readings

Below is the recommended book for this course:



Publisher: O'Reilly Media; 1st edition (Jan. 8 2019)

Language: English

Paperback: 424 pages

ISBN-10: 1491971940

ISBN-13: 978-1491971949

*Additional readings may be assigned or recommended during the course.*

## 8. Evaluation Method

Students will be graded according to the following distribution:

| | | |
|---|---|---|
| Assignment 1 | 15% | Details TBA on Canvas |
| Development Assignment 2 | 15% | Details TBA on Canvas |
| Research Assignment 3 | 15% | Details TBA on Canvas |
| Cryptocurrency Video Assignment | 25% | Details TBA on Canvas |
| Final Project Code | 20% | Details TBA on Canvas |
| Final Project Presentation | 10% | Details TBA on Canvas |

**Note:** You must meet the following criteria in order to receive credit for this course:

1. Pass at least one development assignment
2. Pass one of: cryptocurrency video assignment OR final project code

*Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found at:*
https://calendar.ontariotechu.ca/content.php?catoid=55&navoid=2422

## 9. Assignments and Tests

**Important Due Dates**

| | |
|---|---|
| Assignment 1 | October 7th 2022 |
| Development Assignment 2 | October 29th 2022 |
| Research Assignment 3 | November 15th 2022 |
| Cryptocurrency Video Assignment | November 1st 2022 |
| Final Project Code | November 21st 2022 |
| Final Project Presentation | 22nd & 29th November 2022 |

**Note**: All students must demonstrate contribution to their group's video assignment and final project in order to pass this course (unless a deferral has been granted by the faculty or instructor).

**All development assignment details will be released in-class prior to the due date. The cryptocurrency video assignment and final project details will be released on Canvas during the third week of September.**

### Missed Course Work

Coursework missed for medical or serious personal reasons must be documented and reported to the instructor within three (3) working days of the missed work using an Academic Consideration form. Coursework includes, assignments and Project. If missed coursework totals more than 25% of the final grade, this must be documented through the FBIT Academic Advising office, instructor will then contact you for make-up course work. If you miss coursework and do not notify the instructor within the three (3) working day deadline, you will receive a score of zero on the missed component.

## 10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: https://itsc.ontariotechu.ca/remote-learning.php.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotechu.ca

**By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.**

### 11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain e.g. graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.

### 12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

### 13. Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to a Support Worker, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. Support Workers can offer help and resolution options which can include safety plans, accommodations, mental health support, and more. To make an appointment with a Support Worker, call 905.721.3392 or email studentlife@ontariotechu.ca
- Learn more about your options at: https://studentlife.ontariotechu.ca/sexualviolence/

### 14. Students with Disabilities

Accommodating students with disabilities at Ontario Tech is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

**When on campus access is allowed,** students taking courses on north Oshawa campus can visit Student Accessibility Services in Shawenjigewining Hall, third floor, room 320. Students taking courses on the **downtown Oshawa campus** can visit Student Accessibility Services in the 61 Charles St. Building, 2nd Floor, Room DTA 225 in the Student Life Suite.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday to Friday, closed Wednesday’s 8:30am – 10:00am. For more information on services provided, you can visit the SAS website at https://studentlife.ontariotechu.ca/services/accessibility/index.php. Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

**When on campus access is allowed**, students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here https://disabilityservices.ontariotechu.ca/uoitclockwork/custom/misc/home.aspx. Students must sign up for tests, midterms, or quizzes AT LEAST seven (7) days before the date of the test.

Students must register for final exams by the registration deadline, which is typically two (2) weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

## 15. Professional Suitability

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so. (See Appendix A for more information about how students can raise concerns about academic matters.)
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic/academic-conduct-and-professional-suitability-policy.php and the related procedures are hosted at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic-misconduct-and-professional-unsuitability.php

## 16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. This information can be found at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic/academic-integrity-policy.php

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at https://studentlife.ontariotechu.ca/services/academic-support/index.php

## 17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: https://tlc.ontariotechu.ca/educational-technology/assignment-cover-sheet_updatedmay2021-1.pdf

## 18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

## 19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and **when on campus access is allowed,** may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their Student ID card (campus ID) when **in-person examinations are allowed.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at https://registrar.ontariotechu.ca/campus-id/index.php.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit a Request for Accommodation for Religious Obligations to the Faculty concerned as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic/procedures-for-final-examination-administration.php

## 20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

### Notice of Collection and Use of Personal Information

Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO*

*2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Turnitin, cryptocurrency wallets etc

For more information relating to these technologies, we encourage you to visit: https://tlc.ontariotechu.ca/learning-technology/index.php Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

**By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.**

## 21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring a campus environment that is equitable and inclusive. Requirements to refrain from harassment and discrimination apply broadly to the classroom, including in lectures, labs and practicums, as well as through the use of sanctioned and unsanctioned technological tools that facilitate remote learning, e.g. class and other chat functions, video conferencing, electronic mail and texts, and social media content amongst or about University students, faculty and staff.

## 22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used.

Where permitted, students using “chat” functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

### 23. Copyright Notice

All teaching materials provided by the instructor throughout the course, including, but not limited to, in whole or in part, recorded lectures, slides, videos, diagrams, case studies, assignments, quizzes, and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42. Teaching materials are owned by the faculty member, instructor or other third party who creates such works. The copyright owner(s) reserves all intellectual property rights in and to the teaching materials, including the sole right to copy, reproduce, distribute, and modify the teaching materials. Consistent with the university's Intellectual Property Policy, teaching materials are intended only for the educational use of Ontario Tech University students registered in the course that is the subject of this course outline. Any distribution or publishing of this material (e.g. uploading material to a third-party website) is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the Intellectual Property Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

### 24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University’s programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

### University Response to COVID-19

The government response to the COVID-19 pandemic is continually evolving. As new information becomes available from federal and provincial public health authorities, the Province of Ontario and the Regional Municipality of Durham, Ontario Tech University will remain nimble and prepared to respond to government orders, directives, guidelines and changes in legislation to ensure the health and safety of all members of its campus community. In accordance with public health recommendations, the university may need to adjust the delivery of course instruction and the availability and delivery mode of campus services and co-curricular opportunities. Ontario Tech University appreciates the understanding and flexibility of our students, faculty and staff as we continue to navigate the pandemic and work together to demonstrate our strong commitment to academic, research and service excellence during these challenging and unprecedented times.

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University’s Accessibility Policy.

# Appendix A – Dealing with Course Concerns

## Dealing with Course Concerns: Navigating University Processes

### Start with your professor

Suppose you are frustrated with some element of the course organization. Or maybe you disagree with how an assignment was graded. Or perhaps you are struggling to understand a concept. **Your first step is always to talk to your professor.** Set up an appointment. TALK with your professor to ensure clarity in communication.

### Ongoing concerns or struggling with your studies

Our Academic Advisors are amazing. They can offer support and point you to resources to assist you with your studies and with other challenges, including anxiety, stress, and concerns about your courses.

### Unresolved concerns about grades

If your conversation with your professor does not resolve concerns or questions you have about a grade on a test or assignment, **you can appeal the grade**. At the end of the term, file a Request for a Grade Reappraisal. Your request will be assessed by a neutral, independent faculty member.

### Course-related concerns and feedback

The end-of-term course evaluations give you an opportunity to share your feedback about a course. **The course evaluations are taken seriously by the Faculty**, and you should use them to share what worked in the course and what didn't.

### More questions about these processes?

Reach out to your advisor! FBITAdvising@ontariotechu.ca

Faculty of Business and Information Technology

MITS 5620G: Special Topics in IT Management – AI & Security

Course outline for **SPRING/SUMMER 2021**

## 1. Course Details & Important Dates*

| Term | Course Type | Day | Time | Location | CRN # |
|---|---|---|---|---|---|
| Spring/Summer 2021 | Lecture - Online | Tuesdays | 6:10 PM – 9:0-0 PM | SYNC - Online | 10904 |

| Classes Start | Classes End | Last day to drop course without academic consequence | Final Exam Period |
|---|---|---|---|
| Spring/Summer term: May 3, 2021 | August 3, 2021 | May 31, 2021 | August 5 – 8, 2021 |

* For other important dates go to: https://ontariotechu.ca/current-students/academics/important-dates-and-deadlines.php

## 2. Instructor Contact Information

| Instructor Name | Office | Phone | Email |
|---|---|---|---|
| Ruba Al Omari | NA | NA | Ruba.alomari@durhamcollege.ca |
| Office Hours: | | | |

| Laboratory/Teaching Assistant Name | Office | Phone | Email |
|---|---|---|---|
| | | | |
| Office Hours: | | | |

## 3. Course Description

This course introduces the use of artificial intelligence in identifying and predicting cybersecurity threats. Students will learn: the fundamentals of using artificial intelligence in network anomaly detection, malware threat detection, user behavioral analytics for fraud prevention, and detecting email cybersecurity threats; generative adversarial networks and their use in attack and defense scenarios, and the challenges and promises of artificial intelligence in Cybersecurity.

## 4. Learning Outcomes

On the successful completion of the course, students will be able to:

1. Demonstrate and verbalize a deep understanding of the use of artificial intelligence in predicting security threats
2. Learn how to predict network intrusions and detect anomalies with machine learning algorithms
3. Learn how to detect email threats such as phishing using machine learning algorithms
4. Learn how to detect zero-day and polymorphic malware samples
5. Evaluate the effectiveness of various alternative solutions, using appropriate analysis metrics

## 5. Course Design

***The course is delivered through online class sessions and students must have stable internet connection for the online lectures. Note that this will require access to a specific set of technology tools; access to a laptop/tablet/PC with a built-in or external microphone and camera or web cam.***

This course focuses on the use of artificial intelligence (AI) in cybersecurity. It explores the use of machine learning algorithms in detecting threats, network anomaly, spam, malware, and user behavioral analytics for fraud prevention.

The primary teaching method will be class lectures and out of class assignments. The lectures will discuss the course topics listed below, while out of class assignments acquaint students with practical skills and techniques relevant to the disciplines which are discussed in the lectures.

All lecture notes, including student presentations, will be recorded and uploaded to Canvas.

Class attendance is highly recommended, and students must complete all in-class coding exercises in order to understand the concepts and ideas introduced in the class.

## 6. Outline of Topics in the Course

| Lecture # | Date | Time | Topics | Details of topics to be covered in the course, by unit or by week |
|---|---|---|---|---|
| 1 | May 4 | 6:10 pm – 9:00 pm | Introduction to the use of AI and Machine Learning in Cybersecurity | Course Plan |
| 2 | May 11 | 6:10 pm – 9:00 pm | Ham or Spam? Detecting Email Cybersecurity Threats with AI | Assignment#1 |
| 3 | May 18 | 6:10 pm – 9:00 pm | Anomaly Detection and Network Traffic Analysis | |
| 4 | May 25 | 6:10 pm – 9:00 pm | Malware Analysis and Threat Detection | Assignment#2 |
| 5 | June 1 | 6:10 pm – 9:00 pm | Individual Paper Presentations - I | |
| 6 | June 8 | 6:10 pm – 9:00 pm | Individual Paper Presentations - II | |

| | | | | |
|---|---|---|---|---|
| STUDY BREAK | June 15 – 19, 2021 | | Study Break, no scheduled academic activities | |
| 7 | June 22 | 6:10 pm – 9:00 pm | Securing User Authentication | Assignment#3 |
| 8 | June 29 | 6:10 pm – 9:00 pm | Fraud Prevention with AI Solutions | |
| 9 | July 6 | 6:10 pm – 9:00 pm | Protecting the Consumer Web | |
| 10 | July 13 | 6:10 pm – 9:00 pm | Adversarial Machine Learning | |
| 11 | July 20 | 6:10 pm – 9:00 pm | Final Project Presentations + Group Project Discussion | |
| 12 | July 27 | 6:10 pm – 9:00 pm | Final Project Presentations + Group Project Discussion | |
| | August 4, 2021 | | Study break, no scheduled academic activities. | |

## 7. Required Texts/Readings

There is no assigned textbook. All assigned readings and cases will be introduced in the class. A list of recommended readings and references will be provided for each lecture.

*Additional readings may be assigned or recommended during the course.*

## 8. Evaluation Method

This course takes a project-based approach to provide experiential learning through its development. Project information will be made available on Canvas after the course starts.

Students will be and evaluated as follows:

| Item | Weight (%) |
|---|---|
| Assignments (3 x 15% each) | 45 |
| Individual Paper Presentation | 15 |
| Group Project Plan | 5 |
| Group Project Report | 25 |
| Group Project Presentation | 10 |

*Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found at:* [http://calendar.uoit.ca/content.php?catoid=22&navoid=879#Grading](http://calendar.uoit.ca/content.php?catoid=22&navoid=879#Grading)

## 9. Assignments and Tests

| Item | Release Week/Time* | Due Week/Time* | Weight (%) |
|---|---|---|---|
| Assignments (3 x 15% each) | Tuesdays during class time on Weeks 2,4,and 7 | Sundays @ 11:59 PM (second Sunday after release) | 45 |
| Group Project Plan | Week 1 (In-Class) | Week 4 | 5 |
| Individual Paper Presentation + Group Project Discussion | Week 1 (In-Class) | Weeks 5 and 6 (In-Class) | 15 |
| Group Project Report | Week 1 (In-Class) | Week 10 | 25 |
| Group Project Presentation | Week 1 (In-Class) | Weeks 11 and 12 (In-Class) | 10 |

*Check Canvas for the exact date and time.

Any issues related to the assignments should be brought to the professor’s attention within 5 days of the mark release. No review of assignment’s marking will be done after that.

All other term issues must be brought to the professor’s attention and be resolved by the last lecture (July 28th). Instructions for the assignments and final project will be available on Canvas. We will be using electronic submission for the labs and final project via Canvas. No other means of submission (e.g., hard copy, email, fax, etc.) will be accepted. Project plan and final project presentations will be presented by students during our class time.

### Missed Course Work

Coursework missed for medical or serious personal reasons must be documented and reported to the instructor within three (3) working days of the missed work using an Academic Consideration form. Coursework includes, but is not limited to, quizzes; written assignments; participation; case studies; etc… If missed coursework totals more than 25% of the final grade, this must be documented through the FBIT Academic Advising office. The weight of the missed course component will be reweighted to the next equivalent component (e.g., Assignment#1 mark is carried over to Assignment#2 mark). If you miss coursework and do not notify the instructor within the three (3) working day deadline, you will receive a score of zero on the missed component.

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

## 10. Technology Requirements

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: https://itsc.ontariotechu.ca/remote-learning.php.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotechu.ca

**By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.**

### 11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain examples that are applicable to the course subject matter – [e.g. graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality]. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.

### 12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

### 13. Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all is forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to a Support Worker, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. Support Workers can offer help and resolution options which can include safety plans, accommodations, mental health support, and more. To make an appointment with a Support Worker, call 905.721.3392 or email studentlife@ontariotechu.ca
- Learn more about your options at: https://studentlife.ontariotechu.ca/sexualviolence/

### 14. Students with Disabilities

Accommodating students with disabilities at Ontario Tech is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

**When on campus access is allowed,** students taking courses on north Oshawa campus can visit Student Accessibility Services in the Student Life Building, U5, East HUB (located in the Founders North parking lot). Students taking courses on the **downtown Oshawa campus** can visit Student Accessibility Services in the 61 Charles St. Building, 2nd Floor, Room DTA 225 in the Student Life Suite.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday to Friday, closed Wednesday's 8:30am – 10:00am. For more information on services provided, you can visit the SAS website at https://studentlife.ontariotechu.ca/services/accessibility/index.php. Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

**When on campus access is allowed**, students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here https://disabilityservices.ontariotechu.ca/uoitclockwork/custom/misc/home.aspx. Students must sign up for tests, midterms, or quizzes AT LEAST seven (7) days before the date of the test.

Students must register for final exams by the registration deadline, which is typically two (2) weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

## 15. Professional Conduct (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

Additional information on professional suitability can be found at http://calendar.uoit.ca/content.php?catoid=22&navoid=879#Academic_conduct

## 16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. This information can be found at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic/academic-conduct-and-professional-suitability-policy-undergraduate.php

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at https://studentlife.ontariotechu.ca/services/academic-support/index.php

## 17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: https://shared.uoit.ca/shared/department/academic-integrity/Forms/assignment-cover-sheet.pdf

## 18. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and **when on campus access is allowed,** may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their Student ID card (campus ID) when **in-person examinations are allowed.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at https://registrar.ontariotechu.ca/campus-id/index.php.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit a Request for Accommodation for Religious Obligations to the Faculty concerned as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic/procedures-for-final-examination-administration.php

## 19. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act (“FIPPA”). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA’s definition of “personal information” includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of [Insert Faculty name] encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

### Notice of Collection and Use of Personal Information

Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO*

*2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course may use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below; according to the instructor:

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, others indicated by the instructor.

For more information relating to these technologies, we encourage you to visit: https://tlc.ontariotechu.ca/learning-technology/index.php Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

**By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.**

### 20. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

### 21. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

### University Response to COVID-19

The government response to the COVID-19 pandemic is continually evolving.  As new information becomes available from federal and provincial public health authorities, the Province of Ontario and the Regional Municipality of Durham, Ontario Tech University will remain nimble and prepared to respond to government orders, directives, guidelines and changes in legislation to ensure the health and safety of all members of its campus community.  In accordance with public health recommendations, the university may need to adjust the delivery of course instruction and the availability and delivery mode of campus services and co-curricular opportunities.  Ontario Tech University appreciates the understanding and flexibility of our students, faculty and staff as we continue to navigate the pandemic and work together to demonstrate our strong commitment to academic, research and service excellence during these challenging and unprecedented times.

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

UNIVERSITY OF ONTARIO
INSTITUTE OF TECHNOLOGY

**Faculty of Science**

# CSCI 5010G – Survey of Computer Science Research Topics & Methods

Course outline for Fall 2016

## 1. Course Details & Important Dates*

| Course Type | Day | Time | Location |
|---|---|---|---|
| Lecture | Tues. | 2:10pm – 5:00pm | ERC1094 |

* for other important dates go to: www.uoit.ca >Current Students >Important Dates and Deadlines

## 2. Instructor Contact Information

| Instructor Name | Office | Email |
|---|---|---|
| Dr. Jeremy S. Bradbury | UA4016 | jeremy.bradbury@uoit.ca |
| Office Hours: Fri. 11:00am-12:00pm, or by appointment. | | |

## 3. Course Description

**CSCI 5010G – Survey of Computer Science Research Topics and Methods.** This course is a survey of some of the main research topics in computer science and the corresponding computer science research methods. Topics covered vary from year to year and may include digital media, computer graphics, human-computer interaction, computer networks, security, health informatics, databases and software design. Research methods covered include library methods, topic analysis, data management, technical writing, presentations, evaluation methods and peer review. This course includes guest lectures by experts in the research topics covered. Credit hours: 3

## 5. Course Design

Survey of Computer Science is a required course for all Computer Science MSc and PhD students. The course is designed as a comprehensive survey of Computer Science research areas and research methods that provides a strong research foundation for any student pursing graduate studies in Computer Science. The research areas/topics surveyed will be presented by weekly guest lectures from graduate faculty in the Computer Science program. In addition to surveying Computer Science topics the course will also survey Computer Science research methods. Each week half of the lecture will be devoted to introducing a new research method. Students will be evaluated by applying the covered research methods to their own area of interest within Computer Science.

## 6. Outline of Topics in the Course

- State-of-the-art research examples from the Computer Science graduate program fields:
    - Digital Media
    - Information Systems
    - Networks and IT Security
    - Software Design
- Research Methods to address the following questions:
    - How do I learn about my chosen field of research?
        - Finding research papers and creating an annotated bibliography
        - Conducting literature reviews, classifications and taxonomies
    - How do I select a research topic?
        - Conducting a topic analysis
        - Technical writing
    - How do I write a thesis proposal?
        - The structure of a thesis proposal
        - Defining a research hypothesis
        - Proposing a methodology and understanding the possible outcomes
    - Is there a right way to manage my research?
        - Research logs
        - Research meetings – agendas, notes
        - Backing up data! – The benefit of version control systems
    - How do I evaluate my research work?
        - Evaluation methods for computer science research tools and techniques
        - Evaluation methods for computer science research involving human subjects
        - The importance of reproducibility, threats to validity
        - Conducting ethical research
    - How do I write up and defend my thesis?
        - The structure of a thesis proposal
        - Advice on obtaining feedback from your supervisor and committee
    - How do I publish and disseminate my research?
        - Different kinds of research publication venues – workshops, conferences, journals, books
        - Publication quantity vs. quality – understanding publication metrics, citation counts, etc.
        - The peer review process and how to review a paper
        - Oral communication and research presentations

## 7. Required Texts/Readings

*Textbooks.*

**Writing the Doctoral Dissertation: A Systematic Approach, 3/E**
by Gordon B. Davis & Clyde A. Parker

**Writing for Computer Science, 3/E**
by Justin Zobel

*Online Resources.*

Online articles and websites will be used to supplement the textbook. Links to all online resources will be posted on the course website.

## 8. Evaluation Method

| | |
|---|---|
| Annotated Bibliography | 15% |
| Paper | 25% |
| Peer Review | 15% |
| Presentations | 25% |
| Attendance & Participation | 20% |

*All students are required to attend 80% of the lectures and 80% of the Computer Science seminars in order to pass the course.*

## 9. Assignments and Tests

The schedule for course deliverables is as follows:

- Presentation 1 –Oct. 11, 2016
- Annotated Bibliography – mid Oct. 2016
- Paper (preliminary submission) – mid. Nov. 2016
- Peer Review – late Nov. 2016
- Paper (final submission) – early Dec. 2016
- Presentation 2 – Nov. 29, 2016

## 10. Students with Disabilities

Accommodating students with disabilities at UOIT is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

Students taking courses on the North Campus Location can visit Student Accessibility Services in the U5 Building located in the Student Life Suite
Students taking courses on the Downtown Oshawa Campus Location can visit Student Accessibility Services in the 61 Charles St. Building, 2nd Floor, Room DTA 225 in the Student Life Suite.

Disability-related support and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Mon-Fri. For more information on services provided, you can visit the SAS website at http://uoit.ca/studentaccessibility

Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@uoit.ca

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here www.uoit.ca/SASexams. Students must sign up for tests, midterms or quizzes AT LEAST seven (7) days before the date of the test.
Students must register for final exams by the registration deadline, which is typically 2 weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

## 12. Academic Integrity

Students and faculty at UOIT share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by UOIT's regulations on Academic Conduct (Section 5.15 of the Academic Calendar) which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with UOIT's regulations on academic conduct does not constitute a defense against its application.

Further information about academic misconduct can be found in the Academic Integrity link on your laptop. Extra support services are available to all UOIT students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found in the Academic Calendar (Section 8).

## 15. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes and other evaluative material in your courses in the Faculty of Science.

As you may know, UOIT is governed by the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that UOIT not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Science encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that UOIT will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@uoit.ca

## 16. Course Evaluations

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of UOIT's programs and instructional effectiveness.  To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes.  Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Blackboard, Weekly News and signage around the campus.

# Appendix _ – Faculty Information

*Please include here only those currently at the institution and affiliated with the program. Examples in purple to be removed.* ***Where available, link each faculty name to their Research or Profile page on the website.***

## Faculty members by home unit, rank, and supervisory privileges

| Name and Faculty Status/Rank (Tenure/tenure-track, teaching-focused, continuing sessional, special appointment, emeritus, etc.) | Terminal Degree | Home Faculty/Unit | Areas of Expertise | Supervisory Privileges and Role in New Program (Note if faculty will be teaching and/or supervising in the program; indicate primary supervisor by asterisks) | Total Graduate Teaching (including New Program) (Note in bold type if faculty is a course developer for the program) |
|---|---|---|---|---|---|
| Patrick Hung, Professor | Ph.D. | FBIT | Privacy and Security | Teaching and Supervising | One course |
| Miguel Vargas Martin, Professor | Ph.D. | FBIT | Cryptography and Network Security | Teaching and Supervising | One course |
| Khalil El-Khatib, Professor | Ph.D. | FBIT | Privacy and Security | Teaching and Supervising | Two courses,<br>Course developer |
| Salma Karray, Professor | Ph.D. | FBIT | Operational Research, Game Theory | Supervising | |
| Stephen Marsh, Professor | Ph.D. | FBIT | Information Trust and Privacy | Teaching and Supervising | Two courses<br>Course developer |
| Julie Thorpe, Professor | Ph.D. | FBIT | Privacy and Security | Teaching and Supervising | One course<br>Course developer |
| Andrea Slane, Professor | Ph.D., J.D. | FSSH | Legal and policy; privacy; intellectual Property | Teaching and Supervising | One course<br>Course developer |
| Isabel Pedersen, Professor | Ph.D. | FSSH | Digital Life and Digital Media | Teaching and Supervising | One course<br>Course developer |
| Shahram S. Heydari, Associate Professor | Ph.D. | FBIT | Communication networks and security | Teaching and Supervising | One course<br>Course developer |

| | | | | | |
|---|---|---|---|---|---|
| Richard Pazzi, Associate Professor | Ph.D. | FBIT | Multimedia communication, Cloud networks | Supervising | |
| Amirali S. Abari, Associate Professor | Ph.D. | FBIT | Artificial Intelligence; IT Forensics | Teaching and Supervising | One course |
| Peter Lewis, Associate Professor | Ph.D. | FBIT | Trustworthy Artificial Intelligence | Teaching and Supervising | One course |
| Rajen Akalu, Associate Professor | Ph.D. | FBIT | Privacy and Artificial Intelligence; Information Privacy Law | Teaching and Supervising | One course |
| Fletcher Lu, Associate Professor | Ph.D. | FBIT | Cybercrime and online Fraud | Teaching and Supervising | One course |
| Hui Zhu, Associate Professor | Ph.D. | FBIT | Securities; Corporate Social responsibility; International Finance | Teaching and Supervising | One course,<br>Course developer |
| Pooria Madani, Assistant Professor | Ph.D. | FBIT | Adversarial Machine Learning; Cybersecurity | Teaching and Supervising | One course<br>Course developer |
| Li Yang, Assistant Professor | Ph.D. | FBIT | AI and data analytics; Cybersecurity | Teaching and Supervising | One course |

## Graduate Thesis supervisory records/experience by faculty member

| Name | Completed (last 5 years) | | | Current | | |
|---|---|---|---|---|---|---|
| | Master’s | Ph.D. | PDF | Master’s | Ph.D. | PDF |
| Miguel Vargas Martin | 6 | 2 | | 1 | 4 | |
| Khalil El-Khatib | 7 | 3 | | | 3 | |
| Salma Karray | | 2 | | 1 | 2 | |
| Stephen Marsh | 1 | 2 | | 2 | | |
| Julie Thorpe | 6 | 2 | | 1 | 2 | |
| Andrea Slane | 5 | | | | 1 | |
| Isabel Pedersen | 1 | 1 | | | | |
| Shahram S. Heydari | 3 | 1 | 1 | 1 | 2 | |
| Richard Pazzi | 5 | 2 | | | | |
| Amirali S. Abari | 7 | 1 | | 3 | | |
| Peter Lewis | | 4 | 10 | 3 | 1 | 2 |
| Pooria Madani | | | | 1 | | |

### Publication records at Ontario Tech by year and outlet (current and last 5 years)

| Year | Faculty Members | Articles | Books | Book Chapters | Reports | Conference Presentations |
|---|---|---|---|---|---|---|
| 2023 | 17 | 20 | 1 | | | 28 |
| 2022 | 16 | 22 | 1 | 1 | 1 | 20 |
| 2021 | 15 | 34 | 1 | 2 | 4 | 25 |
| 2020 | 14 | 13 | 1 | 4 | 4 | 15 |
| 2019 | 14 | 23 | | 1 | 2 | 28 |
| 2018 | 14 | 17 | 1 | | | 28 |

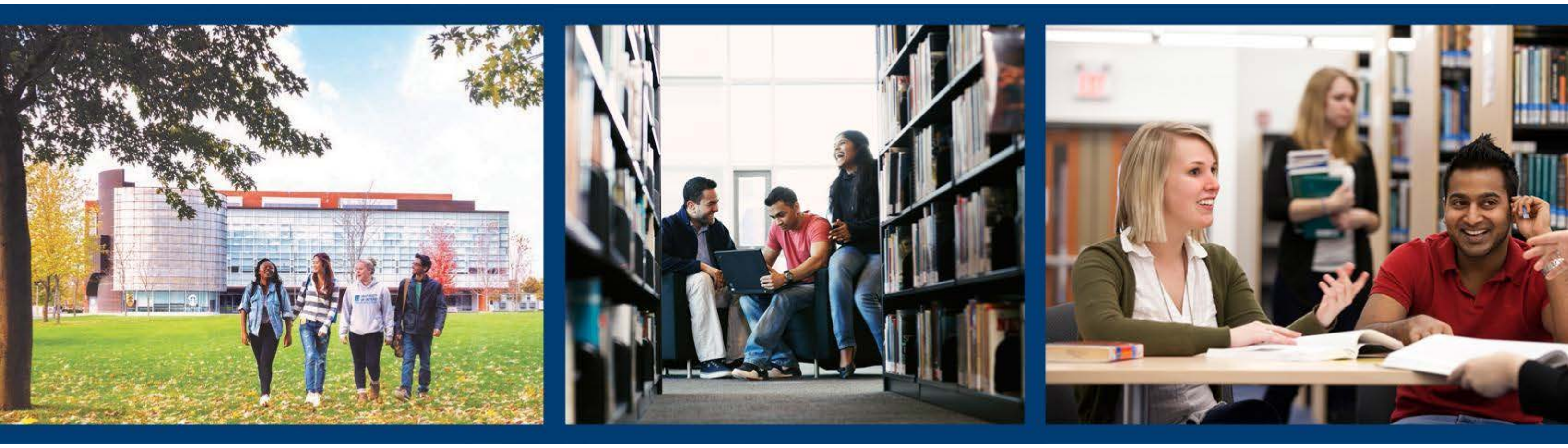
### Research funding at Ontario Tech by source and year

| Year | Faculty Members | Canadian Granting Councils | Canadian Government | International Government | Others |
|---|---|---|---|---|---|
| 2023 | 17 | $567000 | | | $31000 |
| 2022 | 16 | $611000 | $95000 | | $24000 |
| 2021 | 15 | $765000 | $16000 | | $24000 |
| 2020 | 14 | $483000 | $16000 | | |
| 2019 | 14 | $406000 | $5500 | | $80000 |
| 2018 | 14 | $330000 | | | $110000 |

Appendix F

# Library Statement of Support for Proposed Doctor of Philosophy in Cybersecurity

Prepared by: Catie Sahadath, Associate University Librarian, Scholarly Resources, April 2024



OntarioTech
Library

# Contents

# Summary

Ontario Tech University Library's holdings in Business and Information Technology are strong.

The PhD in Cybersecurity program is a socio-technical, multidisciplinary research-intensive program that covers a broad range of themes related to cybersecurity; including technology, policy and governance, AI and human behaviour.

The Library's research holdings, as well as archives and special collections total more than 98, 000 print volumes and 167,892 journal subscriptions. In addition, our holdings include more than 1.3 million e-books, and primary source materials. Collection strengths support the research and instructional programs at Ontario Tech University.

Opportunities exist to incorporate information literacy directly into the PhD, Cybersecurity program. Student feedback from information literacy sessions overwhelmingly shows that students find the skills to be useful and that information literacy instruction should ideally be incorporated into foundational and methods courses. The following courses have been identified as ideal candidates for incorporating elements of library-delivered information, digital and data literacy instruction:

- INFR5010G: Fundamentals of IT Security
- CSCI 5010G: Survey of Computer Science Research Topics and Methods

## Resource Requirements

Include a summary of any resource requirements to support the program, indicating one time startup or ongoing funding requests:

| Resource | Rationale | Budget Requirement | OTO or Ongoing |
|---|---|---|---|
| Data Breach Chronology Database | This resource was identified by a faculty member as an important resource for the newly proposed course "Financial Implications of Cyber Risk." | $1 000 | Ongoing |
| **Total** | | $1000 | |

# Introduction

The Library supports the teaching, learning and research missions of Ontario Tech University and Durham College. Ontario Tech students have access to a joint collection of more than 98, 000 print books. Additionally, our collections include extensive online resources such as e-books and online databases that are selected to meet curricular needs. Students and faculty are supported by a team of subject specialist librarians and trained library technicians who provide an array of research and teaching support services including information literacy instruction, workshops, research help and reference service.

# Library Collections

The Library's collections support the PhD, Cybersecurity program. The existing collections that support similar and related programs, such as the BA, Information Technology, the MA and PhD in Computer Science, and the MA in IT Security, create a strong foundation of resources pertinent to the PhD, Cybersecurity program.

The Library's collections budget for 2023-24 was just under $2 M . Approximately 95% of this budget is directed to online resources, while the remainder is allocated to acquisition of other formats, including journals, print books, multimedia and other specialized material.

With respect to programs in the Faculty of Business and Information Technology, including the PhD, Cybersecurity program, our existing collection spans technology, policy, information, governance, IT security, AI, and human behaviour. Further, the collection covers topics of interdisciplinary relevance such as criminology and justice studies, social sciences, and business.

Suggestions for new resources are welcome and faculty and students are encouraged to contact their subject specialist. All recommended purchases are evaluated according to the Collection Development Policy and with consideration to budget constraints.

## Consortial Licensing

Thanks to our participation in two consortia – the Ontario Council of University Libraries (OCUL) and the Canada Research Knowledge Network (CRKN) – Ontario Tech benefits from optimal pricing through licensing content as a collective, providing access to research published both open access and commercially through publishers such as Elsevier, Wiley, ACS, Taylor and Francis etc.

## Journals

Our journal holdings in disciplines related to Cybersecurity is strong, including coverage related to engineering, computer science, criminology, critical policy studies, and artificial intelligence.

We provide access, through subscription, to most of the relevant journals with the highest impact factors, according to Clarivate's Journal Citation Reports (JCR) database and Google Scholar metrics.

By subject category:

| JCR Subject Category | Ontario Tech Access | Select Titles |
|---|---|---|
| Computer Science, Interdisciplinary Applications | 10/10 | ● Journal of Cybersecurity<br>● Cybersecurity<br>● Computers & Education |
| Criminology and Penology | 10/10 | ● Annual Review of Criminology<br>● Criminology & Public Policy |
| Political Science | 10/10 | ● Policy Review<br>● Social Science Quarterly |
| Law | 10/10 | ● Internet Policy Review |

## Books & E-Books

As noted, we provide access to over 98,000 print books and over 1.3 million e-books that support teaching, learning and research across all programs and disciplines. Students and faculty have access to collections of books and e-books from major academic publishers.

Through our Omni Search, students and faculty have seamless access to holdings not just from Ontario Tech, but all Omni member libraries across Ontario universities. Articles and books that are not available through Omni Libraries can be requested through our interlibrary loan service.

The following table highlights Library holdings by subject heading for print books and e-books that encompass the Library's collections in Cybersecurity

| Subject | # Print Books | # E-Books |
|---|---|---|
| Cybersecurity | 186 | 3,332 |
| Forensic Computing | 74 | 5 |
| Information Policy | 32 | 5,293 |
| Criminology | 270 | 3,591 |

## Search Tools

The Library subscribes to many research databases and indexes that provide access to the literature in Cybersecurity. Systematic searching of these resources enables students and faculty to access journals and other academic resources such as conference proceedings, theses and dissertations, trade publications and reports.

| Highly Relevant Databases: Computer Science | Relevant Databases: Multidisciplinary | Relevant Databases: Related Disciplines |
|---|---|---|
| ● IEEE Xplore Digital Library<br>● ACM Digital Library<br>● Computers and Applied Science Complete<br>● McGraw Hill Access Engineering | ● Web of Science<br>● Scopus<br>● SpringerLINK Journals<br>● CBCA: Science and Technology | Forensic Science<br>● FORENSICnetBASE<br><br>Criminology and Law<br>● Martin’s Online Criminal Code<br>● National Criminal Justice Reference Service<br>● Proquest Criminal Justice |

## Standards and Codes

The Library provides access to Standards and Codes in print and online from the following sources:

- Canadian Standards Association (CSA)
- International Standards Organization (ISO)
- ASME
- ASTM
- IEEE
- Techstreet

Standards relating to Cybersecurity are available to faculty and students, as provisioned in the Library’s Collection Development policy, for use in teaching, learning, and research. Faculty and students are encouraged to contact their subject specialist Librarian with suggestions for purchase.

## Data Resources

To support research that requires statistics and datasets, the Library subscribes to three main resources:

- **Data Liberation Initiative (DLI):** Access to datasets from Statistics Canada surveys including public use microdata files (PUMF).
- **odesi**: A web-based data exploration, extraction and analysis tool that enables researchers to search for variables across thousands of datasets including Statistics Canada datasets and polling data.
- **Interuniversity Consortium for Political and Social Research (ICPSR):** Access to a data archive of more than 250,000 files of research in the social and behavioral sciences. Includes specialized collections of data in education, aging, criminal justice, substance abuse, terrorism, and other fields. Resources for teaching and learning include classroom exercises and materials to support

data literacy in the classroom.

In addition, we provide access to Borealis: The Canadian Dataverse Repository, which supports research data management and open access data requirements for Tri-Agency research funding compliance.

### Multimedia Resources

The Library acquires DVD and streaming video resources that are relevant to the disciplines in the Cybersecurity  program. Multimedia resources are selected individually or as part of standing subscriptions.

Omni retrieves over 350 results for videos available through the Library's streaming video subscriptions on the topic of cybersecurity.

## Library Services

A range of library services support teaching, learning and research at the University. Students and faculty in the PhD, Cybersecurity program have access to services in-person, online and via email or telephone.

### Research Support

The Library plays a vital role in supporting student and faculty research at Ontario Tech.

### Reference Service & Research Consultations

Students and faculty have access to research support in-person and online, via telephone, email and through online chat help.

Librarians provide individualized research consultations with students and faculty, in person or online. These consultations are tailored to meet the needs of individual researchers and can cover a range of topics from basic introductions to more advanced search techniques and support for literature reviews.

### Open Access & Research Data Management

We provide support to faculty and students in complying with the Tri-Agency Open Access Policy (SSHRC, NSERC, CIHR). Faculty and students can make their work open by publishing in an open access or hybrid journal, by depositing their work in a subject repository, or by depositing their work in Ontario Tech's institutional repository, eScholar (https://ir.library.ontariotechu.ca).

We also provide direct support to Faculties through dedicated subject specialist/liaison librarians and online guidance with the Library's Open Access Guide (http://guides.library.ontariotechu.ca/openaccess). The Library has a Research Data Management guide (http://guides.library.ontariotechu.ca/rdm) to support faculty and students in creating data management plans and sharing research data.

### Research Metrics & Impact

The Library supports various departments on campus by fielding requests for reports on author, article, journal and institutional metrics. Subscribed tools include: Web of Science, Scopus and Journal Citation Reports (JCR).

Our Research Metrics guide (http://guides.library.ontariotechu.ca/researchmetrics) provides background information and support for these tools.

### Theses & Dissertations

To ensure that the Ontario Tech community has access to national and international thesis and dissertation databases, we provide access to PQDT (ProQuest Dissertations and Theses) and the Theses Canada Portal. The Library plays a key role in the dissemination and preservation of Ontario Tech theses, managing copies in the institutional open-access digital repository, E-Scholar, as well as maintaining print copies in the Library archives.

## Teaching & Learning Support

As partners in teaching and learning at Ontario Tech, we provide a range of instructional and curriculum supports, both in person and online.

### Information Literacy Instruction

In collaboration with teaching faculty, Librarians deliver customized information literacy instruction that support the development of students' 21st century skills to successfully search, evaluate and ethically use scholarly resources in their course requirements. These library services are aligned with the Association of College and Research Libraries (ACRL) Framework for Information Literacy for Higher Education. Information literacy sessions are tailored to the specific requirements of the course or assignment. Information literacy may be delivered synchronously or asynchronously to classes, in person or online. Library information literacy modules are available in the Canvas Learning Management System and can be adapted and added direct into courses, or instructors can opt for asynchronous recordings.

Students may also receive Information Literacy instruction from a Librarian in their elective or communications courses.

Ideally, Information Literacy instruction is scaffolded across the required curriculum, enabling students to build increasingly sophisticated research skills throughout their program of study. Student feedback from information literacy sessions indicates that 78% of students felt more confident using the library after receiving library instruction, 84% if students felt that they learned something new, and that students often wish they would have received this training earlier in their program. Some comments include:

- "Definitely could have used this tutorial in prior classes for research"
- "I wish I had known about this stuff in first year"
- "I wish I had learned about this 3 years ago"
- "I wish this was mandatory for all first year students"
- "I think this course would be great for all first year students"

The following courses have been identified as potential Information Literacy touchpoints, due to the research skills outcomes built into the curriculum:

- INFR5010G: Fundamentals of IT Security
- CSCI 5010G: Survey of Computer Science Research Topics and Methods

### *Co-curricular Workshops*

In addition to Information Literacy instruction that is integrated into the curriculum, the library offers a number of co-curricular workshops that help develop student and faculty skills. Some examples of workshops offered to Ontario Tech students in the past include:

- 3D Printing
- Managing Your Research Identity
- Citation Management
- Finding and Using Open Educational Resources
- Research Data management and Data Management Plans

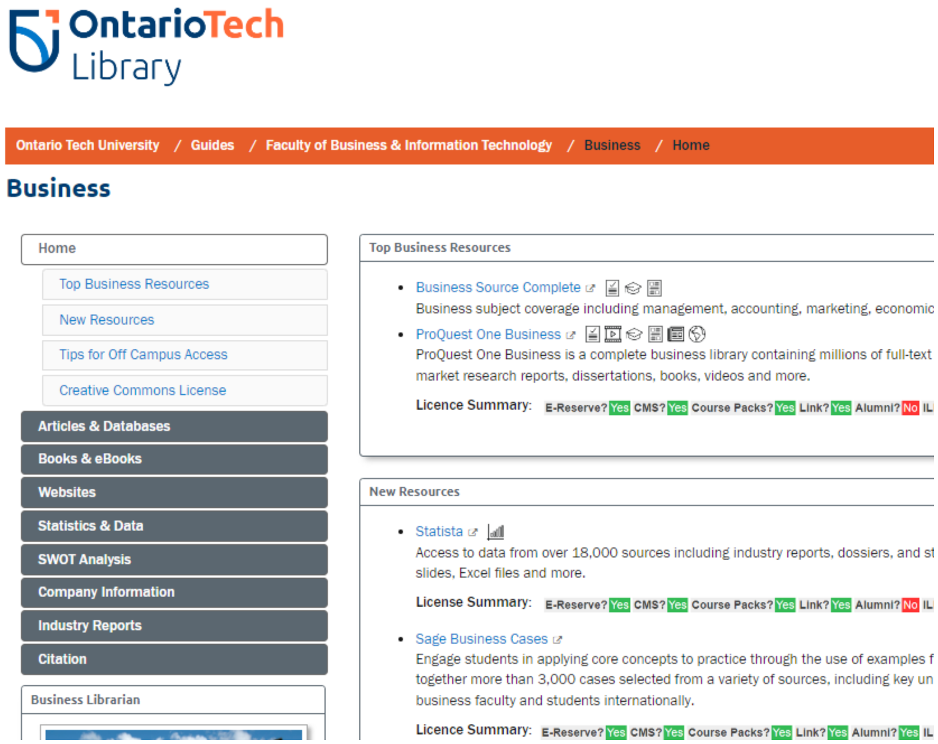
Workshop offerings are regularly updated in response to the changing needs of the community.

We also are regular contributors to the University's Grad Pro Skills offerings.

## Online Research Guides

Subject specialist librarians create custom Research Guides for each subject area that are available from the Library website. Research Guides include program and course guides that are directly related to the program and course curriculum, as well as topic guides that have cross-disciplinary relevance. Research Guides of particular importance to students in the PhD, Cybersecurity program include:

- Business: https://guides.library.ontariotechu.ca/business
- Network & IT Security: https://guides.library.ontariotechu.ca/networkingITsecurity
- Citation Guide: https://guides.library.ontariotechu.ca/citation



Top Business Resources

- Business Source Complete
  Business subject coverage including management, accounting, marketing, economic
- ProQuest One Business
  ProQuest One Business is a complete business library containing millions of full-text market research reports, dissertations, books, videos and more.

  Licence Summary: E-Reserve? Yes CMS? Yes Course Packs? Yes Link? Yes Alumni? No IL

New Resources

- Statista
  Access to data from over 18,000 sources including industry reports, dossiers, and st slides, Excel files and more.

  License Summary: E-Reserve? Yes CMS? Yes Course Packs? Yes Link? Yes Alumni? No IL
- Sage Business Cases
  Engage students in applying core concepts to practice through the use of examples f together more than 3,000 cases selected from a variety of sources, including key un business faculty and students internationally.

  Licence Summary: E-Reserve? Yes CMS? Yes Course Packs? Yes Link? Yes Alumni? Yes IL

## Copyright & Academic Integrity

The Library provides copyright guidance for faculty and students. Library staff advise on license terms and the integration of content into the Learning Management System (LMS). We also help faculty find, evaluate and integrate Open Educational Resources into their courses.

Our research support services including our citation guides help students avoid plagiarism and comply with the University's Academic Conduct policy.

## Course Reserves

Instructors can place materials on course reserve in the library, or make course materials available online through our electronic course reserves system. Online course reserves can include the library's print holdings, as well as digitized chapters, and links to journals, e-book chapters, videos and more. We are dedicated to providing equitable access to resources, and our online reserves are subject to copyright compliance and licensing restrictions.

## 3D Printing & Equipment Loans

Students have access to 3D printers and 3D printing workshops and can borrow equipment such as laptops and device chargers.

## Library Staffing

The anticipated enrollment for students in the PhD, Cybersecurity program for years 1-5 is as follows:

| | |
|---|---|
| 2024-2025: | 4 |
| 2025-2026: | 9 |
| 2026-2027: | 14 |
| 2027-2028: | 19 |
| 2028-2029: | 20 |

We anticipate that there will be additional staffing requirements associated with growth in graduate and undergraduate degree programs across the University. These requests will be part of the regular budget planning process, following a fulsome and strategic analysis of our staffing needs.

# Conclusion

## Supports for Graduate Students

Graduate students are encouraged to take advantage of all of  the Library supports that are available to them.  Their subject specialist librarian can help them identify the best databases for their research questions, as well as to define effective search strategies to make the best use of their time in locating articles, books, datasets etc.  We can also assist in understanding the current publishing landscape, open access, open educational resources as well as managing research profiles,  depositing research into eScholar, our institutional repository and determining research impact.

To conclude, the Library is very well-positioned to support the Faculty of Business and IT's proposed PhD in Cybersecurity and we look forward to a positive outcome and future launch of the program.

REVIEWERS' REPORT FOR NEW PROGRAMS

# Reviewers' Report on the Proposed PhD-Cybersecurity Program at Ontario Tech University

Ali Dehghantanha
School of Computer Science
University of Guelph
ON, Canada

Isaac Woungang
Department of Computer Science
Toronto Metropolitan University
ON, Canada

## 1. OUTLINE OF THE REVIEW

Please indicate whether this review was conducted by desk audit or site visit. For those reviews that included a site visit, please indicate the following:

- Who was interviewed
- What facilities were seen
- Any other activities relevant to the appraisal

The program review was initially intended to be hosted in-person, but due to unforeseen circumstance, it was rescheduled to happen virtually in the form of desk audit and adjusted to avoid any substantial delay.

This report is based on the findings from the desk audit and an intensive review of the following documents that were made accessible to the review team (Professor Dehghantanha and Professor Woungang) via a Google drive folder:

- New Program Proposal
- Template for External Reviewers' Report
- Ontario Tech University's Institutional Quality Assurance Process Policy (IQAP)
- Information about Ontario Tech University
- Faculty and full curriculum information
- Strategic Research Plan
- Integrated Academic-Research Plan Summary
- Graduate Viewbook

During the desk audit online, we met with the following people:

- Deputy Provost
- Associate Dean, Graduate and Postdoctoral Studies
- Dean, Faculty of Business and IT
- Associate Dean, Academic Strategy
- Chair of Internal Assessment Team
- Graduate Program Assistant
- Director of Ontario Tech's Institute for Cyber Security and Resilient Systems
- Program and Curriculum Analyst-Centre for Institutional Quality Enhancement
- Manager, Graduate and Postdoctoral Studies
- Graduate Academic Affairs Specialist
- Graduate Admissions and Registration Coordinator
- Graduate Program Assistant
- Faculty Program Assistant
- Executive Assistant
- Faculty members & Staff
- A sampling of students
- Representatives from Student Life & School of Graduate and Postdoctoral Studies (SGPS)
- Faculty of Business and Information Technology Networking and IT Security Laboratory Managers

We also had Labs Virtual Tour, https://ontariotechu.ca/virtualtour/ of the following:

- *Networking lab (for teaching)* - which has leading-edge equipment (such as routers, switches, IP phones, wireless access points, and more, including remotely accessible ones) to teach concepts from fundamental networking skills to enterprise-level network engineering.
- *Biometric Access Control Lab* - for students to gain an understanding of biometric security concepts.
- *Hackers Research Lab* - for students to gain hands-on training in IT security
- *Security Operation Centre (SOC) Lab* - with appraise infrastructure and relevant applications.
- *Faculty of Business and Information* Technology *(FBIT) Cybersecurity and Resilience Testing Infrastructure (CRTI)* - currently under construction thanks to the recently obtained CFI/JELF grants. This will host the relevant equipment such as Spirent CyberFlood Security and Performance Testing Platform, ufiSpace programmable P4 switches, to support the envisaged research projects.
- *FBIT Research Labs/Groups* - which make use of the Cybersecurity-Related Research Facilities of the Institute for Cybersecurity and Resilient Systems (ICRS). These labs are:
  - Advanced Networking and Security (ANTS) Lab
  - Human Machine Lab
  - Security, Artificial Intelligence and Networks (SAIN) Lab
  - Trustworthy AI Lab
  - Business Analytics and AI Group
  - Interactive Media and Virtual Reality Research Group

## 2. EVALUATION CRITERIA

**NOTE:** Reviewers are asked to provide feedback on each of the following Evaluation Criteria (Quality Assurance Framework 2021, Section 2.1.2).

### 2.1 Program Objectives

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

The objectives of the proposed PhD in Cybersecurity program at Ontario Tech University are consistent with the institution's mission and academic plans. Here are the key points that illustrate this alignment:
Institution's Mission and Vision: Ontario Tech's mission includes advancing the application of knowledge to address societal needs, fostering innovation, and nurturing a technology-enriched learning environment. The proposed PhD program, being multidisciplinary and research-intensive, focuses on technology, policy, and human behavior within cybersecurity, aiming to develop specialized socio-technical academics. This aligns well with the university's goals of advancing scientific and technical knowledge and addressing complex societal issues through a "Tech with a Conscience" approach.

- *Strategic and Academic Plans*: The program supports Ontario Tech's strategic priorities, including partnership and intellectual resilience. The affiliation with the Institute for Cybersecurity and Resilient Systems (ICRS) facilitates connections with industry, government, and research institutes, promoting interdisciplinary research and collaboration. These elements align with the university's emphasis on partnership and innovation as stated in its strategic plans.
- *Integrated Academic and Research Plan*: The PhD program contributes to areas identified as strengths or growth within the university's strategic mandate, such as digital technologies and artificial intelligence. By building on the successful Master of IT Security program and expanding into cybersecurity, the program supports the university's focus on developing programs that meet market demands and enhance its research capacity in emerging, impactful areas.

Thus, the proposed PhD program in Cybersecurity is well-aligned with the Ontario Tech University's mission, stated strategic priorities, and academic plans, reflecting a commitment to excellence and innovation in education and research in the field of cybersecurity. It is also consistent with the Graduate Degree Level Expectations (GDLEs).

## 2.2 Program requirements

- Appropriateness of the program's structure and the requirements to meet its objectives and program-level learning outcomes
- Appropriateness of the program's structure, requirements and program-level learning outcomes in meeting the undergraduate or graduate Degree Level Expectations
- 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 structure of the proposed PhD in Cybersecurity program at Ontario Tech University and the requirements to meet program objectives and program-level learning outcomes are appropriately designed. Here's a detailed look at how the program structure and requirements align with and support the achievement of its objectives and learning outcomes:

- *Coursework:* The program includes a combination of prerequisite and specialized courses, ensuring a comprehensive understanding of both fundamental and advanced topics in cybersecurity. This includes courses on IT security, law and ethics, AI in cybersecurity, and more.
- *Research Components*: The PhD program emphasizes research with components like a seminar course, thesis proposal, candidacy exam, and a final dissertation. This structure supports deep research engagement and innovation, critical for a doctoral level program.
- *Interdisciplinary Approach:* The program's affiliation with the Institute for Cybersecurity and Resilient Systems (ICRS) promotes interdisciplinary research, enhancing the breadth and depth of students' academic and professional development.
- *Admission Requirements:* Admission criteria are stringent, requiring a thesis-based Master's degree and a strong academic record, ensuring that incoming students are well-prepared and capable of high-level research. The multidisciplinary nature of the program suggests that some students may come to the program with more or less Science, Technology, Engineering, and Mathematics (STEM) in their background, the program is designed to move these students to an equal footing in the same way as any other graduate programs in cybersecurity.
- *Learning Outcomes:* The program defines clear learning outcomes related to knowledge of cybersecurity threats, risk management practices, the application of AI in cybersecurity, and the social, economic, and business aspects of the field. These outcomes are assessed through exams, defense presentations, and the thesis, ensuring that students achieve a deep and practical understanding of the field.
- *Supporting Activities:* The program includes activities like seminars and workshops that are critical for developing communication skills and professional capabilities, further supporting the learning outcomes aimed at preparing students for academia, industry, and policy-making roles.

The structure and requirements are designed to ensure that graduates:

- Have a deep and broad understanding of cybersecurity, from technical aspects to policy implications.
- Are capable of conducting independent, impactful research.
- Can effectively communicate complex ideas and research findings to a variety of audiences, crucial for roles in academia, industry, and government.

In summary, the program's structure and the requirements are well-tailored to meet its stated objectives and learning outcomes, preparing students for high-level careers in cybersecurity and related fields. This alignment supports Ontario Tech University's mission to foster knowledge and innovation in areas of societal importance.

## 2.3 Program requirements for graduate programs only

- Clear rationale for program length that ensures that students can complete the program level learning outcomes and requirements within the proposed time
- Evidence that each graduate student in the program is required to take a minimum of two-thirds of the course requirements from among graduate-level courses
- For research-focused graduate programs, clear indication of the nature and suitability of the major research requirements for degree completion

Yes, the structure, requirements, and program-level learning outcomes of the proposed PhD in Cybersecurity at Ontario Tech University are designed to meet the institution's Graduate Degree Level Expectations (GDLEs). Here's how the program aligns with these expectations:

Alignment with Graduate Degree Level Expectations

- *Depth and Breadth of Knowledge*: The program offers specialized coursework and interdisciplinary research opportunities that provide comprehensive knowledge in cybersecurity. Courses like "Fundamentals of IT Security" and "AI in Cybersecurity" ensure depth and breadth of knowledge in the field.
- *Research and Scholarship*: A strong emphasis on research is evident in the structure of the program, which includes a research thesis, candidacy exam, and dissertation defense. These components aim to foster the ability to generate new knowledge and satisfy peer review, key aspects of the GDLEs.
- *Level of Application of Knowledge*: The program is designed to train students to apply their knowledge in practical settings, addressing complex cybersecurity issues. This application is supported through specialized courses and the research thesis, where students tackle real-world problems.
- *Professional Capacity and Autonomy*: The PhD program encourages intellectual independence and ethical behavior in research. Program requirements such as the development of a personal research statement and the need for a faculty supervisor support the development of professional skills and autonomy.
- *Communication Skills*: Students are expected to communicate their research findings effectively, a requirement that is directly assessed during the thesis and candidacy defenses. Additionally, the program includes seminars where students can refine their presentation and communication skills.
- *Awareness of Limits of Knowledge*: The curriculum and research components of the program are designed to cultivate an appreciation of the complexity and limits of knowledge within the cybersecurity domain. This is achieved through critical analysis tasks and discussions on the ethical, social, and legal implications of cybersecurity technologies and practices.

Supporting Activities and Outcomes

- *Interdisciplinary Learning*: The program's affiliation with the Institute for Cybersecurity and Resilient Systems promotes interdisciplinary collaboration, enhancing students' ability to integrate knowledge from various fields into their cybersecurity research.
- *Practical and Ethical Training*: Courses on law, ethics, and governance in IT security ensure that students are well-versed in the practical and ethical aspects of cybersecurity, aligning with professional capacity expectations.
- *Research Opportunities and Innovation*: Opportunities for innovative research are supported by the program's structure, which encourages collaboration with industry and government agencies, fostering real-world impact and innovation.

In conclusion, the PhD in Cybersecurity program at Ontario Tech University is well-structured to meet the Graduate Degree Level Expectations by ensuring that graduates are knowledgeable, capable researchers, effective communicators, and ethically aware professionals prepared to contribute significantly to the field of cybersecurity and beyond.

## 2.4 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
  iv. How the resulting information will be documented and subsequently used to inform continuous program improvement

The methods used to assess student achievement of the program-level learning outcomes and degree level expectations. These methods also aim to monitor and assess the overall quality of the program, its achievement of proposed objectives, and whether students are meeting the program-level learning outcomes. Here's how the program plans to achieve these assessments:

Assessment of Learning Outcomes:

- *Examinations and Coursework*: Courses within the program utilize exams, projects, and presentations to assess students' understanding and application of knowledge. These assessments directly relate to specific learning outcomes outlined in the course syllabi.
- *Thesis Proposal and Defense*: The research proposal and final thesis defense are critical components where students must demonstrate their depth of knowledge, research skills, and the ability to contribute original insights to the field of cybersecurity.
- *Candidacy Exam*: This serves as a formal assessment of students' preparedness to conduct doctoral-level research, testing their knowledge and research plans against program objectives and learning outcomes.

Monitoring Program Quality and Objectives:

- *Annual Reviews*: The program plans to conduct annual reviews involving faculty assessments, student feedback, and program outcome analyses. These reviews help evaluate the effectiveness of the teaching methods and curriculum structure.
- *External Reviews*: Regular external assessments by academic peers and industry stakeholders provide objective insights into the program's relevance and effectiveness in meeting current cybersecurity challenges.

Assessing Achievement of Program Objectives:

- *Alumni Surveys and Employment Data*: By tracking graduates' career progress and obtaining feedback on their professional achievements, the program can assess how effectively it prepares students for roles in academia, industry, or policy-making.
- *Research Output and Impact*: Evaluations of students' research contributions to peer-reviewed journals and conferences provide measurable outcomes that reflect the program's success in achieving its academic objectives.

Documentation and Use of Assessment Information:

- *Continuous Improvement Process*: Assessment results are documented systematically and reviewed by the program committee to identify areas for improvement. This ongoing process ensures that the curriculum remains current and aligned with industry and academic advancements.
- *Strategic Adjustments*: Findings from these assessments inform curriculum revisions, teaching methods, and student support services, enhancing the program's overall effectiveness and its alignment with Degree Level Expectations.

The proposed PhD in Cybersecurity program at Ontario Tech University utilizes a comprehensive and structured approach to assess and monitor student achievements and the program's overall quality. The use of varied and rigorous assessment tools, combined with a clear mechanism for using the resulting data to drive continuous improvement, ensures that the program remains effective in meeting its objectives and adapting to the evolving field of cybersecurity. These measures are aligned with the standards set by the Quality Assurance Framework, ensuring that the program not only meets academic and industry standards but also prepares graduates to effectively contribute to and lead in the cybersecurity domain.

## 2.5 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 admission requirements for the PhD in Cybersecurity program at Ontario Tech University are well-structured and appropriately aligned with the program's objectives and program-level learning outcomes. The requirements ensure that incoming students possess the necessary academic background and research potential to succeed in this multidisciplinary, research-intensive program.

- *Educational Background*: Applicants are expected to have completed a four-year undergraduate degree and a thesis-based Master's degree in a relevant field. This ensures that students have a strong foundational knowledge and research experience in fields pertinent to cybersecurity. The requirement of an overall academic standing of at least 3.5 on a 4.0/4.3 scale underscores the program's commitment to academic excellence and ensures that students are well-prepared for the rigors of doctoral-level study.
- *Letters of Reference*: A minimum of two letters of reference from individuals who have direct knowledge of the applicant's academic competence is required. This allows the admissions committee to assess the applicant's suitability for the program based on feedback from credible sources who can attest to their research abilities and academic performance.
- *English Proficiency*: Proof of English proficiency for applicants whose first language is not English ensures that all students can effectively communicate and engage with the program's content, facilitating a productive learning environment.
- *Prospective Supervisor*: Applicants must find a prospective faculty supervisor from the list of graduate faculty members and receive formal acceptance from the supervisor. This requirement ensures that students have a clear research direction and mentorship from the outset, which is crucial for success in a research-intensive program.
- *Personal Research Statement*: The requirement of a minimum 3000-word personal research statement allows applicants to articulate their research interests and proposed academic research plan. This helps in assessing the applicant's alignment with the program's research objectives and their preparedness for undertaking significant research projects.
- *Sufficient Explanation of Alternative Requirements*: Graduates of Ontario Tech University's Master of IT Security (MITS) program can apply to the PhD program if they have an overall academic standing of at least 3.5/4.3. This provides a clear and accessible pathway for students from a related master's program to advance to doctoral studies.
- *Waiver Requests for Prerequisites*: Students who demonstrate sufficient proficiency through prior graduate-level coursework or extensive related work experience can request a waiver for certain prerequisite courses. This flexibility recognizes prior learning and professional experience, ensuring that students are not required to repeat content they have already mastered.

The admission requirements for the PhD in Cybersecurity program are comprehensive and appropriately tailored to the program's objectives and learning outcomes. They ensure that students have the requisite academic preparation, research potential, and language proficiency to succeed in the program. The inclusion of alternative requirements and pathways, such as the MITS pathway and waiver requests, demonstrates a thoughtful and inclusive approach to recognizing diverse educational backgrounds and professional experiences. Overall, these admission criteria are well-designed to attract and admit highly qualified candidates who are well-prepared to contribute to the field of cybersecurity research.

## 2.6 Resources for all programs

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 and achieve the goals of 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 resource commitments to support the program in step with its ongoing implementation

The resources available to sustain the quality of scholarship and research activities for the proposed PhD in Cybersecurity at Ontario Tech University are adequately provided, covering aspects such as library support, information technology support, and laboratory access:

- *Library Support*: The Library Report details a robust collection of resources that support the cybersecurity field, including over 98,000 print volumes and 167,892 journal subscriptions. Additionally, there are more than 1.3 million e-books and substantial electronic resources accessed through consortia licensing with major academic publishers. This provides a strong foundation for research and scholarship needs of PhD students.
- *Information Technology Support*: The university has committed resources to ensure that IT support is sufficiently robust to handle the specialized needs of cybersecurity research. This includes access to high-performance computing resources and secure data storage solutions, which are essential for handling the large datasets and complex simulations often required in cybersecurity research.
- *Laboratory Access*: The program proposal outlines access to specialized laboratories and research facilities that are part of the Institute for Cybersecurity and Resilient Systems. These facilities are designed to support advanced research in cybersecurity, including practical experiments and simulations, providing a crucial resource for doctoral research activities.

These resources collectively ensure that students have access to the necessary tools and environments to conduct high-level research, fostering innovation and maintaining a high standard of academic rigor within the program.

### 2.7 Resources for graduate programs only

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

- Evidence that faculty have the recent research or professional/clinical expertise needed to sustain the program, promote innovation, and foster an appropriate intellectual climate
- Where appropriate to the program, evidence that financial assistance for students will be sufficient to ensure adequate quality and numbers of students
- Evidence of how supervisory loads will be distributed, in light of qualifications and appointment status of the faculty

The faculty associated with the proposed PhD in Cybersecurity program at Ontario Tech University have the requisite recent research expertise and professional credentials to sustain the program, foster innovation, and maintain an appropriate intellectual climate. The Faculty CVs highlight diverse research activities and professional experience in areas critical to cybersecurity, including but not limited to, network security, AI, information trust, ethical hacking, and data privacy. Moreover, many faculty members have active research projects and collaborations that not only align with the program's focus but also ensure ongoing contributions to cutting-edge developments in the field. This active engagement in current research ensures that the program remains at the forefront of technological and academic advancements, which is essential for promoting innovation and fostering an intellectual climate conducive to advanced study and research in cybersecurity. The faculty's alignment with the program's multidisciplinary approach also supports a robust intellectual climate, where knowledge from different sub-fields of cybersecurity is integrated, offering students a comprehensive and nuanced understanding of the subject. This approach not only enriches the students' learning experience but also prepares them to tackle complex challenges in the cybersecurity landscape.

The financial assistance provided to students in the proposed PhD in Cybersecurity at Ontario Tech University appears sufficient to ensure the quality and numbers of students are maintained. The self-study document outlines various scholarships, awards, and funding opportunities that are available to graduate students. Specifically, students have access to scholarships like the Ontario Graduate Scholarship and Canada Graduate Scholarships, along with various internal awards provided by the university. Additionally, research assistantships funded by faculty grants can also provide financial support to students. The document also mentions the university's commitment to ensuring competitive funding packages to attract high-quality students. It acknowledges that the ability to offer competitive funding is crucial for attracting and retaining the best students, which directly impacts the program's quality and success.

The supervisory loads for the proposed PhD in Cybersecurity at Ontario Tech University are adequately distributed, considering the qualifications and appointment status of the faculty involved. The document details that faculty members from various departments and specializations will contribute to supervising students, ensuring a broad base of expertise and support. Furthermore, the faculty's qualifications, including their academic backgrounds, research accomplishments, and practical cybersecurity experience, align with the program's multidisciplinary approach. This diversity allows for a more enriching supervisory experience for students and ensures that supervisory duties are not concentrated among a few faculty members, thus preventing overloading. Additionally, the program plans to leverage industry partnerships and external collaborations, which could further distribute supervisory responsibilities and enhance the learning experience by integrating real-world perspectives and expertise into student supervision.

## 2.8 Quality and other indicators

- Evidence of 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

**NOTE**: Reviewers are urged to avoid using references to individuals. Rather, they are asked to assess the ability of the faculty as a whole to deliver the program and to comment on the appropriateness of each of the areas of the program (fields) that the university has chosen to emphasize, in view of the expertise and scholarly productivity of the faculty.

The faculty involved in the proposed PhD program in Cybersecurity at Ontario Tech University appears well-equipped to deliver a comprehensive and research-intensive program based on their qualifications, research achievements, and commitment to mentoring students.

- *Qualifications and Expertise*: The faculty members hold advanced degrees in relevant fields, including computer science, cybersecurity, and information technology, among others. This educational background is essential for delivering the multidisciplinary aspects of the cybersecurity program which includes technology, policy and governance, artificial intelligence, and human behavior.

- *Research and Scholarly Record*: The faculty members are, as expected, diverse in their research interests and have a range of expertise from deep specialization through to tangential interests, but they are actively involved in cutting-edge research, contributing to areas critical to the program such as cyber-physical systems security, data privacy, and the applications of AI in cybersecurity. Their work is well-circulated in reputable academic journals, indicating a strong scholarly output which is critical for a PhD-level program. The faculty members are qualified to deliver various aspects of the proposed program and provide a solid foundation to initiate the program.
- *Funding, Honours, and Awards*: Many faculty members have secured significant research grants and awards from national and international bodies, enhancing the program's profile and providing ample research opportunities for students. Such funding is crucial for sustaining high-level research activities and for students to engage in funded projects.
- *Commitment to Student Mentoring*: The faculty have a demonstrated commitment to mentoring, with several members having received accolades for their teaching and student guidance. This mentorship is vital in a PhD program for fostering a supportive and productive learning environment.
- *Program Delivery and Teaching Methods*: The program uses a diverse set of delivery methods, including traditional lectures, seminars, and hybrid formats, which cater to different learning preferences and enhance student engagement. This variety helps in addressing complex cybersecurity topics comprehensively. The delivery modality is consistent with most modern graduate programs in cybersecurity.
- *Research Opportunities*: The program provides extensive research opportunities that are integrated into the curriculum through thesis work, specialized courses, and direct involvement with the Institute for Cybersecurity and Resilient Systems (ICRS). This exposure to active research projects under the guidance of experienced faculty ensures that students are at the cutting edge of cybersecurity developments.
- *Student Support and Resources*: The university ensures that cybersecurity PhD students have access to substantial academic resources, including a robust library system with specialized journals and databases in cybersecurity, and support for data management and open access publishing. These resources are critical for supporting high-level academic work and innovation in the field.
- *Mentorship and Professional Development*: The program emphasizes mentorship and the development of professional skills through seminars and personalized guidance from faculty. This approach not only enhances the academic rigor of student projects but also prepares them for future roles in academia, industry, or government.
- *Interdisciplinary Collaboration*: The program's structure encourages interdisciplinary collaboration, which is crucial for addressing the multifaceted challenges in cybersecurity. This interdisciplinary approach is supported by collaborations between faculties and departments, enriching the student learning experience by integrating diverse perspectives and expertise.
- The PhD program in Cybersecurity at Ontario Tech University has established strong criteria and support systems for student success, which are evident in several key areas.
- *Grade-Level for Admission*: Students applying to the program are expected to have a strong academic background, typically requiring a minimum GPA of 3.5 on a 4.0/4.3 scale in their last two years of a thesis-based master's degree in a relevant field. This high standard ensures that incoming students can engage deeply with the program's advanced content.
- *Scholarly Output and Awards*: The program is designed to enhance students' research capabilities, which is reflected in their scholarly output. While specific data on publications and conference presentations by current students were not detailed, the program's structure and faculty support are oriented towards producing high-quality research, which likely contributes to student success in these areas.

- *Success Rates in Scholarships and Competitions*: The students in the program are encouraged and supported in applying for provincial and national scholarships, with the structured mentorship and resources aimed at improving their competitiveness in these arenas.
- *Commitment to Professional and Transferable Skills*: The program incorporates professional development through seminars and workshops that focus on both the specific skills needed for cybersecurity and transferable skills such as communication, project management, and ethical considerations in technology. This commitment is critical for preparing students for diverse career paths in academia, industry, or government.
- *Times-to-Completion and Retention Rates*: The program aims for a completion time of around four to five years for full-time students, reflecting a structured and efficient pathway through coursework, research, and thesis completion. Retention rates are supported by comprehensive academic and personal support systems, although specific statistics on retention were not provided.

## 3. EQUITY, DIVERSITY, INCLUSION, AND DECOLONIZATION

Please comment on any consideration of the principles of equity, diversity, inclusion, and decolonization in the new program.

The proposed PhD program in Cybersecurity at Ontario Tech University demonstrates a commitment to the principles of equity, diversity, inclusion, and decolonization (EDID). These principles are integrated into various aspects of the program to ensure a supportive, inclusive, and equitable environment for all students. Here are some key points highlighting how these principles are considered in the new program:

- *Admissions Process*: The program has clear, transparent admission criteria that consider diverse academic backgrounds and professional experiences. By allowing waiver requests for certain prerequisite courses, the program recognizes prior learning and work experience, ensuring equitable access for students from various educational pathways.
- *Support for Underrepresented Groups*: The program encourages applications from underrepresented groups in the field of cybersecurity. This includes specific outreach efforts to attract a diverse applicant pool, ensuring that all students have equal opportunities to access the program.
- *Inclusive Curriculum*: The program covers a broad range of themes related to cybersecurity, including technology, business, policy, governance, AI, and human behavior. This multidisciplinary approach ensures that diverse perspectives are integrated into the curriculum, enriching the learning experience for all students.
- *Diverse Faculty*: The program is affiliated with the Institute for Cybersecurity and Resilient Systems (ICSR), which brings together a multidisciplinary team of researchers and faculty members. This diversity in expertise and background provides students with a wide range of perspectives and mentorship opportunities.
- *Support Services*: The program offers various support services to ensure an inclusive learning environment. This includes access to academic support, counseling services, and mentorship programs designed to help all students succeed, regardless of their background.
- *Library Resources*: The library provides extensive resources, including e-books, journals, and databases that cover diverse topics and perspectives in cybersecurity. Additionally, the library offers information literacy instruction tailored to the needs of students, ensuring they can effectively utilize these resources.
- *Curriculum Content*: The program includes a critical examination of the social and ethical implications of technology, which encompasses discussions on decolonization and the impact of cybersecurity on indigenous communities. This ensures that students are aware of and can critically engage with these important issues.
- *Research Opportunities*: Students are encouraged to undertake research that addresses the needs and concerns of marginalized and indigenous communities. This approach not only contributes to decolonization efforts but also broadens the scope and impact of cybersecurity research.

The PhD program in Cybersecurity at Ontario Tech University incorporates the principles of equity, diversity, inclusion, and decolonization in a comprehensive manner. From the admissions process to curriculum content and support services, the program is designed to provide an inclusive and equitable educational environment. These efforts ensure that students from diverse backgrounds can thrive and contribute to the field of cybersecurity, ultimately enriching the academic community and the society.

## 4. OTHER ISSUES

- Please highlight any unique curriculum or program innovation, creative components, or significant high-impact practices
- Please identify any other issues that may not be covered above

The PhD program in Cybersecurity at Ontario Tech University offers several unique and innovative elements that distinguish it from other programs in the field. These innovations and high-impact practices are designed to enhance the educational experience and ensure that graduates are well-prepared for both academic and industry roles in cybersecurity. One of the standout features of the PhD in Cybersecurity program is its multidisciplinary approach. The program integrates themes from technology, business, policy, governance, artificial intelligence, and human behavior. This broad perspective ensures that students gain a comprehensive understanding of cybersecurity, which is essential for addressing the complex and interconnected challenges in this field. By covering a wide range of topics, the program prepares students to tackle issues from various angles, fostering innovation and critical thinking.

Another innovative aspect of the program is its affiliation with the Institute for Cybersecurity and Resilient Systems (ICSR). This affiliation provides students with access to a multidisciplinary, global center for cybersecurity research, innovation, teaching, and outreach. The ICSR's resources and networks offer students unparalleled opportunities to engage in cutting-edge research and collaborate with leading experts in the field. This connection enhances the program's academic rigor and provides students with valuable industry connections and practical experience.

The program also includes a strong emphasis on real-world applications and high-impact practices. For example, the curriculum incorporates specialized courses that address current and emerging topics in cybersecurity, such as artificial intelligence in cybersecurity, usable security, information trust, and blockchain technologies. These courses ensure that students are not only learning the theoretical foundations but also gaining practical skills that are directly applicable to contemporary cybersecurity challenges. Moreover, the program's structure includes seminars, a thesis proposal, and a final thesis, which are designed to foster research skills and academic excellence. The requirement for students to present seminars and defend their thesis proposals and final dissertations in oral examinations ensures that they develop strong communication and presentation skills, which are crucial for both academic and professional success.

One of the key strengths of the PhD in Cybersecurity program is its flexibility in recognizing prior learning and professional experience. The program allows students to request waivers for certain prerequisite courses if they can demonstrate sufficient proficiency through prior graduate-level coursework or extensive related work experience. This flexibility is important for accommodating students from diverse educational and professional backgrounds, ensuring that the program is accessible to a wider range of applicants. The program's admission requirements, which include finding a prospective faculty supervisor and submitting a detailed personal research statement, ensure that students have a clear research direction and are well-prepared for the demands of the program. However, it is crucial to ensure that prospective students receive adequate guidance and support in identifying potential supervisors and developing their research proposals, as this can be a challenging process for applicants. Additionally, while the program's multidisciplinary approach and broad range of topics are strengths, it is important to ensure that the curriculum remains coherent and focused. Maintaining a balance between breadth and depth in the curriculum is essential to ensure that students gain a comprehensive yet detailed understanding of cybersecurity.

Overall, the PhD program in Cybersecurity at Ontario Tech University is well-designed, innovative, and aligned with current trends and challenges in the field. Its multidisciplinary approach, strong industry connections, and emphasis on practical skills and high-impact practices make it a standout program that is well-equipped to prepare students for successful careers in cybersecurity. By continuing to support students throughout the admission process and maintaining a balanced curriculum, the program can ensure that it remains at the forefront of cybersecurity education and research.

## 5. SUMMARY AND RECOMMENDATIONS

Please provide a summary of your conclusions and include a numbered list of each of your recommendations.

The proposed PhD program in cybersecurity at Ontario Tech University is designed to meet the growing global demand for advanced research and practical skills in the cybersecurity field. This program is expected to provide a robust curriculum that equips students with both theoretical and practical knowledge needed to address and mitigate modern cybersecurity challenges effectively. Key aspects of the program likely include a strong focus on interdisciplinary learning, which integrates insights from fields such as artificial intelligence, law, ethics, and business with core cybersecurity principles. This approach not only broadens the students' understanding, but also enhances their ability to innovate and solve complex problems across different sectors. Hands-on learning experiences are anticipated to be a cornerstone of the program, with students gaining practical skills through labs, simulations, and real-world projects. These activities are crucial for translating theoretical knowledge into practical, actionable skills in a real-world context. Collaboration with industry is expected to play a significant role in the program, providing students with exposure to the latest challenges and innovations in the field. These collaborations are also vital for networking, job placement, and practical insights into the cybersecurity industry. The program aims to continuously evolve by incorporating cutting-edge research, technology, and teaching methods. This ensures that graduates are not only well-prepared to enter the workforce but are also capable of leading the way in innovation and best practices in cybersecurity.
To further improve the program, in the long-term, following actions can be taken:

- *Funding for Research Chairs in the field*: Seek external funding to establish research chairs in cybersecurity including industry chairs, Canada Research Chairs, Canada Excellence Research Chairs to attract top-tier faculty and researchers.
- *Enhance Interdisciplinary Opportunities*: The program should further integrate interdisciplinary courses and projects that involve fields such as AI, law, and business ethics. This can be achieved by developing new courses or modifying existing ones to include interdisciplinary perspectives and problem-solving experiences.
- *Industry Collaboration and Partnerships*: Strengthen ties with the cybersecurity industry to facilitate ongoing student engagement through internships, guest lectures, and live project collaborations. This requires reaching out to potential industry partners and setting up agreements that benefit both the students and the companies involved.

Overall, the proposed PhD program at Ontario Tech University represents a significant step forward in cybersecurity education, aligning academic rigor with industry needs and future technological advancements. The program's success will rely on its ability to adapt, innovate, and maintain relevance in the rapidly changing landscape of global cybersecurity challenges.

**NOTE:** The responsibility for arriving at a recommendation on the final classification of the program belongs to the Appraisal Committee. Individual reviewers are asked to refrain from making recommendations in this respect.

**Signature:**

**Date: July 3, 2024**

**Signature:**

**Date: July 3, 2024**

Faculty Response to the External Review for the

Ph.D. in CyberSecurity

Submitted By:

Shahram Heydari

Date 13 August, 2024

Carolyn McGregor, FBIT Dean

13 August, 2024

## Introduction

We thank the external reviewers Dr. Ali Dehghantanha (University of Guelph) and Dr. Isaac Woungang (Toronto Metropolitan University) for their positive and constructive comments. Dr. Dehghantanha and Dr. Woungang have prior experience in directing relevant graduate programs at their respective institutions. They conducted a thorough analysis of the program, identified our strengths, and concluded that the proposed program "is well-designed, innovative, and aligned with current trends and challenges in the field. Its multidisciplinary approach, strong industry connections, and emphasis on practical skills and high-impact practices make it a standout program that is well-equipped to prepare students for successful careers in cybersecurity. By continuing to support students throughout the admission process and maintaining a balanced curriculum, the program can ensure that it remains at the forefront of cybersecurity education and research."

They also note that the proposed program "represents a significant step forward in cybersecurity education, aligning academic rigor with industry needs and future technological advancements. The program's success will rely on its ability to adapt, innovate, and maintain relevance in the rapidly changing landscape of global cybersecurity challenges."

They have also kindly pointed out the areas to be considered for improvement and long term success of the program. We greatly appreciate their vote of confidence and recommendations and will address them to improve the program.

## Summary of Recommendations and Faculty Responses

- *Restate the recommendations summarized in the external reviewers' report and provide the Program's comments and responses*
- *The Dean should then provide summative comments/responses from an overarching Faculty perspective for each recommendation and program response*

**Recommendation 1**
*Funding for Research Chairs in the field: Seek external funding to establish research chairs in cybersecurity including industry chairs, Canada Research Chairs, Canada Excellence Research Chairs to attract top-tier faculty and researchers.*

**Program's Response**
This is an excellent idea and will certainly bring expertise and recognition to the program. The proposal will be updated to recommend prioritizing research chair positions in the field of cybersecurity.

**Dean's response**
Within Ontario Tech University, allocation of Canada Research Chairs (CRC)s is managed centrally by the Office of Research Services and faculties have the option to bid for CRC. Cybersecurity is one of the four key research priority areas within FBIT and we will work to ensure we bid for a CRC in Cybersecurity (or related area) position within our faculty at any opportunity in the coming years.

In addition, I am currently working with Advancement to create opportunities for donor funds to support a research chair position in Cybersecurity (or related area).

**Recommendation 2**

*Enhance Interdisciplinary Opportunities: The program should further integrate interdisciplinary courses and projects that involve fields such as AI, law, and business ethics. This can be achieved by developing new courses or modifying existing ones to include interdisciplinary perspectives and problem-solving experiences.*

**Program's Response**
We agree that including of interdisciplinary courses are essential to the success of the program. In addition to the existing courses in these areas, several new courses have been proposed by the affiliated faculty members in the program and will be sent for approval to FBIT faculty council.

**Dean's response**
This recommendation is well received and we will work to ensure that new courses are proposed and receive Faculty Council so they can then continue through the remaining governance structure of approvals. Actual course offerings year on year will be managed within the context of the overall budget of courses offered within the faculty and specifically for this program based on enrolment.

**Recommendation 3**
*Industry Collaboration and Partnerships: Strengthen ties with the cybersecurity industry to facilitate ongoing student engagement through internships, guest lectures, and live project collaborations. This requires reaching out to potential industry partners and setting up agreements that benefit both the students and the companies involved.*

**Program's Response**
We agree. Our initial plan includes accelerating such partnerships through the Institute for CyberSecurity and Resilient Systems (ICRS) and the National Cybersecurity Consortium (NCC). Once the program is approved, an industry advisory board will be established to provide further directions and contacts for FBIT cybersecurity programs

**Dean's response**
We will capitalise on our partnerships through the Institute for CyberSecurity and Resilient Systems (ICRS) and the National Cybersecurity Consortium (NCC) to create such student engagement opportunities.

## Suggested Revisions for the Proposal following External Review

- *Program to list all suggested revisions to the proposal*
- *For each suggested revision, the Dean should include a comment indicating whether the revision will proceed. If the revision will not proceed, please indicate a rationale*

Added in Section 4.b:

“As recommended in the external reviewers report, it is recommended that the university prioritize hiring or appointing research chairs (NSERC CRC, Industry chairs or university research chairs) in cybersecurity, particularly in areas related to social and business aspects of cybersecurity. This is an important area of growth in the faculty and a differentiating factor that would enhance the multidisciplinary nature of the program.”

**Graduate Studies Committee**

**Monthly Library Report**

Date: October 22, 2024

## Copyright and Creative Commons Licensing on Tuesday, October 22 from 11am-12pm.

Date: Tuesday October 22, 11:00 am - 12:00 pm
Facilitators: Chelsie Lalonde, Pranjal Saloni

Open educational resources (OER) may be free, but free resources may not necessarily be open! In this workshop, participants will explore basic concepts of copyright in an educational context, including the rights, limitations, and implications of using and creating educational materials.

## Everyone is invited to join us in celebrating Science Literacy Week – October 27 – November 2!

We're celebrating Science Literacy Week at the Library this year from **Sunday, October 27th to Saturday, November 2nd**. This year's theme is intended to showcase and explore **Diversity of Information in STEM**.

> There is an increasing awareness of the need to include the voices and lived experiences of Black, Indigenous, and people of colour (BIPOC), women, and other marginalized groups who continue to be underrepresented in science, technology, engineering, and mathematics fields, as well as in leadership positions within academia and industry. Our goal this week, as well as every week throughout the year, is to help make diversity in STEM more visible within the academic community in hopes of inspiring greater appreciation and recognition of these author's important contributions.

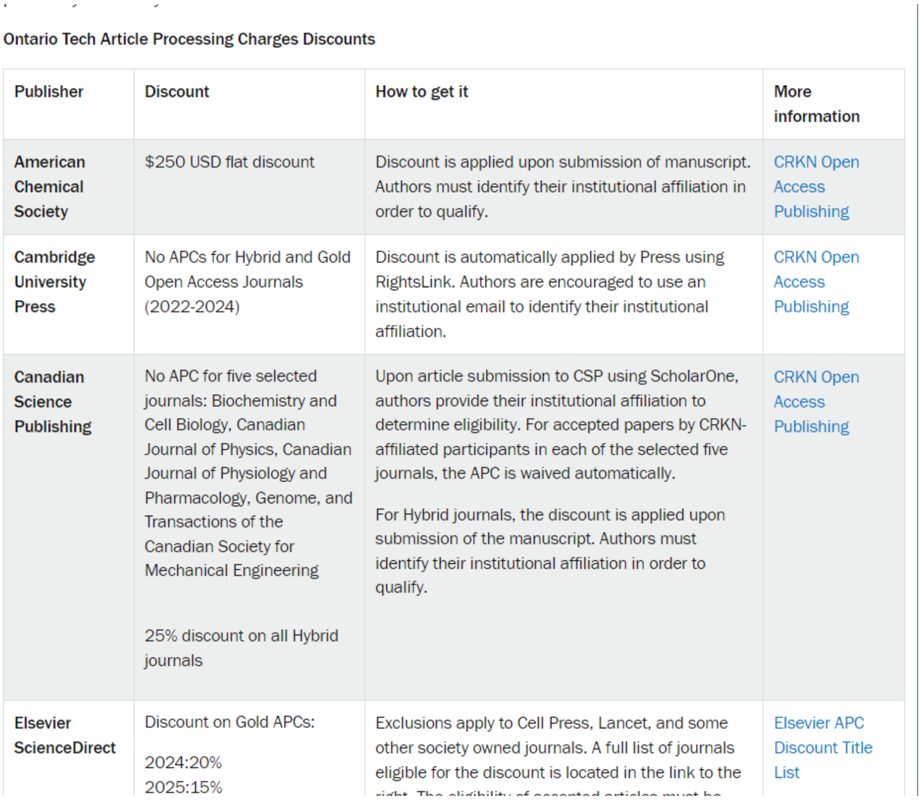
Come and say hi at our pop up at the Destress Desk at the North Oshawa Library from 11 a.m. - 12:30 p.m. on **Wednesday, October 30th**. Please drop in, grab a free coffee, a Halloween treat, and chat with us about diversity in STEM. There will also be free STEM buttons and fun STEM related activities!

**Publishing Open Access: Supports offered by the Library.**

a. *People:*
Welcoming our new Scholarly Communications and Copyright Librarian: Mia Clarkson, November 4, 2024

**b.** *Resources and guides*:

- Publishing your article open access
https://guides.library.ontariotechu.ca/openaccess/wheretopublish
- Article Processing Charges (APCs)
https://guides.library.ontariotechu.ca/openaccess/APC
  - Did you know ? APC discounts are available to Ontario Tech authors through membership in Canadian Research Knowledge Network (CRKN) negotiated agreements with publishers.



**Ontario Tech Article Processing Charges Discounts**

| Publisher | Discount | How to get it | More information |
|---|---|---|---|
| **American Chemical Society** | $250 USD flat discount | Discount is applied upon submission of manuscript. Authors must identify their institutional affiliation in order to qualify. | CRKN Open Access Publishing |
| **Cambridge University Press** | No APCs for Hybrid and Gold Open Access Journals (2022-2024) | Discount is automatically applied by Press using RightsLink. Authors are encouraged to use an institutional email to identify their institutional affiliation. | CRKN Open Access Publishing |
| **Canadian Science Publishing** | No APC for five selected journals: Biochemistry and Cell Biology, Canadian Journal of Physics, Canadian Journal of Physiology and Pharmacology, Genome, and Transactions of the Canadian Society for Mechanical Engineering<br>25% discount on all Hybrid journals | Upon article submission to CSP using ScholarOne, authors provide their institutional affiliation to determine eligibility. For accepted papers by CRKN-affiliated participants in each of the selected five journals, the APC is waived automatically.<br>For Hybrid journals, the discount is applied upon submission of the manuscript. Authors must identify their institutional affiliation in order to qualify. | CRKN Open Access Publishing |
| **Elsevier ScienceDirect** | Discount on Gold APCs:<br>2024:20%<br>2025:15% | Exclusions apply to Cell Press, Lancet, and some other society owned journals. A full list of journals eligible for the discount is located in the link to the right. The eligibility of accepted articles must be | Elsevier APC Discount Title List |

**Preamble**

This report template is designed for use by the members of the Graduate Studies Committee (GSC) at Ontario Tech University to facilitate focused and strategic discussions in the Graduate Studies Committee meetings. Reports will support understanding of developments and discussions across Faculties and Departments. The purpose of this template is to:

- Showcase achievements and innovative initiatives.
- Share collaborative efforts within and outside the university.
- Outline strategic goals and plans for graduate studies.

The template guides the presentation of information in a structured and concise manner, enabling productive dialogue and strategic planning.

## Graduate Studies Committee Report Template

*Faculty / Unit / Society Represented:* FSSH

*Submitted By:* Olga Marques, Criminology GPD

### Section 1: Departmental Highlights and Achievements

*Major Achievements*:

- Forensic Psychology has developed a recruitment flyer

### Section 2: Collaborative Efforts and Interdisciplinary Activities

*Internal Collaborations:*

The FSSH Graduate Committee met, discussed, and shared overall recruitment strategies for our respective MA/MSc/PhD programs.

### Section 3: Strategic Development and Future Plans

*Upcoming Projects/Initiatives:*

- MSPI is participating in various recruitment events next month
- MSPI is developing a part-time program map
- Forensic Psychology is organizing a virtual open house
- Criminology will be developing a recruitment flyer and other recruitment strategies
- Criminology is participating in a recruitment event on October 18

### Section 4: Additional Information

Graduate courses or events requiring support or amplification:

- Criminology would like to flag the issue of transparency for students, particularly with respect to funding. With respect to the ‘time to completion’ to be removed from the calendar, we want to ensure that it is made clear – via a note on the website and/or relevant program pages - to students that funding is no longer guaranteed for MA students who go beyond the 24 months (if this is still going to be the case).

# GRADUATE STUDIES COMMITTEE REPORT

**ACTION REQUESTED:**

**Recommendation** ☐
**Information** ☒
**Discussion/Direction** ☐
**Decision** ☐

**DATE:** **October 22nd 2024**

**PRESENTED BY:** **Adam Wingate, Associate Registrar and Director, Records and Scheduling**

**SUBJECT:** **Revisions to the Graduate Academic Schedule**

## OVERVIEW:

- The information herein falls under the Administrative Guidelines for Determining the Academic Schedule.

- The Office of the Registrar is presenting the following revisions to the Graduate Academic Schedule, published in the Academic Calendar, for information.

## BACKGROUND/CONTEXT & RATIONALE:

- The revisions to the Graduate Academic Schedule include adding specific fall and spring Convocation ceremony dates and adding grade release dates for each semester/session.

- These are established dates that are now being added to the public-facing Academic Calendars in the spirit of transparency. As Convocation ceremony dates for the upcoming academic year are already established at the time of calendar planning and publishing, it is logical to include this information in the calendar. Furthermore, as grade release timelines are established years in advance, this is pertinent information that can easily be integrated into the calendar. In the case of the latter, we have received feedback from students, faculty members, and staff alike that not having this information readily available can lead to confusion and uncertainty.

## RESOURCES REQUIRED:

- No resources required.

## PRESENTATION DATES:

- Undergraduate Studies Committee for information: October 15, 2024
- Graduate Studies Committee for information: October 22, 2024.
- Academic Council for information: October 22, 2024.

**NEXT STEPS:**
The calendar revisions will be published immediately.

## Academic schedule

- Fall semester
- Winter semester
- Spring/Summer semester

### Fall semester

| | |
|---|---|
| August 10, 2024 | Last day to submit an online application for graduation for students completing degree requirements at the end of the summer semester. |
| September 2, 2024 | Labour Day, no lectures. |
| September 3, 2024 | Lectures begin, fall semester. |
| | Last day to submit for reinstatement, fall semester. |
| | Last day to submit return from leave of absence form, fall semester. |
| | Deadline for payment of fees or submission of the Graduate Student Promissory Note, fall semester. |
| | Last day to submit a program change request, fall semester. |
| | Last day to change full-time/part-time status, fall semester. |
| | Last day to submit a leave of absence form, fall semester. |
| September 16, 2024 | End of regular registration period; last day to add courses, fall semester. |
| | Last day to drop courses in fee-per-credit graduate programs and receive a 100 per cent refund of tuition and ancillary fees, fall semester. |

| | |
|---|---|
| | Last day to withdraw from a flat-fee graduate program and receive a 100 per cent refund of tuition and ancillary fees, fall semester. |
| September 30, 2024 | Last day to withdraw from fall semester courses without academic consequences (i.e., without receiving a grade). Courses dropped after this date will be recorded on the academic transcript with a grade of W to indicate withdrawal. |
| | Last day to drop courses in fee-per-credit graduate programs and receive a 50 per cent refund of tuition fees, fall semester. |
| | Last day to withdraw from a flat-fee graduate program and receive a 50 per cent refund of tuition fees, fall semester. |
| October 14, 2024 | Thanksgiving Day, no lectures. |
| October 15 to 20, 2024 | Fall study week, no lectures. |
| October 17, 2024 | Fall Convocation Ceremonies. |
| November 13, 2024 | Last day to withdraw from fall semester courses. Active fall semester courses will be graded by instructors. |
| December 2, 2024 | Lectures end, fall semester. |
| December 3, 2024 | Study break, no lectures. |
| December 4 to 14, 2024 | Fall semester final examination period. Students are advised not to make commitments during this period (i.e., vacation, travel plans). |
| December 16, 2024 | Last day to submit final thesis package to program office to ensure graduation by end of fall semester. |
| | Last day for faculty to submit Certificate of Approval for project/paper to the School of Graduate and Postdoctoral Studies to ensure graduation by end of fall semester. |
| December 19, 2024 | Fall semester grades released. |

| | |
|---|---|
| December 24, 2024 to January 1, 2025 | University closed. |
| December 31, 2024 | Last day to submit online application for graduation for students completing degree requirements at the end of the fall semester. |

## Winter semester

| | |
|---|---|
| January 2, 2025 | University reopens. |
| January 6, 2025 | Lectures begin, winter semester. |
| | Last day to submit a return from leave of absence form, winter semester. |
| | Last day to request reinstatement, winter semester. |
| | Deadline for payment of fees or submission of Graduate Student Promissory Note, winter semester. |
| | Last day to submit a program change request, winter semester. |
| | Last day to change full-time/part-time status, winter semester. |
| | Last day to submit a leave of absence form, winter semester. |
| January 17, 2025 | End of regular registration period; last day to add courses, winter semester. |
| | Last day to drop courses in fee-per-credit graduate programs and receive a 100 per cent refund of tuition and ancillary fees, winter semester. |
| | Last day to withdraw from a flat-fee graduate program and receive a 100 per cent refund of tuition and ancillary fees, winter semester. |
| January 31, 2025 | Last day to withdraw from winter semester courses without academic consequences (i.e., without receiving a grade). Courses dropped after this date will be |

| | |
|---|---|
| | recorded on the academic transcript with a grade of W to indicate withdrawal. |
| | Last day to drop courses in fee-per-credit graduate programs and receive a 50 per cent refund of tuition fees, winter semester. |
| | Last day to withdraw from a flat-fee graduate program and receive a 50 per cent refund of tuition fees, winter semester. |
| February 17, 2025 | Family Day, no lectures. |
| February 18 to 23, 2025 | Winter study week, no lectures. |
| February 28, 2025 | Last day to submit online application for graduation for the spring session of convocation for students completing degree requirements at the end of the winter semester. |
| March 15, 2025 | Last day to withdraw from winter semester courses. Active winter semester courses will be graded by instructors. |
| April 4, 2025 | Lectures end, winter semester. |
| April 6, 2025 | Study break, no lectures. |
| April 7 to 17, 2025 | Winter semester final examination period. Students are advised not to make commitments during this period (i.e., vacation, travel plans). |
| April 17, 2025 | Last day to submit final thesis package to program office to ensure graduation by end of winter semester. |
| | Last day for faculty to submit Certificate of Approval for project/paper to the School of Graduate and Postdoctoral Studies to ensure graduation by end of winter semester. |
| April 18, 2025 | Good Friday, no scheduled academic activities. |
| April 24, 2025 | Winter semester grades released. |

## Spring/Summer semester

May 5, 2025

Lectures begin, six-week spring session and 12-week summer semester.

Last day to submit a return from leave of absence form, summer semester.

Last day to request reinstatement, summer semester.

Deadline for payment of fees or submission of Graduate Student Promissory Note, six-week spring session and 12-week summer semester.

Last day to submit a program change request, summer semester.

Last day to change full-time/part-time status, summer semester.

Last day to submit a leave of absence form, summer semester.

May 9, 2025

Last day to add six-week spring session courses.

Last day to drop six-week spring session courses in fee-per-credit programs and receive a 100 per cent refund of tuition and ancillary fees.

May 16, 2025

Last day to add courses, 12-week summer semester.

Last day to drop 12-week summer semester courses in fee-per-credit graduate programs and receive a 100 per cent refund of tuition and ancillary fees.

Last day to withdraw from a flat-fee graduate program and receive a 100 per cent refund of tuition and ancillary fees, summer semester.

Last day to withdraw from six-week spring session courses without academic consequences (i.e., without receiving a grade). Courses dropped after this date will be recorded on the academic transcript with a grade of W to indicate withdrawal.

Last day to withdraw from six-week spring session courses in fee-per-credit graduate programs and receive a 50 per cent refund of tuition fees.

May 19, 2025

Victoria Day, no lectures.

June 2, 2025

Last day to withdraw from 12-week summer semester courses without academic consequences (i.e., without receiving a grade). Courses dropped after this date will be recorded on the academic transcript with a grade of W to indicate withdrawal.

Last day to drop 12-week summer semester courses in fee-per-credit graduate programs and receive a 50 per cent refund of tuition fees.

Last day to withdraw from a flat-fee graduate program and receive a 50 per cent refund of tuition fees, summer semester.

June 4, 2025

Last day to withdraw from six-week spring session courses. Active six-week spring session courses will be graded by instructors.

June 4 to 6, 2025

Spring Convocation Ceremonies.

June 16, 2025

Lectures end, six-week spring session.

June 17, 2025

Spring six-week session study break, no lectures.

June 17 to 21, 2025

Study break, 12-week summer semester, no lectures.

June 18 to 21, 2025

Spring session final examination period. Students are advised not to make commitments during this period (i.e., vacation, travel plans).

June 22, 2025

Last day to submit an online application for graduation for students completing degree requirements at the end of the spring session.

June 23, 2025

Lectures begin, six-week summer session.

Deadline for payment of fees or submission of Graduate Student Promissory Note (fee-per-credit programs only), six-week summer session.

Lectures resume, 12-week summer semester.

June 25, 2025

Spring session grades released.

June 27,

Last day to add courses, six-week summer session.

2025

Last day to drop six-week summer session courses in fee-per-credit graduate programs and receive a 100 per cent refund of tuition and ancillary fees.

July 1, 2025

Canada Day, no scheduled academic activities.

July 7, 2025

Last day to withdraw from six-week summer session courses without academic consequences (i.e., without receiving a grade). Courses dropped after this date will be recorded on the academic transcript with a grade of W to indicate withdrawal.

Last day to drop six-week summer session courses in fee-per-credit graduate programs and receive a 50 per cent refund of tuition fees.

July 16, 2025

Last day to withdraw from 12-week summer semester courses. Active 12-week summer semester courses will be graded by instructors.

July 24, 2025

Last day to withdraw from six-week summer session courses. Active six-week summer session courses will be graded by instructors.

August 4, 2025

Civic Holiday, no lectures.

August 5, 2025

Lectures will follow the Monday schedule on this day only. Lectures end, 12-week summer semester and six-week summer session.

August 6, 2025

Study break, no lectures.

August 7 to 10, 2025

Six-week summer session and 12-week summer semester final examination period. Students are advised not to make commitments during this period (i.e., vacation, travel plans).

August 10, 2025

Last day to submit online application for graduation for students completing degree requirements at the end of the summer session.

August 15, 2025

Summer session and Spring/Summer semester grades released.

August 22, 2025

Last day to submit final thesis package to program office to ensure graduation by end of summer semester.

Last day for faculty to submit Certificate of Approval for project/paper to the School of Graduate and Postdoctoral Studies to ensure graduation by end of summer semester.

**Notes:**

- Courses offered outside the normal teaching timeframe will have add/drop deadlines pro-rated accordingly. In such cases, faculties will advise students of appropriate deadline dates during the first meeting of the class.
- It is expected that students in a fee-per-credit program will register before the beginning of classes. If you register in a fee-per-credit course after the tuition payment deadline, your tuition fees are due immediately and you may be assessed a late payment fee. Visit gradstudies.ontariotechu.ca/tuitionandfees for a list of fee-per-credit programs.
- Deadlines related to the following can be found on the Graduate Studies website: application deadlines for admission to graduate programs; deadlines for the submission of projects and major papers; deadlines for the submission of theses/dissertations and defences; tuition refund deadlines for thesis completion during a term; and deadlines for scholarships, awards and bursaries.
- Spring/summer session courses in Education may run on a schedule that varies from the above. Consult the Mitch and Leslie Frazer Faculty of Education’s website for specific start and end dates.
- Spring convocation will be held in June 2025. Fall convocation will be held in October 2025. For more details, please refer to ontariotechu.ca/convocation.

OntarioTech UNIVERSITY

**Graduate Studies Committee (GSC)**

**Draft Work Plan**
**2024-2025**

DRAFT

| Meeting | Agenda Item (Lead) | Academic Council (If Applicable) | Board (if Applicable) |
|---|---|---|---|
| **September 24, 2024** | • Associate, Assistant and Grad Faculty appointment – if applicable **(SGPS)**<br>• Curriculum Items – if Applicable **(CIQE)**<br>• Faculty/Library & Student Reports **(Chairs)** | **October 22, 2024** | **November 28, 2024** |
| **October 22, 2024** | • Associate, Assistant and Grad Faculty appointment – if applicable **(SGPS)**<br>• Curriculum Items – if Applicable **(CIQE)**<br>• Faculty/Library & Student Reports **(Chairs)**<br>• 2024-2025 Work Plan **(NC/KA)** | **November 26, 2024** | **February 20, 2025** |
| **November 26, 2024** | • Associate, Assistant and Grad Faculty appointment – if applicable **(SGPS)**<br>• Curriculum Items – if Applicable **(CIQE)**<br>• Faculty/Library & Student Reports **(Chairs)** | **January 28, 2025** | **February 20, 2025** |
| **No December Meeting** | | | |

| | | | |
|---|---|---|---|
| **January 28, 2025** | • Associate, Assistant and Grad Faculty appointment – if applicable **(SGPS)**<br>• Curriculum Items – if Applicable **(CIQE)**<br>• Faculty/Library & Student Reports **(Chairs)**<br>***Major Program Modification (MPM)  Deadline (CIQE)***<br>• Last meeting to accept MPM's (Academic Council deadline April) ; changes published to calendar in May<br>***Academic Policy Changes***<br>• Last meeting to accept Academic Policy changes ( Academic Council deadline April); changes published to calendar in May | **February 25, 2025** | **April 17, 2025** |
| **February 25, 2025** | • Associate, Assistant and Grad Faculty appointment – if applicable **(SGPS)**<br>• Curriculum Items – if Applicable **(CIQE)**<br>• Faculty/Library & Student Reports **(Chairs)**<br>• 2025-2026 Graduate Academic Calendar<br>***Minor Program Adjustments (MPA) Deadline (CIQE)***<br>• Last meeting to accept MPA's ( Academic Council for information deadline - March) ; changes published to calendar in May<br>***Minor Curriculum Changes (MCC) Deadline (CIQE)*** | **March 25, 2025** | **April 17, 2025** |

| | | | |
|---|---|---|---|
| | • Last meeting to accept MCC's for information- Does not go to Academic Council ; published to calendar in May | | |
| **March 25, 2025** | • Associate, Assistant and Grad Faculty appointment – if applicable **(SGPS)**<br>• Curriculum Items – if Applicable **(CIQE)**<br>• Faculty/Library & Student Reports **(Chairs)** | **April 22, 2025** | **June 26, 2025** |
| **April 22, 2025** | • Associate, Assistant and Grad Faculty appointment – if applicable **(SGPS)**<br>• Curriculum Items – if Applicable **(CIQE)**<br>• Faculty/Library & Student Reports **(Chairs)**<br>• Terms of Reference Review | **May 27, 2025** | **June 26, 2025** |
| **May 27, 2025** | • Associate, Assistant and Grad Faculty appointment – if applicable **(SGPS)**<br>• Curriculum Items – if Applicable **(CIQE)**<br>• Faculty/Library & Student Reports **(Chairs)** | **June 24, 2025** | **Sept 2025 TBD** |
| **June 24, 2025** | • Associate, Assistant and Grad Faculty appointment – if applicable **(SGPS)**<br>• Curriculum Items – if Applicable **(CIQE)**<br>• Faculty/Library & Student Reports **(Chairs)** | **Sept 2025 TBD** | **Sept 2025 TBD** |