

## Overview

The Master of Cybersecurity is a postgraduate degree that provides you with the skills to manage and administer cybersecurity and blockchain and prepares you for careers as security systems analysts, systems designers, data communications specialists or security software engineers or administrators.

The Master of Cybersecurity is a postgraduate degree that provides you with the skills to manage and administer cybersecurity and blockchain and prepares you for careers as security systems analysts, systems designers, data communications specialists or security software engineers or administrators.

## Notes

You can enrich your degree by honing your academic and professional skills through the Monash Innovation Guarantee (MIG). The MIG is your unique opportunity to collaborate with renowned industry leaders and design innovative solutions that result in real social change. MIG will give you the leadership skills you will need to adapt and thrive in a rapidly changing world and is your chance to make connections before you graduate. The MIG unit may be credited in place of a free elective as a 6 credit point unit option. For information on eligibility please see [FREE](#).

## Mode and location

Collapse all

### On campus

keyboard\_arrow\_down

### Clayton

## Learning outcomes

These course outcomes are aligned with the [Australian Qualifications Framework and Monash Graduate Attributes](#).

Upon successful completion of this course it is expected that you will be able to:

Collapse all

### 1.

critically assess existing systems using the theories, techniques, and software tools that are available in the field of cybersecurity.

keyboard\_arrow\_down

**2.**

adapt new and emerging technologies in application development based on an understanding of the underpinning principles of cybersecurity.

keyboard\_arrow\_down

**3.**

analyse and document the core issues in building secure systems, evaluate the strengths, weaknesses and propose and articulate solutions effectively.

keyboard\_arrow\_down

**4.**

competently design secure systems at project and team levels.

keyboard\_arrow\_down

**5.**

review, synthesise, apply and evaluate existing systems and extend them with new technologies through either a significant research thesis component or research-grounded industrial project.

keyboard\_arrow\_down

**6.**

analyse issues and solutions in security and system design as they affect general and particular communities.

keyboard\_arrow\_down

**7.**

evaluate the implication of ethical issues and norms in privacy and security.

keyboard\_arrow\_down

### **Professional recognition**

This course is accredited by the Australian Computer Society (ACS) as meeting the standard of knowledge for professional-level membership.

### **Structure**

The course is structured in three parts: Part A. Foundation studies, Part B. Core studies, and Part C. Applied studies.

### **Part A. Foundation studies**

These studies will provide an orientation to the field of cybersecurity at graduate level. They are intended for students whose previous qualification is not in a cognate field.

### **Part B. Core studies**

These studies draw on best practices within the broad realm of IT security theory and practice. You will gain an understanding of cybersecurity, blockchain and IT project management principles. Your study will focus on your choice of units within cybersecurity.

### **Part C. Applied studies**

The focus of these studies is professional or scholarly work that can contribute to a portfolio of professional development. You have two options:

- a program of coursework involving advanced study and an industry experience studio project.
- a research pathway including a thesis. If you wish to use this master's course as a pathway to a higher degree by research you should take this option.

### **Master's entry points**

Depending on prior qualifications you may receive entry level credit which determines your point of entry to the course:

- If you are admitted at entry level 1 you complete 96 credit points, comprising Part A, Part B and Part C.
- If you are admitted at entry level 2 you complete 72 credit points, comprising Part B and Part C.

Note: If you are eligible for credit for prior studies you may elect not to receive the credit and complete the higher credit-point option.

### **Course progression map**

The [course progression map](#) provides guidance on unit enrolment for each semester of study.

**Requirements**  
**96 credit points**

Collapse all

**Part A. Foundation studies24 credit points**

keyboard\_arrow\_down

You must complete the following units

[FIT9132](#)

[6 CP](#)

[Introduction to databases](#)

[FIT9136](#)

[6 CP](#)

[Introduction to Python programming](#)

[FIT9137](#)

[6 CP](#)

[Introduction to computer architecture and networks](#)

[FIT9138](#)

[6 CP](#)

[Information systems analysis, design and systems thinking](#)

## **Part B. Core studies48 credit points**

keyboard\_arrow\_down

You must complete 48 credit points, comprising:

- the following six units (36 credit points); and
- two units (12 credit points) of Specified elective studies.

[FIT5003](#)

[6 CP](#)

**[Software security](#)**

[FIT5037](#)

[6 CP](#)

**[Network security](#)**

[FIT5057](#)

[6 CP](#)

**[Project management](#)**

[FIT5125](#)

[6 CP](#)

**[IT research and innovation methods](#)**

[FIT5129](#)

6 CP

**Cyber operations**

FIT5163

6 CP

**Introduction to cryptography for cybersecurity**

**Specified elective studies12 credit points**

keyboard\_arrow\_down

You must complete one of the following units (6 credit points) plus one Level 5 elective unit (6 credit points) from the faculty or across the university. You must have the required prerequisites for the unit you choose.

FIT5124

6 CP

**Emerging topics for cybersecurity in practice**

FIT5223

6 CP

**IT forensics**

FIT5225

6 CP

**Cloud computing and security**

## **Part C. Applied studies24 credit points**

keyboard\_arrow\_down

You must complete either the Industry experience pathway or Research pathway.

### **Industry experience pathway24 credit points**

keyboard\_arrow\_down

You must complete the following units (18 credit points) plus one FIT-coded Level 5 unit (6 credit points). You must have the required prerequisites for the unit you choose.

[FIT5120](#)

[12 CP](#)

[Industry experience studio project](#)

[FIT5122](#)

[6 CP](#)

[Professional practice](#)

### **Research pathway24 credit points**

keyboard\_arrow\_down

You must complete the following units.

Note 1: Enrolment in the research units is dependent on available supervisors and projects. Eligible students will be ranked based on their entire academic record and assessed for suitability to undertake the research component of this program.

Note 2: To be eligible for the research pathway:

You must have successfully completed at least 24 credit points of level 5 FIT-coded units;

and have an overall average of at least 80% across all Level 5 units; and must have achieved at least a distinction (75%) in FIT5125 IT research methods; and achieved an overall course WAM of 70%.

If you have a WAM between 75-79% across all Level 5 units you must have successfully completed at least 24 credit points of level 5 FIT-coded units; and demonstrated research capability with written support from a prospective supervisor; and must have achieved at least a distinction (75%) in FIT5125 IT research methods; and achieved an overall course WAM of 70%.

[FIT5126](#)

[6 CP](#)

**[Masters thesis part 1](#)**

[FIT5127](#)

[6 CP](#)

**[Masters thesis part 2](#)**

[FIT5128](#)

[6 CP](#)

**[Masters thesis final](#)**

[FIT5122](#)

[6 CP](#)

**[Professional practice](#)**



**Alternative exit(s)**

You may exit this course early and apply to graduate with one of the following awards, provided you have satisfied the requirements for that award during your enrolment in this master's course:

- Graduate Certificate of Cybersecurity (C4001) after successful completion of 24 credit points of study, comprising FIT5057 Project management, FIT5163 Introduction to cryptography for cybersecurity, FIT5003 Software security and one of the listed specified FIT units (6 credit points) from Part A or Part B.
- Graduate Diploma of Cybersecurity (C5001) after successful completion of 48 credit points of study, comprising all core studies units in Part B and two units (12 credit points) from Part A or Part B (specified elective studies) with a maximum of 12 credit points from Part A.

**Progression to further studies**

Successful completion of this course may provide a pathway to a graduate research degree.

Progression will be conditional on you completing the minor thesis research pathway (as described in Part C, Research Pathway) and achieving the minimum entry requirements for either the Master of Philosophy (3337) or the Doctor of Philosophy (0190).