HED009

MASTER OF CYBER SECURITY

(ADVANCED)

TAFE Queensland | STUDY PACIFIC

MASTER OF CYBER SECURITY

(ADVANCED)

HED008 | CRICOS: 117453K | PROVIDER: 03020E

This Master of Cyber Security (Advanced) course is designed to prepare students with the comprehensive knowledge, skills and ethical understanding required to actively engage in the fast-evolving challenges of the digital landscape. Students are encouraged to explore emerging technologies, anticipate future threats, and develop creative solutions that stay ahead of cyber adversaries.

WHAT YOU WILL STUDY

The successful achievement of this qualification requires you to complete 160 credit points comprising 11 core units (120 credit points) and elective units (40 credit points) from the list below.

CORE UNITS

UNIT CODE	UNIT NAME	Credit points	EFTSL
CYB801	Cyber Security Risk and Incident Management	10	0.125
CYB802	Cyber Security Law and Ethics	10	0.125
CYB803	Information and Network Security	10	0.125
CYB804	Applied Project	10	0.125
CYB805	Cyber Security Policy and Governance	10	0.125
CYB806	Penetration Testing and Defence	10	0.125
CYB901	Cyber Security Project Management	10	0.125
CYB902	Emerging Cyber Security Threats	10	0.125
CYB903	Professional Project	10	0.125
CYB904	Psychology of Cybercriminals	10	0.125
CYB906	Cyber Project 3	20	0.250

Elective units

CYB807	Digital Forensics	10	0.125
CYB808	Operational Technology	10	0.125
CYB905	Cyber Project 1 and 2	20	0.250
CYB907	Applied Digital Forensics and Law	20	0.250

TAFE Queensland

STUDY PACIFIC

ENTRY REQUIREMENTS

Entry requirements All applicants To commence the Master of Cyber Security (Advanced) you should have:

Bachelor's Degree within the last six years or other qualification at a higher AQF level in a relevant related discipline;
OR
Five years of relevant IT industry/work experience;
OR
Evidence of academic capability deemed to be equivalent;
OR
Combination of the above

A relevant/related qualification means Computer Science, Information Technology, Information Systems, Business Data Analytics, Software Engineering, Cyber Security, or another comparable/equivalent field.

Relevant work experience includes a minimum of five years' work in a professional, knowledge-based or information-oriented workplace. Such as demonstration of experience in a technology or enterprise role related to Computer Science, Cyber Security, Information Technology, Information Systems, Business Data Analytics, Software Engineering or another comparable/equivalent field. This will need to be supported with evidence.

ENGLISH

Language requirements

English language requirements apply to applicants whose previous study was undertaken in a language other than English. The minimum English language requirements for such applicants for entry to this course are described below and applicants must sit the academic version, not the general version.

English Language Proficiency Standards:

PTE:	Minimum overall score of 58 and a minimum score of 58 in each of the four communicative skills
Academic IELTS:	6.5 (no individual band less than 6.0)
TOEFL:	iBT: 79 (19 reading, 20 listening, 20 speaking, 24 writing)
OET:	Pass at "B" level in each of four components

COURSE LEARNING OUTCOMES

1. Demonstrate application of high-level knowledge and technical skills to design, develop, implement and manage innovative and sustainable solutions to complex cyber security challenges through advanced skills in professional practice and teamwork.
2. Apply specialised knowledge to critically analyse and evaluate cyber security policies, governance and risks, as well as develop and plan implementation of cyber security policies, governance and risk mitigation strategies.
3. Show an extended knowledge of recent and emerging developments in cyber security by undertaking an applied project and critical reflection to investigate and synthesise an advanced body of cyber security knowledge.
4. Demonstrate an advanced understanding of cyber security standards, regulations, law and ethical principles by critically analysing and interpreting complex technical cyber security cases, ethical issues, principles and liabilities.
5. Use high level written, verbal, and interpersonal communication skills to address cyber security challenges with customised solutions for diverse audiences.

POTENTIAL PATHWAYS

- Cyber Security Analyst
- Forensic Computer Analyst
- Cyber Security Architect
- Cyber Risk and Governance Consultant
- Cyber Security Manager
- Cyber Security Policy Officer

STUDY LOCATION

Gold Coast

NEXT INTAKE

Start date: 13 Jul 2026
Duration: 2 years

ANNUAL INDICATIVE COST

International $30,000

Call Pawan on 70759 24568
Email: info@studypacific.ac.fj

STUDY PACIFIC

1st Floor, Dalmax Lincoln Building, Lot 1, Nadi Back Road, Nadi
Phone +679 971 4432 | info@studypacific.ac.fj | www.studypacific.ac.fj

TAFE Queensland