Master of Cyber Security (MCYS) - MCyberSec

CRICOS code (International applicants): 0100380

You are currently viewing the 2023 Handbook. For study in 2024, please refer to the 2024 UniSQ Handbook.

Please be advised that this program will be transitioning from Semester to Trimester study periods in 2024. Trimester 1 starts on 22 January 2024. Read more in our new academic calendar FAQs.

	On-campus	Online
Start:	Semester 1 (February) Semester 2 (July)	Semester 1 (February) Semester 2 (July) Semester 3 (November)
Campus:	Springfield, Toowoomba	-
Fees:	Domestic full fee paying place International full fee paying place	Domestic full fee paying place International full fee paying place
Standard duration:	2 years full time, up to 4 years part-time	

Notes:

In 2023 the program follows the Semester calendar. The Academic Calendar and Important Dates webpage will allow you to view and download a copy of the important dates for the Semester calendar.

Contact us

Future Australian and New Zealand students	Future International students	Current students
Ask a question Freecall (within Australia): 1800 269 500 Phone (from outside Australia): +61 7 4631 5315 Email: study@usq.edu.au	Ask a question Phone: +61 7 4631 5543 Email: international@usq.edu.au	Ask a question Freecall (within Australia): 1800 007 252 Phone (from outside Australia): +61 7 4631 2285 Email: usq.support@usq.edu.au

Program aims

The Master of Cyber Security is a program that enables students to acquire an advanced level of knowledge and skills, including project experience in Cyber Security. The program will provide students with skills in Cyber Security and broaden this knowledge into contemporary domains including data mining, big data analytics, web and cloud security, Internet of Things, Financial Technology, and digital forensics. The capstone project provides students with skills comparable to industry practice.

Program objectives

Upon successful completion of this program, students should be able to:

- Expertly synthesise and apply advanced Cyber Security specific knowledge, including contemporary and emerging theories and concepts, to a range of business contexts and scenarios;
- Critically examine, analyse, implement and articulate a range of innovative solutions to a variety of real-life Cyber-Security business scenarios;
- Apply specialised cogniti25.568 Tm(usiness scen8e)Tj5.568 Tm(rea.0aro2.368.03 71 611100.334 Tmr1et of)Tj1 0 s

- Employ a range of oral, written and digital literacies to transmit complex Cyber Security knowledge in professional and scholarly contexts to a diverse audience;
- Apply principles of integrity and high calibre ethical behaviour in accordance with academic, industry and professional standards.

Australian Qualifications Framework

The Australian Qualifications Framework (AQF) is a single national, comprehensive system of qualifications offered by higher education institutions (including universities), vocational education and training institutions and secondary schools. Each AQF qualification has a set of descriptors which define the type and complexity of knowledge, skills and application of knowledge and skills that a graduate who has been awarded that qualification has attained, and the typical volume of learning associated with that qualification type.

This program is at AQF Qualification Level 09. Graduates at this level will have specialised knowledge and skills for research, and/or professional practice and/or further learning.

The full set of levels criteria and qualification type descriptors can be found by visiting www.aqf.edu.au.

Admission requirements

To be eligible for admission, applicants must satisfy the following requirements:

- Completion of an Australian university bachelor degree, or equivalent.
- English Language Proficiency requirements for Category 2.

All students are required to satisfy the applicable English language requirements.

If students do not meet the English language requirements they may apply to study a University-approved English language program. On successful completion of the English language program, students may be admitted to an award program.

Program fees

Domestic full fee paying place

Domestic full fee paying places are funded entirely through the full fees paid by the student. Full fees vary depending on the courses that are taken. Students are able to calculate the fees for a particular course via the Course Fee Schedule

Domestic full fee paying students may be eligible to defer their fees through a Government loan called FEE-HELP provided they meet the residency and citizenship requirements.

Australian citizens, Permanent Humanitarian Visa holders, Permanent Resident visa holders and New Zealand citizens who will be resident outside Australia for the duration of their program pay full tuition fees and are not eligible for FEE-Help.

International full fee paying place

International students pay full fees. Full fees vary depending on the courses that are taken and whether they are studied on-campus, external or online. Students are able to calculate the fees for a particular course via the Course Fee Schedules.

Program structure

The Master of Cyber Security consists of 16 units and has the following structure:

- six foundation core courses, each of one unit
- four advanced core courses, each of one unit
- four advanced specialisation courses, each of one unit; and
- one capstone project course of two units.

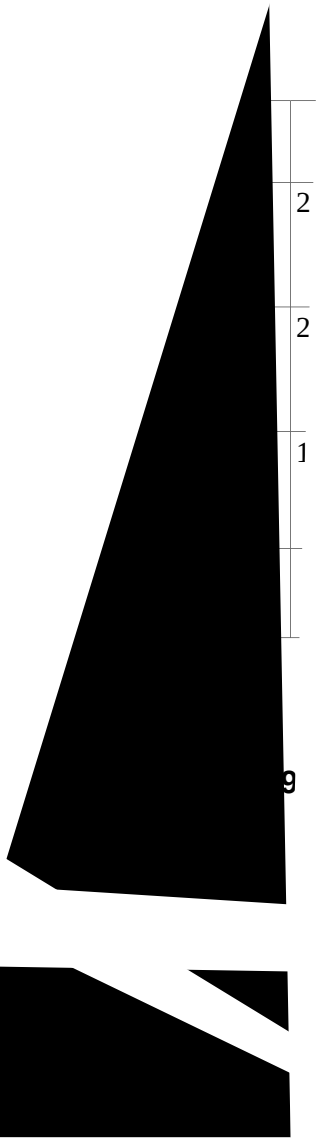
CIS801	al
Innovat	
CIS80	Data
Visual	
CIS8	ckchain
Fund	ls£

Footn

£ ster 3, 2(Nov
2024

Go nce

Cou
C ' C
M m
! s



Exit points