



# Diploma of Information Technology

## Specialisation: Cyber Security

 Qualification Code:  
**ICT50220**

 CRICOS Course Code:  
**113797G**

 Duration  
Course duration is calculated on 20 hours per week of face-to-face training for 44 weeks & 8 weeks of allocated term break.  
**Total Course Duration: 52 weeks**

 Mode of Delivery

- Face to face classroom based.
- Multicultural groups in an instructor-led learning environment.
- Assessment in simulated environment.

### Qualification Overview

This qualification reflects the roles of individuals in a variety of information and communications technology (ICT) roles who have established specialised skills in a technical ICT function.

Individuals in these roles carry out moderately complex tasks in a specialist field, working independently, as part of a team or leading a deliverable with others. They may apply their skills across a wide range of industries, business functions and departments, or as a business owner (sole trader/contractor).

The specialised skills required for a wide variety of roles are listed in the Training Package.

### Who can Enrol?

Target group for this program will be the international students over the age of 18 including mature aged clients who wish to further develop or formalise their skills in Cyber Security.

### Recommended Pathways from the Qualification

After achieving this qualification, individuals could progress to ICT60220 - Advanced Diploma of Information Technology qualification. They may choose to advance their selected specialisation areas or expand their skills and knowledge in new areas.

### Entry Requirements

There are no formal prerequisites required to enter the Diploma of Information Technology. However, applicants must meet the following entry requirements:

### English Language Requirement

Minimum IELTS score of 6.0 Or PTE score of 52 or Certificate IV in EAL or equivalent\*.

\*For equivalency of various English Languages proficiency testing, and other forms of equivalency please refer to the admissions and student selection policy available in the student's handbook ([www.omni.edu.au](http://www.omni.edu.au)).

### Academic Requirement

No prior academic requirements apply for this qualification; however, Omni College requires successful completion of Australian Equivalent Year 12 qualification or higher.

### Employment Pathways from the Qualification

Job roles and titles vary across different industry sectors. Possible job titles relevant to this qualification include:

- Cyber Security Specialist
- Network Support Analyst
- Network Operations Analyst
- Network Technician
- Network Security Analyst
- Network Security Administrator

### Age Requirement

All applicants must be aged 18 years or over at the time of applying for admission to the course.

### Other

Applicants should have proficiency in digital literacy and MS Office skills (Word, Excel and Power Point). Applicants should be in possession of their personal computer (the minimum configuration should be Intel Core i3 (sixth generation or newer) or equivalent. Operating System: Microsoft Windows 10 Professional x64, Memory: 4 GB RAM, Storage: 120 GB internal storage).

### Language Literacy and Numeracy (LLN) Requirement

Applicants will be required to demonstrate their LLN capabilities and/or complete an LLN assessment prior to the commencement of the course as per the Omni Pre-training and LLN Policy and Procedure. Omni College uses LLN Robot platform for the assessment.

**Note:** In the absence of formal English qualifications Omni College may prefer English Placement Test.



## CORE UNITS

BSBCRT512	Originate and develop concepts
BSBXCS402	Promote workplace cyber security awareness and best practices
BSBXTW401	Lead and facilitate a team
ICTICT517	Match ICT needs with the strategic direction of the organisation
ICTICT532	Apply IP, ethics and privacy in ICT environments
ICTSAS527	Manage client problems

## SPECIALISED ELECTIVE UNITS – CYBER SECURITY

ICTCYS407	Gather, analyse and interpret threat data
ICTCYS610	Protect critical infrastructure for organisations
ICTCYS613	Utilise design methodologies for security architecture
ICTSAS524	Develop, implement and evaluate an incident response plan
ICTSAS526	Review and update disaster recovery and contingency plans

## GENERAL ELECTIVE UNITS\*

ICTICT519	Develop detailed component specifications from project specifications
ICTPMG505	Manage ICT projects
ICTSAS502	Establish and maintain client user liaison
ICTNPL413	Evaluate networking regulations and legislation for the telecommunications industry
ICTSAD509	Produce ICT feasibility reports
ICTICT523	Gather data to identify business requirements
ICTICT526	Verify client business requirements
ICTICT443	Work collaboratively in the ICT industry
ICTSAS512	Review and manage delivery of maintenance services

**Note:** \*The general elective units may change at college's discretion, if necessary.

