UNIVERSITY OF THE COMMONWEALTH CARIBBEAN

A Member of the Commonwealth & OAS Consortia of Universities

MSc in Cyber Security and Data Privacy Protection

PROGRAMME INFORMATION SHEET

PROGRAMME OVERVIEW

Master of Science in Cyber Security and Data Privacy Protection programme is a rigorous and comprehensive programme designed to provide students with the skills and knowledge to protect sensitive data and information from cyber threats. Modern civilisation depends highly on computer software, which creates the need for a tremendous and formidable level of cyber security and data protection. This programme will deliver practical knowledge, develop technical and problem-solving skills, and offer intellectual experience in various aspects such as cyber security, privacy, and trust.

Additionally, students will learn how to:

- Evaluate and address privacy issues, privacy threats and vulnerabilities.
- Mitigate privacy and security threats by integrating and applying knowledge to solve real problems.
- Design, research, and implement robust cyber security measures.

PROGRAMME STRUCTURE

The MSc. in Cyber Security and Data Privacy Protection programme typically takes twenty (20) months to complete, with 42 credits. The programme comprises core courses, and a thesis or capstone project. Core courses cover topics such as:

	Course Description	MScDPPC	# Weeks per Course	Credits Hours
1	**Compulsory**	MSC507 Information Systems Security Professional	5	3
2	**Compulsory**	MSC508 Cyber Security Planning and Risk Analysis	5	3
3	**Compulsory**	MSC509 Cyber Security Ethical and Legal Concerns	5	3
4	**Compulsory**	MSC510 Advanced Privacy and Data Protection	5	3
5	**Compulsory**	MSC511 Mobile Computing and Wireless	5	3
6	**Compulsory**	MSC512 Ethical Hacking and Countermeasures	5	3
7	**Compulsory**	MSC513 Malware Analysis and Defense	5	3
8	**Compulsory**	MSC607 Advanced Offensive Cyber Security	5	3
9	**Compulsory**	MSC608 Advances in Management of Cyber Security	5	3
10	**Compulsory**	MSC609 Disaster Recovery	5	3
11	**Compulsory**	MSC610 Cybercrime and Digital Forensics	5	3
12	**Compulsory**	MSC611 Blockchain Technology	5	3
13	**Compulsory**	MSC612 Cyber Security Capstone 1	5	3
14	**Compulsory**	MSC613 Cyber Security Capstone 2	5	3
				TOTAL 42 CREDITS

DURATION
20 months

CLASS STRUCTURE:
8 cycles and each cycle = 5 weeks
Venue: Worthington Avenue Campus (WAC) and Online

CAREER OPPORTINUITES

Graduates of the MSc. in Cyber Security and Data Privacy Protection programme are well-equipped to pursue careers in a variety of roles, such as:

- Security Administrator
- Cyber Risk Analyst
- Cryptographer
- Security Auditor
- Secure Software Developer
- Penetration Tester
- Ethical Hacker
- Information Security Analyst
- Cybersecurity Consultant
- Data Privacy Officer
- Risk Manager
- Network Security Engineer

SALARY EXPECTATIONS

The salary for graduates of the MSc. in Cyber Security and Data Privacy Protection programme varies depending on the job position, company, and location. On average, graduates can earn between $3,537,206 to 4,597,935 annually.

WHY CHOOSE THIS PROGRAMME?

Data is an important asset in any organisation and is constantly at risk of being breached. The MSc. in Cyber Security and Data Privacy Protection programme provides students with the necessary skills and knowledge to excel in a fast-growing industry. The programme is designed to keep up with the ever-evolving cybersecurity landscape, ensuring graduates are prepared to tackle emerging threats. Additionally, the programme's focus on data privacy and cybersecurity gives students a well-rounded education, making them highly competitive in the job market.

ADMISSION REQUIREMENTS:

In general, admission to the MSc programme requires the following:

- An earned Baccalaureate Degree in BSc. in Information Technology, Computer Science or any related field from a recognised or/and accredited institution.
- A minimum of three years' working experience.
- Fluent in English language at the postgraduate studies level.
- Certain prerequisite courses may be required to be taken at the UCC (where necessary).

In addition to the above requirements, applicants will need to submit the following documents:

- Official transcripts from all post-secondary institutions attended.
- A resume or CV detailing work experience, relevant coursework, and any relevant certifications.
- Two letters of recommendation from professionals who can attest to the applicant's academic and professional abilities.
- A statement of purpose outlining the applicant's motivation for pursuing the MSc in Cyber Security and Data Privacy Protection career goals, and any relevant experience or skills.

Program Name	AS	Course Number	Course Name	Course Description	Course Length (in weeks)	Course Credit Hours
MSc in Cybersecurity and Data Privacy Protection	1	MSC507	Information Systems Security Professional	This course covers information systems security, including access control, application security, business continuity, cryptography, risk management, legal issues, physical security, telecommunications and network security. This course prepares for the CISSP certification exam and is ideal as a bridge for non technical degree holders into the MS in Cybersecurity and Data Privacy Protection.	5	3
	2	MSC508	Cyber Security Planning and Risk Analysis	In this course students will study the concepts in cyber security design and implementation for computer systems (both hardware and software). Security architecture, organization policies, standards, procedures, and security system implementation, including diagnostic testing of databases and networks. Throughout this course, practical skills will also be acquired through a series of interactive risk assessment workshops and case studies.	5	3
	3	MSC509	Cyber Security Ethical and Legal Concerns	In this course students study Cybersecurity law, policy and compliance, legal rights and liabilities associated with computer security; the application of ethical principles (respect for persons, beneficence, and justice) in cyber security; Information privacy; Rights enforceable by private parties; Liabilities associated by private parties and governments; Legal aspects of records management; Un-authorized computer use; Computer Fraud and Abuse Act; Trade Secrets; Economic Espionage Act; Civil Law Claims; Privacy; Export Control; Constitutional Rights; USA-PATRIOT Act; HIPAA, Gramm-LeachBliley; Digital Rights Management.	5	3
	4	MSC510	Advanced Privacy and Data Protection	This course is tailored for students who already possess a foundational knowledge of privacy and data protection and are seeking to deepen their expertise in this vital area. It is particularly beneficial for legal professionals, privacy officers, compliance experts, and those aspiring to specialize in privacy and data protection. By covering advanced topics such as international and regional privacy frameworks, data protection principles, data subject rights, data impact assessments, and enforcement mechanisms, the course aims to prepare students to navigate and address the complex challenges of privacy and data protection in today's digital age.	5	3
	5	MSC511	Mobile Computing and Wireless	In this course students will study theconcepts in nomadic computing and mobility; challenges in design and deployment of wireless and ad-hoc networks; MAC issues, routing protocols and mobility management for ad-hoc networks and networks of the future.	5	3
	6	MSC512	Ethical Hacking and Counter Measures	This course is designed for students to be trained in understanding vulnerabilities in networks, operating systems, database management systems and web servers. Students will learn how exploits are designed by an adversary attacker to penetrate into vulnerable systems. Students will also learn how the hacker can move into a compromised system and remove her/his footprints. The course will introduce students to tools used for network scanning, finger printing, and password cracking. Tools include Nmap, Nessus and Backtrack.	5	3
	7	MSC513	Malware Analysis and Defense	In this course students will study malicious software detection and defenses including tripwire, Bit9, and other techniques such as signature and hash algorithms. Viruses, worms, Trojan horses, logic bombs, malicious web server scripts, mobile code issues, and methodologies used by anti-virus/spyware vendors will be studied.	5	3
	8	MSC607	Advanced Offensive Cyber Security	This course is designed for students to be trained in Advanced Offensive Security tactics and techniques. This includes the full hacking lifecycle from enumeration/vulnerability discovery, to exploitation, followed by post exploitation activities. Students will learn how to strategically enumerate network devices and exploit various resources, fuzz applications and network protocols to identify bugs/vulnerabilities, execute advanced Man-in-the-Middle attacks, along with conducting post exploitation activities on both Linux and Windows machines. Additionally, students will be introduced to Python - including Python fundamentals and development of custom tools/exploits, along with PowerShell usage from a penetration testers perspective. Lastly, students will be introduced to Splunk to provide a better understanding of the network traffic generated as result of our activities, along with how security teams can identify/alert/investigate all resulting traffic.	5	3
	9	MSC608	Advances in Management of Cyber Security	This course is designed for the graduate level cyber security and business student who wants to deepen the knowledge of the management aspects of cyber security. This course takes a "view from the top" and presents exactly what future managers need to know about cyber security. Harvard Business cyber cases and a cyberattack simulation are used in this course.	5	3

Program Name	AS	Course Number	Course Name	Course Description	Course Length (in weeks)	Course Credit Hours
	10	MSC609	Disaster Recovery	In this course students will learn how to identify cyber security vulnerabilities and implement appropriate countermeasures to mitigate risks. Techniques will be taught for creating a continuity plan and methodology for building an infrastructure that supports its effective implementation. Throughout this course, skills in disaster recovery planning will be acquired through a series of interactive workshops and case studies. Students will design and develop a disaster recovery plan.	5	3
	11	MSC610	Cybercrime and Digital Forensics	The topics covered in this course include cyber-crime investigation, digital forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anti-forensics techniques, anonymity and pseudonymity, cyber law, computer security policies and guidelines, court report writing and presentations, and case studies. The course will include lecture and demonstrations and is designed around a virtual lab environment that provides for robust and realistic hands-on experience in working with a range of information assurance topics. Students will be assigned projects to apply information security practices and technologies to solve real-world cyber security problems.	5	3
	12	MSC611	Blockchain Technology	Students will learn what blockchain is and how it works, from a business as well as technical standpoint. They will gain insight into how blockchain will affect the future of industry / organizations. Upon course completion students will have knowledge of the following: what is blockchain and the real world problems that blockchain can solve; how blockchain works and the underlying technology of transactions, blocks, proof-of-work, and consensus building; how blockchain exists in the public domain (decentralized, distributed) yet maintain transparency, privacy, anonymity, security, and history; recognize how blockchain is incentivized without any central controlling or trusted agency; platforms such as Ethereum to build applications on blockchain; how cryptocurrency works and why people value a 'digital' currency; and how to design and implement blockchain for applications in the financial services, manufacturing, and retail industries.	5	3
	13	MSC612	Cyber Security Capstone I	This course is the capstone experience for graduate students in the Master's degree in Cyber Security and provides students with the opportunity to carry out in depth research on a specific topic in cyber security. The student's project will reflect the integration and application of the cyber security knowledge gained over the course of the program.	5	3
	14	MSC613	Cyber Security Capstone II		5	3

UNIVERSITY OF THE COMMONWEALTH CARIBBEAN
Fostering Leadership & Innovation

SCHOOL OF MATHEMATICS SCIENCE & TECHNOLOGY
Department of Information Technology

MSc in Cyber Security & Data Privacy Protection

PRE-REQUISITE COURSES FOR MATRICULATION

REQUIRED COURSE #1: CERTIFIED IN CYBERSECURITY

OVERVIEW

The ISC2 Certified in Cybersecurity (CC) certification will demonstrate to employers that you have foundational knowledge of industry terminology, network security, security operations and policies and procedures that are necessary for an entry- or junior-level cybersecurity role. It will signal your understanding of fundamental security best practices, policies and procedures, as well as your willingness and ability to learn more and grow on the job.

Complete the ISC2 Certified in Cybersecurity Certification Course

1. Click here to navigate to the ISC2 website.
2. Select **Get Started**, then **Become an ISC2 Candidate**.
3. **Sign Up** for an isc2.org account (or **Sign In** if you already have one).
4. Select **Get Certified** then **CC Entry-Level Cybersecurity**.
5. Next, select **Free Exam and Training**.
6. Click **Get Started** to begin the course.

Cost: Free

Duration: 14 hours

Deliverable:

- Certificate of Completion: ISC2 Certified in Cybersecurity

  How to Download:

  1. Click here to navigate to the ISC2 Online Learning platform.
  2. Go to the Awards menu then select the Certificates filter on the right.
  3. Download and save your certificate as PDF.

Additional Information:

- ISC2 stands for the International Information Systems Security Certification Consortium
- Certification exam is FREE, and exam voucher becomes available upon completion of the course.
- Certification requires an annual maintenance fee of US$50.00

REQUIRED COURSE #2: ENDPOINT SECURITY

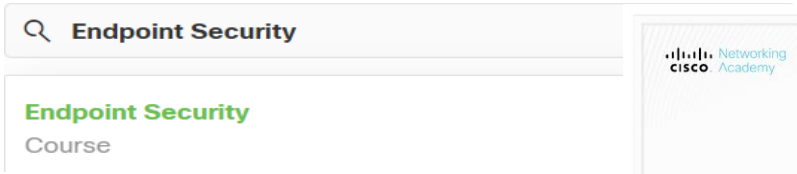
OVERVIEW

Each day billions of devices are connected to the network, and each one needs to be protected. Build the skills to secure your network all the way to the edge, including hardware, software, and media.

In this course, you will learn how to assess the network, operating systems, and endpoints for vulnerabilities, and how to secure the network. You will also gain skills to maintain the integrity, confidentiality, and availability in your network and your data.

Complete the Endpoint Security Course

1. Click here to navigate to the CISCO Networking Academy website.
2. Click the **Login** button then **Sign Up** for a netacad.com account (or **Sign In** if you already have one).
3. Enter Endpoint Security in the **Search** bar.
4. Select the Endpoint Security **Course** from the search results (see screenshot below).



Cost: Free

Duration: 27 hours

Deliverable:

- Certificate of Completion: Endpoint Security

  How to Download:

  1. Go to your Networking Academy Learner Profile
  2. Select Badges & Certificates then the Endpoint Security certificate
  3. View and download your certificate

REQUIRED COURSE #3: DATA GOVERNANCE FUNDAMENTALS

OVERVIEW

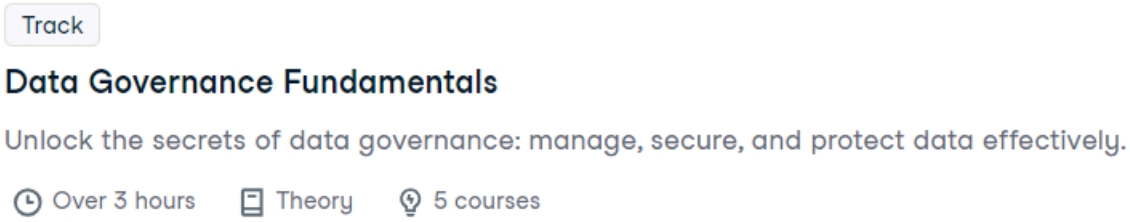
The Data Governance Fundamentals track enables you to unlock the secrets of data governance: manage, secure, and protect data effectively through the acquisition of the following competencies:

- Gain a clear understanding of data privacy principles and how to implement privacy and security processes.
- Explore the basics of data quality management. Learn the key concepts, dimensions, and techniques for monitoring and improving data quality.
- Discover how to become a data defender and keep data safe and secure with this beginner-friendly interactive course.

- Gain an introduction to data governance, exploring its meaning, purpose, and how to implement a data governance framework.
- Master the key concepts of data management, from life cycle stages to security and governance.

Complete the Data Governance Fundamentals Track

1. Click here to navigate to the DataCamp website.
2. **Sign Up** for a datacamp.com account (or **Sign In** if you already have one).
3. Enter Data Governance Fundamentals in the **Search** bar.
4. Select the Data Governance Fundamentals **Track** from the search results (see screenshot below).



5. Select **Start Track**.

Cost: US$29.00 per month [Premium Subscription]
- Requires a month's subscription to complete the track.
- You have the option to cancel your subscription after completing the track.

Duration: 10 hours

Deliverable:
- Certificate of Completion: Data Governance Fundamentals

  How to Download:
  1. Go to My Library
  2. Scroll down to Completed
  3. Download your certificate

Give yourself a double thumbs up!

You are now ready for the MSc in Cybersecurity & Data Privacy Protection!

Please note that the information contained herein is accurate at the time of printing but is subject to amendment at any time.

For further information please contact:

Graduate Recruitment/Director, Administration & Student Services/Programme Coordinator
The College of Graduate Studies and Research, UCC
Tel: (876)906-3000 (Ask for extensions 3991/4002/4006/4027/4049)
Email: graduaterecruitment@ucc.edu.jm

UNIVERSITY OF THE COMMONWEALTH CARIBBEAN (UCC)
Fostering Leadership & Innovation