



**TIIS**  
THE INSTITUTE  
OF INTERNATIONAL  
STUDIES



# Master of Cyber Security

**CRICOS CODE: 115211M**

**[tiis.edu.au](https://tiis.edu.au)**



# Table Of Content

<b>Key Information</b>	<b>03</b>
<b>Course Overview</b>	<b>03</b>
<b>Course Information</b>	<b>03</b>
<b>Course Structure</b>	<b>04</b>
<b>Additional Course Information</b>	<b>06</b>
<b>Compulsory Student Checks</b>	<b>06</b>
<b>Study Load</b>	<b>06</b>
<b>Participation Requirements</b>	<b>07</b>
<b>Admissions</b>	<b>07</b>
Academic	
English Language Requirements	
Technology Requirements	
<b>Credit for Prior Learning</b>	<b>08</b>
<b>Entry and Alternate Exits</b>	<b>09</b>
<b>Careers</b>	<b>09</b>
Graduate Employment Outcomes	
Professional Recognition	
<b>Course Learning Outcomes</b>	<b>09</b>
<b>Graduate Attributes</b>	<b>10</b>
<b>Course Delivery</b>	<b>10</b>
<b>Contact Information</b>	<b>10</b>

# Key Information

🕒 Course Duration: 2 years full time (4 years part time)<sup>12</sup>

📍 Location: On campus - Sydney, Melbourne

📅 Intakes: March, July, November

The Institute of International Studies' (TIIS) **Master of Cyber Security (MCS)** equips you with specialised knowledge and skills to design, develop and manage cyber security systems. It develops your knowledge to mitigate the risks of cyber security threats and respond to cyber security events. TIIS' Master of Cyber Security develops your technical as well as management and business knowledge and skills in Cyber Security resulting in a broader set of skills with which to enter the industry. If you have experience in particular industries or aspire to enter a particular industry, the course assessments allow you to use these industries as contexts to learn and apply MCS knowledge and skills in the cyber security settings.

## Course Information

Award granted: Master of Cyber Security

Course Code: MCS

CRICOS Code: 115211M

AQF Level: Master (level 9)

Accreditation(s): TEQSA



<sup>1</sup> If you receive credit for sections 1 or 2 (see course structure) your course duration may reduce by up to one trimester full time or two trimesters part time.

<sup>2</sup> Part time option is only available to domestic students.

# Course Structure

The **Master of Cyber Security** requires the completion of 16 subjects (96 credit points). Each subject is worth 6 credit points.

The course has five sections.

**Section 1:** Foundation Information Technology (4 subjects)

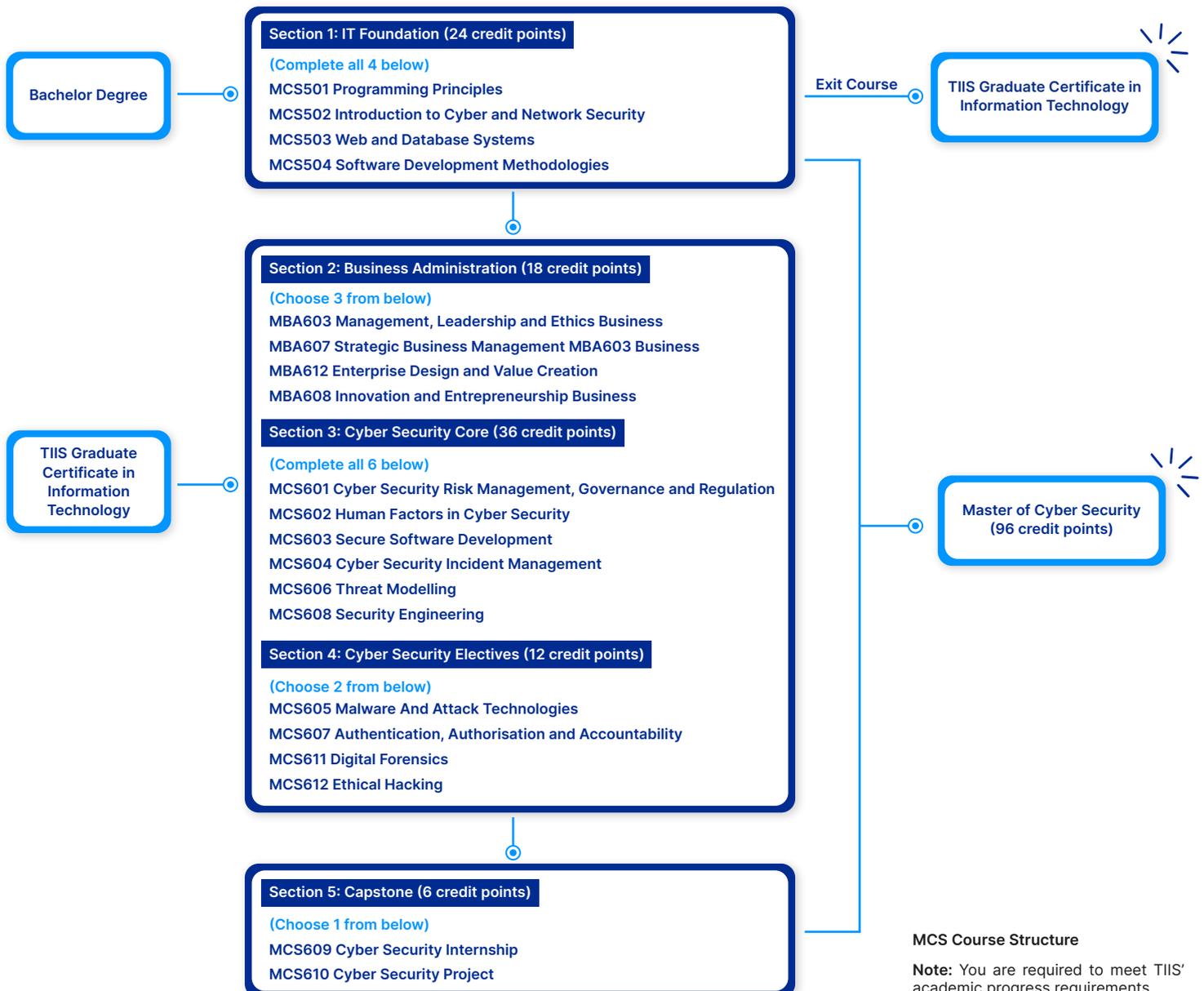
**Section 2:** Business Administration (3 subjects)

**Section 3:** Core Cyber Security (6 subjects)

**Section 4:** Cyber Security Electives (2 subjects)

**Section 5:** Capstone (1 subject)

Depending on the students' prior academic qualifications they may apply for credit for Section 1 or Section 2. If they receive credit for sections 1 or 2, their course duration may reduce by up to one trimester full time or two trimesters part time.



Subject Code	Subject Title	Prerequisites	Subject Area	Subject Level	Subject Type
MCS501	Programming Principles		Information Technology	Foundation	Compulsory
MCS502	Introduction to Cyber and Network Security		Information Technology	Foundation	Compulsory
MCS503	Web and Database Systems		Information Technology	Foundation	Compulsory
MCS504	Software Development Methodologies	MCS501 (co-requisite)	Information Technology	Foundation	Compulsory
MCS601	Cyber Security Risk Management, Governance and Regulation		Cyber Security	Introductory	Compulsory
MCS602	Human Factors in Cyber Security		Cyber Security	Introductory	Compulsory
MBA603	Management, Leadership and Ethics		Business Administration	Introductory	Restricted Elective
MBA608	Innovation and Entrepreneurship		Business Administration	Introductory	Restricted Elective
MCS604	Cyber Security Incident Management	MCS601	Cyber Security	Intermediate	Compulsory
MCS605	Malware and Attack Technologies	MCS603	Cyber Security	Intermediate	Restricted Elective
MBA607	Strategic Business Management	MBA603	Business Administration	Intermediate	Restricted Elective
MBA612	Enterprise Design and Value Creation	MBA608	Business Administration	Intermediate	Restricted Elective
MCS603	Secure Software Development	MCS501 MCS504	Cyber Security	Advanced	Compulsory
MCS606	Threat Modelling	IT foundation subjects MCS601	Cyber Security	Advanced	Compulsory
MCS607	Authentication, Authorisation and Accountability	IT foundation subjects MCS601	Cyber Security	Advanced	Restricted Elective
MCS608	Security Engineering	IT foundation subjects MCS601	Cyber Security	Advanced	Compulsory
MCS611	Digital Forensics	IT foundation subjects MCS 601 and MCS 604	Cyber Security	Advanced	Restricted Elective
MCS612	Ethical Hacking	IT foundation subjects MCS 601 and MCS 603	Cyber Security	Advanced	Restricted Elective

Subject Code	Subject Title	Prerequisites	Subject Area	Subject Level	Subject Type
MCS609	Cyber Security Internship	Last trimester of studies Average 70% cumulative subject mark. Pre-placement activities completed. No convicted cases of academic cheating <sup>3</sup>	Cyber Security	Capstone	Restricted Elective
MCS610	Cyber Security Project	Industry based projects will have the same restrictions as MCS609	Cyber Security	Capstone	Restricted Elective

<sup>3</sup> See Student Academic Integrity and Honesty Policy

## Additional Course Information

Course duration may vary depending on Credit for Prior Learning (CPL) received and enrolment patterns. Students on a student visa are expected to complete within their Confirmation of Enrolment (COE) end date and must enrol accordingly.

## Compulsory Student Checks

Subjects which include work integrated learning or site visits or any form of interaction with the public may require you to obtain a police check and/or working with children check.

## Study Load

It is expected that each subject has three hours of contact time per week with an additional seven hours of selfdirected learning per week. There is an expected additional ten hours per subject expected for completing the final assessment.



# Participation Requirements

The capstone requirement includes an option for an internship. Successful application will require some attendance on site at the organisation's premises.

TIIS supports students who are less able with reasonable adjustments to participation and assessment. See Student Handbook, 'Reasonable Adjustment' for more details.

## Admissions

### Academic

Academic entry requirements are as determined by the Student Selection and Admissions Policy.

Depending on your past qualifications, you may apply for Credit for Prior Learning (CPL) in line with TIIS' Credit for Prior Learning Policy and complete the course in a shorter duration.

#### **1 year 8 months full time (or part time equivalent) – 72 credit points**

To be admitted into the MCS with 24 credit points of CPL you must satisfy the following criteria:

- completion of a bachelor degree (AQF 7) or higher from a recognised institution (or equivalent) in a related field.<sup>4</sup>

CPL will apply to the four foundation information technology subjects.

#### **1 year 8 months full time (or part time equivalent) – 78 credit points**

To be admitted into the MCS with 18 credit points of CPL you must satisfy the following criteria:

- completion of a bachelor degree (AQF 7) or higher from a recognised institution (or equivalent) in a management related field.

CPL will apply to the three business administration subjects

#### **2 years full time (or part time equivalent) – 96 credit points**

To be admitted into the MCS without any CPL<sup>5</sup> you must satisfy the following criteria:

- completion of a bachelor degree (AQF 7) or higher from a recognised institution (or equivalent) in any field.

You may also be considered for alternative admission arrangements as per Section 5 of the Student Selection and Admissions Policy

<sup>4</sup> Related field/s: Information Technology, Information Systems, Computer Science or Engineering.

<sup>5</sup> CPL may still be considered on a case by case basis

## English Language Requirements

English language requirements are as determined by the Student Selection and Admissions Policy. To be admitted to the MCS, you must satisfy one of the following criteria:

- a) achievement of an IELTS average score of 6.5 or above with no band below 6.0 or equivalent
- b) completion of a recognised ELICOS provider certificate that clearly indicates equivalence to the IELTS score
- c) completion of a bachelor course with English as the medium of instruction within the past 2 years
- d) studied and/or worked in an English-speaking environment of a country where English is the primary language for communication, for more than 5 continuous years

## Technology Requirements

While not an entry requirement, it is expected that you have access to high-speed internet and a modern computer. This is to accommodate the higher-than-normal bandwidth and processing requirements in certain subjects. As a minimum, you should have access to computers that:

- have at least **16GB** of RAM though 32GB is ideal
- has **256GB** of hard disk space available, though 512 is ideal
- a minimum of **8 cores** though 16 is ideal
- **1920 x 1080** screen resolution

### Note:

- all software required for the course will be either free to download or be provided by TIIS.
- some software required for the course can only be accessed on a Windows platform. Students with MacBooks can install virtualisation software to run Windows only software.

## Credit for Prior Learning

Granting of credit for prior learning (CPL) ensures that you commence study both at a level that appropriately recognises your prior learning experiences and are not required to repeat equivalent learning successfully undertaken in another context. TIIS is committed to developing open and accessible guidelines to granting CPL towards a course of study based on prior learning, whether from formal studies or professional work experience. See CPL Policy for more details.

Depending on your past academic qualifications you may apply for CPL for Section 1 or Section 2 (see Course Structure) of the course. This may reduce your course duration, depending on your enrolment pattern, by up to two trimesters.

# Entry and Alternate Exits

You may also enter the MCS by completing TIIS' Graduate Certificate in Information Technology (GCIT). You will be credited the four foundation information technology subjects into the MCS.

## Alternate Exit

Upon completing the four foundation IT subjects you may exit early with a Graduate Certificate in Information Technology (GCIT).

# Careers

## Graduate Employment Outcomes

On completion of the MCS, you can pursue careers in the following roles:

- Cyber Threat Analyst
- Intrusion Analyst
- Malware Analyst
- Incident Responder
- Cyber Operations Coordinator
- Penetration Tester
- Vulnerability Assessor
- Cyber Security Adviser/Assessor
- Vulnerability Researcher

Graduates may need to obtain further certification and/or experience to enter directly into these roles.

## Professional Recognition

To be included once ACS accreditation is secured.

# Course Learning Outcomes<sup>6</sup>

<b>CLO 1</b>	Apply foundation, core, and advanced knowledge in cyber security to design, develop, implement, and manage secure systems and processes that are of industry standard, and responsive to the evolving cyber security environment.
<b>CLO 2</b>	Examine the cyber security body of knowledge and critically evaluate practices to inform the design and development of technical and creative solutions to cyber security challenges that align with the overall strategies of the organisation.

<b>CLO 3</b>	Critically evaluate the impacts of ethical and regulatory cyber security issues, from personal, domestic, and global perspectives, and assess the implications for cyber security governance and risk from a technical and organisational perspective.
<b>CLO 4</b>	Work independently, collaboratively, and reflectively to develop technical and creative solutions to cyber security challenges.
<b>CLO 5</b>	Communicate with and effectively manage a wide range of stakeholders, internal and external, both technical and non-technical, to design, develop, implement, and manage solutions to cyber security challenges.
<b>CLO 6</b>	Develop professional practice in cyber security through a synthesis of knowledge and skills and innovatively apply and evaluate knowledge and skills in an independent or collaborative evidencebased industry relevant project or an internship.

<sup>6</sup> Approved by the Academic Board on 01 December 2022

## Graduate Attributes

On the completion of your course, you will be:

- knowledgeable and skilled in your profession
- effective communicators and work well as members of a team
- ethical and socially responsible in your practice
- cross-culturally aware and global in perspective
- innovative and creative in your judgement
- reflective, self-aware, and self-managed professionals

## Course Delivery

TIIS will deliver the course on campus only. Teaching will occur in the physical classroom in three-hour slots.

## Contact Information

Our friendly staff are available to speak with you one on one. Use one of the options below:

**Email:** [info@tiis.edu.au](mailto:info@tiis.edu.au)

**Phone:** 1300 164 600, +61 2 8098 0702