

ICT50220 Diploma of

Information Technology

(Cyber Security & Cloud Engineering)

A practical, industry-focused qualification designed to build real capability across cyber security, cloud infrastructure, network defence, investigations, security architecture, business application and ethical hacking.



This brochure summarises the course structure, subjects, units and VET Student Loans overview.

View the full course page

technologycourses.com.au

Scan the QR code



COURSE OVERVIEW

A clear snapshot of how the course is delivered, what it covers, the main tools used and the study support provided.

ABOUT THE COURSE

The Cyber Security & Cloud Engineering stream is designed for students who want a practical pathway into the technology industry. It combines cyber defence, cloud infrastructure, network security, investigation skills, security architecture, business application and professional ICT practice.

COURSE SNAPSHOT

DELIVERY	100% online
SUPPORT	Course coach
CLASSES	Optional online lectures
PRIOR QUALIFICATION	Not required

ENTRY & SUITABILITY

- No prior qualification is required.
- Applicants must meet the required English and numeracy level.
- Study capacity and course suitability are assessed.
- The entry team reviews each application.

CORE TOPICS

Cyber industry

Attacker mindset

Phishing

Social engineering

Cyber tools

Penetration testing

Firewalls & DDoS

VPNs

Malware defence

Hardware & Wi-Fi

Security reports

TOOLS & PLATFORMS

AWS

Cloudflare

Kali Linux

Wireshark

Cisco Packet Tracer

Virtual Machines

Nessus

Nmap

Splunk SIEM

Docker

CloudTrail

Python

01

Fundamentals of Cyber Security

WHAT YOU'LL LEARN

- Understand who targets Australian organisations, why attacks happen and the common paths attackers use to gain access.
- Build confidence using the command line and terminal environments used by cyber security professionals.
- Analyse modern phishing techniques, including AI-assisted phishing and signals that help identify suspicious content.
- Use open-source intelligence techniques to understand what attackers can learn from publicly available information.
- Recognise social engineering risks, including impersonation, deepfakes and voice cloning, and plan human-centred defences.
- Assess third-party and vendor risk before it becomes an organisational security weakness.

02

Cyber Security Application

WHAT YOU'LL LEARN

- Deploy and secure a live web application using Cloudflare.
- Apply identity and access management controls to restrict access appropriately.
- Configure SSL, rate limiting and firewall controls for a production-style environment.
- Respond to and mitigate distributed denial-of-service activity against a live application.
- Review an organisation against security and privacy frameworks such as Essential Eight, ISO 27001 and Australian privacy requirements.
- Turn technical findings into practical remediation priorities.

03

Cloud Security (Cloud Computing & Security)

WHAT YOU'LL LEARN

- Build a secure AWS environment from a new account through to a functional cloud deployment.
- Launch and secure EC2 compute and S3 storage using encryption and access controls.
- Deploy a containerised application using Docker in an AWS environment.
- Apply the cloud shared-responsibility model to separate provider responsibilities from customer responsibilities.
- Design private and encrypted cloud networking, including VPN connectivity.
- Use CloudTrail and cloud logs to review actions and support security investigations.

04

Network Security & Hardware

WHAT YOU'LL LEARN

- View networks from both attacker and defender perspectives across the OSI model.
- Run reconnaissance and discovery scans in controlled environments using Kali Linux and Nmap.
- Capture and inspect network traffic with Wireshark, including traffic generated during attack simulations.
- Configure a Splunk SIEM environment, ingest logs, query data and create alerts for suspicious activity.
- Understand hardware-layer security, including TPM, Secure Boot, firmware risk and side-channel concepts.
- Run Nessus vulnerability scans and interpret findings so they can be prioritised and remediated.

05

Cyber Investigations

WHAT YOU'LL LEARN

- Understand the Australian cyber investigation ecosystem and the roles of agencies involved in different incident types.
- Preserve digital evidence correctly so it can remain useful for investigation and legal processes.
- Triage and extract information from seized or compromised devices using investigation workflows and tools.
- Conduct structured OSINT investigations across platforms, metadata and historical web sources.
- Follow financial trails through banking and blockchain environments using forensic investigation concepts.
- Guide a cyber incident from initial report through evidence handling, response actions and referral.

06

Cyber Security Business Application

WHAT YOU'LL LEARN

- Translate cyber risk into a business case that decision-makers can understand and act on.
- Recognise AI-accelerated threats such as voice cloning, deepfakes and automated phishing.
- Assess large language models for prompt-injection and related AI security weaknesses.
- Use Python for security-focused tasks such as networking, encryption, hashing and automation.
- Conduct a controlled penetration-testing workflow in Kali Linux from reconnaissance through exploitation.
- Apply Australian AI governance and ethical principles to real business technology workflows.

CORE UNITS

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

ELECTIVE UNITS

- 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
- ICTCLD505 - Implement cloud infrastructure with code
- ICTCLD506 - Implement virtual network in cloud environments
- ICTCLD507 - Build and deploy resources on cloud platforms
- ICTCLD508 - Manage infrastructure in cloud environments
- ICTICT426 - Identify and evaluate emerging technologies and practices
- ICTICT427 - Identify, evaluate and apply current industry-specific technologies to meet organisational needs
- ICTCLD512 - Respond to cloud security incidents
- ICTNWK546 - Manage network security
- ICTICT424 - Address cyber security requirements
- ICTCYS407 - Gather, analyse and interpret threat data
- ICTCYS610 - Protect critical infrastructure for organisations

UNIVERSITY PATHWAYS

The published course page lists pathways with Curtin University, the University of Newcastle, Edith Cowan University and Griffith University.

AUSTRALIAN GOVERNMENT VET STUDENT LOAN

A VET Student Loan is an Australian Government income-contingent loan that can help eligible students pay approved tuition fees for eligible higher-level VET courses.

ELIGIBILITY

- Be enrolled in this approved course with EQC as an approved VSL provider.
- Be an Australian citizen, a permanent humanitarian visa holder usually resident in Australia, a Pacific Engagement visa holder usually resident in Australia, or a qualifying New Zealand Special Category visa holder.
- Be academically suited to the course (see Entry & Suitability, page 2).
- Study the course primarily within Australia.
- Hold a Unique Student Identifier (USI) and supply your Tax File Number through the Australian Government eCAF system — EQC never collects or sees your TFN.
- Have HELP balance remaining.

THE ESSENTIALS

- A VET Student Loan will not be approved for students who do not meet the eligibility requirements.
- A VET Student Loan gives rise to a VETSL debt that continues to be a debt due to the Commonwealth until it is repaid.
- Borrowing is limited by the course loan cap and the
- A loan fee of 20% applies to the loan amount for students who are not eligible for an exemption.
- compulsory repayments apply and can affect borrowing capacity.
- Review your HELP balance and consider independent financial advice where appropriate.

VSL ENROLMENT PROCESS

01 Check course, provider and personal eligibility.

02 Apply to enrol and provide identity, citizenship/residency and academic-suitability evidence.

03 Complete any required entry or literacy/numeracy assessment.

04 Review written information about fees, the loan and student rights before accepting the enrolment.

05 Complete the electronic Commonwealth Assistance Form (eCAF): EQC sets it up and the system emails you your login. Submit it no earlier than 2 business days after you enrol, and by 11:59 pm AEST on or before the census day of the first unit you want the loan to cover.

06 Complete required progression checks and review VSL notices issued during your enrolment.

IMPORTANT STUDENT INFORMATION

VSL tuition charges are associated with fee periods and census days. Students receive prescribed notices about covered fees and Commonwealth assistance. Withdrawal rights depend on the applicable census rules. Students should read the provider's VSL procedures and current Australian Government guidance before applying.

READY TO EXPLORE THE FULL COURSE?

Use the QR code or visit the course page to read the full details, review eligibility information and view the latest published course information.

SCAN THE QR CODE



Open the full course page

VET Student Loan access is subject to current eligibility requirements and provider assessment.

Equinim College trading as EQC Institute of Technology | RTO 45758 | CRICOS 03952E



Information

ICT50220 Fact Sheet

Course code	ICT50220
Course titles	This Fact Sheet covers the three current ICT50220 course structures listed on page 1 and detailed in the unit tables later in this document.
Currency	The qualification should be checked on the official national register at training.gov.au/Training/Details/ICT50220 . Students should confirm the current status before enrolment.
Course duration (estimated)	Approximately 10 months for current intakes. Duration may be varied by approval and the dates for each intake are published in this Fact Sheet.
Delivery locations	Learning and assessment are conducted online.
Delivery method	Online
Third parties providing services on our behalf	None.
Our obligations as a RTO	When you enrol with us, we are obliged to deliver training and assessment in the training product in which you enrol in accordance with the Standards for RTOs 2025 and the requirements of the National VET Regulator, the Australian Skills Quality Authority. We are also obliged to issue qualification certificates, records of results and statements of attainment in accordance with the Standards. We provide a Privacy Notice as part of enrolment setting out information about your personal information and data. The Privacy Notice is available before enrolment from our website.
Your rights as a student	As you progress through your course, you will lodge assessments online. You have the right to appeal academic decisions and to lodge a complaint. Details are set out in the Complaints and Appeals Policy and Procedure, the Student Handbook and our published Policies and Procedures.
Feedback	We value your feedback at all times. We encourage you to tell us where we are doing a great job and where we could improve. You may also lodge a complaint under the Complaints and Appeals Policy and Procedure.
Our assurance regarding pre-paid fees	EQC Institute is committed to quality education and training and maintains systems for the quality and validity of training and assessment across its scope and modes of delivery. We comply with the Standards when collecting student fees in advance. For the current VSL structure, tuition is allocated across three sequential units of study and is disclosed through the Statement of Covered Fees, Fee Notice and Commonwealth Assistance Notice. Any upfront amount must follow the applicable agreement and published fee arrangements.

Resources and Support

ICT50220 Fact Sheet

Your obligations as a student	You are required to make steady progress during your course and complete all learning and assessments. You must submit assessment tasks by the required due dates. Further information is contained in the Student Handbook.
RPL and National Recognition	EQC Institute welcomes applications for recognition of prior learning (RPL) and National Recognition or credit transfer. Contact our team to discuss whether one of these options may be suitable for you.
Student support	You may access support through the Student Services Team by email at team@equinimcollege.com or by phone on 1800 338 883.
Policies and Procedures	You are required to comply with EQC Institute Policies and Procedures, as amended from time to time. Policies and procedures are available at technologycourses.com.au , and key policies are summarised in the Student Handbook.
Assessment and progress	Assessment tasks are completed online. Students are expected to participate, maintain progress and respond to reasonable contact from EQC Institute. Assessment due dates and any approved variations are recorded online.
Privacy	EQC Institute provides a Privacy Notice as part of enrolment. This explains how personal information and data are collected, used, stored and disclosed.

SUPPORT IS AVAILABLE

Please contact EQC Institute early if you are experiencing circumstances that may affect your participation, progress or ability to meet assessment dates. We will explain the support, extension, special consideration and withdrawal processes that may be available.