PERSONAL LEARNING REQUIREMENTS

ICT50220 Diploma of Information Technology (Cyber Security)

Before you Enrol

Please review the requirements listed in this document and think about if you might experience challenges in meeting them related to your disability, health condition, learning support assistance or for any other reason. You should discuss your concerns with us before enrolling in your course and can start the conversation by contacting our Customer Service team at:

Phone: 03 5225 0500 **Email:** courinfo@gordontafe.edu.au

You can also contact any of our support services:

- Disability Support Team
- Learning Support Services: Student wellbeing and support
- Career Counselling
- Geelong or Werribee Skills and Jobs Centre

You can view all courses offered at The Gordon here

The skills and abilities required to study in this course and work in the industry include:

Communication Skills

- Ability to communicate effectively using spoken and written English in an online learning environment, including participation in live virtual classes, discussions, and group activities
- Ability to interpret and follow complex technical instructions, assessment requirements, and cybersecurity scenarios
- Ability to document technical processes, system configurations, incident responses, and project outcomes clearly using appropriate industry terminology
- Ability to collaborate with peers and trainers in virtual environments, including contributing to group projects and participating in discussions using digital communication tools

Physical Skills

- Ability to sit and work at a computer for extended periods, including attending scheduled evening online classes and completing self-paced learning activities
- Ability to use standard computer equipment, including keyboard, mouse, webcam, and headset, for sustained periods
- Sufficient visual ability to read and interpret on-screen content, including technical diagrams, system outputs, and virtual lab environments
- Ability to operate a personal computing device that meets course technical requirements, including participation in virtual labs and simulations

Cognitive Skills

- Ability to analyse complex technical problems and apply logical thinking to troubleshoot cybersecurity, networking, and system issues

- Ability to learn and apply new and emerging technologies, tools, and methodologies in a structured and self-directed environment
- Ability to plan, organise, and prioritise learning and assessment tasks across structured online classes and self-paced study
- Ability to interpret and evaluate technical information such as network diagrams, system configurations, logs, and threat data
- Ability to apply judgement and decision-making in simulated environments, including responding to cybersecurity incidents and project-based scenarios

Behavioural & Social Skills

- Ability to work independently in an online learning environment and take responsibility for meeting course requirements and deadlines
- Ability to collaborate effectively with others in virtual teams, including participation in group projects and simulated workplace activities
- Ability to demonstrate professional behaviour, including reliability, punctuality, and respectful communication in online settings
- Ability to respond positively to feedback and adapt to changing requirements within project-based and simulated SOC environments
- Ability to follow organisational policies, procedures, and acceptable use requirements when accessing systems, virtual labs, and online platforms

Digital Skills

- Ability to use advanced digital skills to engage with complex ICT systems and learning platforms
- Ability to effectively use online learning systems (e.g. LMS), collaboration platforms, and virtual lab environments (e.g. NETLAB)
- Ability to research, analyse, and evaluate technical information from multiple digital sources
- Ability to manage files, data, and digital content securely, including applying cybersecurity principles and maintaining system integrity
- Ability to participate in online classes using video conferencing tools, including breakout rooms, presentations, and collaborative activities
- Able to confidently use digital tools and technologies in complex and varied situations. Can troubleshoot issues, adapt to new systems quickly, and support others in using digital tools. Demonstrates strong problem-solving and critical thinking in digital environments.
- Configure and customise software or applications for specific needs
- Analyse and interpret data using advanced tools (e.g., pivot tables, data visualisation)
- Integrate multiple digital tools to streamline workflows
- Manage digital security settings and permissions
- Use collaboration platforms effectively for project management
- Create interactive or multimedia content for diverse audiences
- Troubleshoot technical issues independently and provide guidance to other
- Ability to configure, manage, and troubleshoot software, virtual machines, and networked environments used in cybersecurity training

Industry Legislation or Licencing

There are no specific licensing or accreditation requirements attached to this qualification at course completion.

However, the cyber security and information technology industry requires knowledge of, and the ability to apply, relevant legislation, standards, and codes of practice in a professional context.

This may include:

- Privacy and data protection legislation (e.g. Australian Privacy Principles)
- Cyber security frameworks and standards (e.g. ISO/IEC 27001, NIST Cyber Security Framework)
- Organisational policies, procedures, and acceptable use requirements
- Workplace Health and Safety (WHS) legislation, regulations, and codes of practice

Depending on the employment context, graduates may be required to:

- Undertake background screening, such as a National Police Check
- Obtain a Working with Children Check (where applicable to the role or employer requirements)