2019-2020 Graduate Calendar

The information published in this Graduate Calendar outlines the rules, regulations, curricula, programs and fees for the 2019-2020 academic year, including the Summer Semester 2019, Fall Semester 2019 and the Winter Semester 2020.

For your convenience the Graduate Calendar is available in PDF format.

If you wish to link to the Graduate Calendar please refer to the Linking Guidelines.

The University is a full member of:

- Universities of Canada

Contact Information:

University of Guelph
Guelph, Ontario, Canada
N1G 2W1

519-824-4120

Revision Information:

Date	**Description**
May 1, 2019	Initial Publication
June 28, 2019	Revision 1
September 2, 2019	Revision 2
December 10, 2019	Revision 3
January 28, 2020	Revision 4

Disclaimer

The Office of Graduate and Postdoctoral Studies has attempted to ensure the accuracy of this on-line Graduate Calendar. However, the publication of information in this document does not bind the university to the provision of courses, programs, schedules of studies, fees, or facilities as listed herein.

Limitations

The University of Guelph reserves the right to change without notice any information contained in this calendar, including any rule or regulation pertaining to the standards for admission to, the requirements for the continuation of study in, and the requirements for the granting of degrees or diplomas in any or all of its programs.

The university will not be liable for any interruption in, or cancellation of, any academic activities as set forth in this calendar and related information where such interruption is caused by fire, strike, lock-out, inability to procure materials or trades, restrictive laws or governmental regulations, actions taken by the faculty, staff or students of the university or by others, civil unrest or disobedience, Public Health Emergencies, or any other cause of any kind beyond the reasonable control of the university.

The University of Guelph reaffirms section 1 of the Ontario Human Rights Code, 1981, which prohibits discrimination on the grounds of race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sex, sexual orientation, handicap, age, marital status or family status.

The university encourages applications from women, aboriginal peoples, visible minorities, persons with disabilities, and members of other under-represented groups.

Introduction

Collection, Use and Disclosure of Personal Information

Personal information is collected under the authority of the University of Guelph Act (1964), and in accordance with Ontario's Freedom of Information and Protection of Privacy Act (FIPPA) http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90f31_e.htm. This information is used by University officials in order to carry out their authorized academic and administrative responsibilities and also to establish a relationship for alumni and development purposes. Certain personal information is disclosed to external agencies, including the Ontario Universities Application Centre, the Ministry of Advanced Education and Skills Development, and Statistics Canada, for statistical and planning purposes, and is disclosed to other individuals or organizations in accordance with the Office of Registrarial Services Departmental Policy on the Release of Student Information. For details on the use and disclosure of this information call the Office of Registrarial Services at the University at (519) 824-4120 or see https://www.uoguelph.ca/registrar/

Statistics Canada - Notification of Disclosure

For further information, please see Statistics Canada's web site at http://www.statcan.gc.ca and Section XIV Statistics Canada.

Address for University Communication

Depending on the nature and timing of the communication, the University may use one of these addresses to communicate with students. Students are, therefore, responsible for checking all of the following on a regular basis:

Email Address

The University issued email address is considered an official means of communication with the student and will be used for correspondence from the University. Students are responsible for monitoring their University-issued email account regularly.

Home Address

Students are responsible for maintaining a current mailing address with the University. Address changes can be made, in writing, through Registrarial Services.

Name Changes

The University of Guelph is committed to the integrity of its student records, therefore, each student is required to provide either on application for admission or on personal data forms required for registration, their complete, legal name. Any requests to change a name, by means of alteration, deletion, substitution or addition, must be accompanied by appropriate supporting documentation.

Student Confidentiality and Release of Student Information Policy Excerpt

The University undertakes to protect the privacy of each student and the confidentiality of their record. To this end the University shall refuse to disclose personal information to any person other than the individual to whom the information relates where disclosure would constitute an unjustified invasion of the personal privacy of that person or of any other individual. All members of the University community must respect the confidential nature of the student information which they acquire in the course of their work.

Complete policy at https://www.uoguelph.ca/secretariat/office-services/university-secretariat/university-policies .

Learning Outcomes

Graduate Degree Learning Outcomes

On May 27, 2013, the University of Guelph Senate approved the following five University-wide Learning Outcomes as the basis from which to guide the development of graduate degree programs, specializations and courses:

1. Critical and Creative Thinking
2. Literacy
3. Global Understanding
4. Communication
5. Professional and Ethical Behaviour

These learning outcomes are also intended to serve as a framework through which our educational expectations are clear to students and the broader public; and to inform the process of outcomes assessment through the quality assurance process (regular reviews) of programs and departments.

An on-line guide to the learning outcomes, links to the associated skills, and detailed rubrics designed to support the development and assessment of additional program and discipline-specific outcomes, are available for reference on the Learning Outcomes website

Critical and Creative Thinking

Critical and creative thinking is a concept in which one applies logical principles, after much inquiry and analysis, to solve problems with a high degree of innovation, divergent thinking and risk taking. Those mastering this outcome show evidence of integrating knowledge and applying this knowledge across disciplinary boundaries. Depth and breadth of understanding of disciplines is essential to this outcome. At the graduate level, originality in the application of knowledge (master's) and undertaking of research (doctoral) is expected.

In addition, Critical and Creative Thinking includes, but is not limited to, the following outcomes: Independent Inquiry and Analysis; Problem Solving; Creativity; and Depth and Breadth of Understanding.

Literacy

Literacy is the ability to extract information from a variety of resources, assess the quality and validity of the material, and use it to discover new knowledge. The comfort in using quantitative literacy also exists in this definition, as does using technology effectively and developing visual literacy.

In addition, Literacy includes, but is not limited to, the following outcomes: Information Literacy, Quantitative Literacy, Technological Literacy, and Visual Literacy.

Global Understanding

Global understanding encompasses the knowledge of cultural similarities and differences, the context (historical, geographical, political and environmental) from which these arise, and how they are manifest in modern society. Global understanding is exercised as civic engagement, intercultural competence and the ability to understand an academic discipline outside of the domestic context.

In addition, Global Understanding includes, but is not limited to, the following outcomes: Global Understanding, Sense of Historical Development, Civic Knowledge and Engagement, and Intercultural Competence.

Communication

Communication is the ability to interact effectively with a variety of individuals and groups, and convey information successfully in a variety of formats including oral and written communication. Communication also comprises attentiveness and listening, as well as reading comprehension. It includes the ability to communicate and synthesize information, arguments, and analyses accurately and reliably.

In addition, Communication includes, but is not limited to, the following outcomes: Oral Communication, Written Communication, Reading Comprehension, and Integrative Communication.

Professional and Ethical Behaviour

Professional and ethical behaviour requires the ability to accomplish the tasks at hand with proficient skills in teamwork and leadership, while remembering ethical reasoning behind all decisions. The ability for organizational and time management skills is essential in bringing together all aspects of managing self and others. Academic integrity is central to mastery in this outcome. At the graduate level, intellectual independence is needed for professional and academic development and engagement.

In addition, Professional and Ethical Behaviour includes, but is not limited to, the following outcomes: Teamwork, Ethical Reasoning, Leadership, Personal Organization and Time Management, and Intellectual Independence.

Table of Contents

Cybersecurity and Threat Intelligence

The Master of Cybersecurity and Threat Intelligence (MCTI) is offered by the School of Computer Science.

This professionally oriented 12-month masters is unique in its core focus on threat intelligence, Security Incident and Event Management (SIEM), intrusion prevention, malware analysis, penetration testing, and computer forensics, and in its integration of experiential lab-based learning. It covers the most challenging and technical aspects of the cybersecurity field and ensures that graduates are equipped with the professional capabilities to respond ethically and with a global social awareness of the implications of their work. Students gain hands-on experience with real and simulated security attacks such that graduates are primed to help organizations create security frameworks, protect sensitive data from threats, and analyse violations to help prevent future breaches.

Administrative Staff

Director
Ali Dehghantanha (3326 Reynolds, Ext. 52999)
adehghan@uoguelph.ca

Graduate Program Coordinator
Joe Sawada (2226 Reynolds, Ext. 53277)
graddir@socs.uoguelph.ca

Graduate Program Assistant
Jennifer Hughes (1116 Reynolds, Ext. 56402)
gradassist@socs.uoguelph.ca

Graduate Faculty

Luiza Antoine
BSc Politehnica (Romania), MSc Alberta, PhD Alberta - Assistant Professor

David A. Calvert
BA, MSc Guelph, PhD Waterloo - Associate Professor

David K.Y. Chiu
BA Waterloo, BSc Guelph, MSc Queen's, PhD Waterloo - Professor

Rozita Dara
BSc Shahid Teheshti, MSc Guelph, PhD Waterloo - Assistant Professor

Ali Dehghantanha
BSc Mashhad, MSc, PhD Putra Malaysia - Assistant Professor

Dan Gillis
BSc, MSc, PhD Guelph - Associate Professor

Gary Gréwal
BSc Brock, MSc, PhD Guelph - Associate Professor

Stefan C. Kremer
BSc Guelph, PhD Alberta - Professor

Xiaodong Lin
BASc Nanjing, MSc East China Normal, PhD Beijing, PhD Waterloo - Associate Professor

Pascal Matsakis
BSc, MSc, PhD Paul Sabatier (France) - Professor

Charlie F. Obimbo
MSc Kiev, PhD New Brunswick - Associate Professor

Stacey Scott
BSc Dalhousie, PhD Calgary - Associate Professor

Fei Song
BSc Jilin (China), MSc Academia Sinica (China), PhD Waterloo - Associate Professor

Deborah A. Stacey
BSc Guelph, MASc, PhD Waterloo - Associate Professor

Fangju Wang
BE Changsha, MSc Peking, PhD Waterloo - Professor

Mark Wineberg
BSc Toronto, MSc, PhD Carleton - Associate Professor

Yang Xiang
BSs, MSc BUAA (Beijing), PhD UBC - Professor

Associated Graduate Faculty

Ritu Chaturvedi
PhD Windsor - Contractually Limited Faculty, School of Computer Science

Hassan Khan
BSc, MSc USC, PhD Waterloo - Contractually Limited Faculty, School of Computer Science

Denis Nikitenko
BSc Ryerson, MSc, PhD Guelph - Contractually Limited Faculty, School of Computer Science

MCTI Program

The Master of Cybersecurity and Threat Intelligence is a terminal masters degree focused on training individuals to become technically skilled and ethically-minded cybersecurity professionals. Students develop mastery in security analysis and design, security architecture, threat intelligence, digital forensics, and penetration testing. Hands-on training in the cybersecurity teaching lab, the Security Operations Centre, enables students to work with real and simulated security attacks independently and collaboratively. The program culminates in an independent project wherein students partner with an industry or academic partner to produce an evidence-based solution to a complex cybersecurity problem.

Admission Requirements

Admission to the Master of Cybersecurity and Threat Intelligence program may be granted on the School of Computer Science's recommendation to:

i. Applicants who have successfully completed an undergraduate degree/baccalaureate in an honours program or the equivalent (having achieved a grade average of at least 75%, B, in the last four semesters of study) in computer science, computer engineering, or a related subject area (or hold a minor in one of these areas) from a recognized university; and

ii. Applicants who have relevant experience or background knowledge of Data Communication and Networking (such as a course equivalent to CIS*3210 Computer Networks) and Computer Programming (such as a course equivalent to CIS*2500 Intermediate Programming).

Successful applicants must also meet the University of Guelph's English Proficiency requirements for admission. If an applicant's first language is not English, an English Language Proficiency test will be required during the application phase.

All applications will be reviewed by the cybersecurity admissions committee. Students are admitted for a September start date. The School of Computer Science office should be consulted for admission deadlines.

Program Requirements

Students in the Master of Cybersecurity and Threat Intelligence program are required to complete a minimum of 4.00 graduate credits, including the following required courses:

CIS*6510	[0.50]	Cybersecurity and Defense in Depth
CIS*6520	[0.50]	Advanced Digital Forensics and Incident Response
CIS*6530	[0.50]	Cyber Threat Intelligence and Adversarial Risk Analysis
CIS*6540	[0.50]	Advanced Penetration Testing and Exploit Development
CIS*6550	[0.50]	Privacy, Compliance, and Human Aspects of Cybersecurity
CIS*6560	[1.00]	Cybersecurity and Threat Intelligence Project

Students can select from the following list of electives to fulfill the remaining 0.50 graduate credit:

CIS*6570	[0.50]	Advanced Cryptography and Cryptanalysis
CIS*6580	[0.50]	Security Monitoring and Cyber Threat Hunting

Students may also take up to one graduate level course in the related areas of Artificial Intelligence or Data Science to fulfill their elective requirement.

Courses

CIS*6510 Cybersecurity and Defense in Depth F [0.50]

This course provides an overview of concepts and technical measures that are employed to enforce security policies and protect networks and systems from malicious activities. Students will learn how to engineer a secure system and how to secure networks in an ethical manner.

Restriction(s): Student registered in the MCTI program.
Department(s): School of Computer Science

CIS*6520 Advanced Digital Forensics and Incident Response F [0.50]

This course provides an in-depth understanding of theoretical concepts and practical issues in the field of digital forensics and incident response. Students will develop necessary skills, methodologies, and processes to detect cyber incidents and conduct in-depth computer and network investigation.

Restriction(s): Student registered in the MCTI program.
Department(s): School of Computer Science

CIS*6530 Cyber Threat Intelligence and Adversarial Risk Analysis W [0.50]

This course provides an in-depth understanding of techniques for detecting, responding to, and defeating Advanced Persistent Threats (APT) and malware campaigns using artificial intelligence and data mining techniques. Students will identify, extract, and leverage intelligence from different types of cyber threat actors.

Restriction(s): Student registered in the MCTI program.
Department(s): School of Computer Science

CIS*6540 Advanced Penetration Testing and Exploit Development W [0.50]

This course provides an in-depth understanding of techniques for detecting, responding to, and defeating Advanced Persistent Threats (APT) and malware campaigns using artificial intelligence and data mining techniques. Students will identify, extract, and leverage intelligence from different types of cyber threat actors.

Restriction(s): Student registered in the MCTI program.
Department(s): School of Computer Science

CIS*6550 Privacy, Compliance, and Human Aspects of Cybersecurity U [0.50]

This course provides an in-depth view of the privacy, regulatory, and ethical issues surrounding cybersecurity. It covers methods of mitigating/treating privacy risks associated with emerging technologies that collect, manage, and analyse data. This course also examines data protection regulations and compliance strategies.

Department(s): School of Computer Science

CIS*6560 Cybersecurity and Threat Intelligence Project W-S [1.00]

Students plan, develop, and write an industry- or faculty-led report and produce required tools, services, and software. Projects should advance knowledge or practice, and address an emerging challenge in cybersecurity, cyber threat intelligence, digital forensics and incident response, cyber threat hunting, or a closely related field.

Restriction(s): Student registered in the MCTI program.
Department(s): School of Computer Science

CIS*6570 Advanced Cryptography and Cryptanalysis U [0.50]

This course provides an in-depth understanding of modern cryptography, with emphasis on practical applications. Topics covered include classical systems, information theory, symmetrical cryptosystems, block ciphers, stream ciphers, DES, AES, asymmetric cryptosystems, ECC, provable security, keyexchange and management, and authentication and digital signatures, among others.

Department(s): School of Computer Science

CIS*6580 Security Monitoring and Cyber Threat Hunting U [0.50]

This course provides a comprehensive review of tools, techniques, and procedures for monitoring network events and assets to build a secure network architecture. It trains students in methods for hunting attackers that could bypass designed network defense mechanisms in an enterprise.

Restriction(s): Student registered in the MCTI program.
Department(s): School of Computer Science