Program Information Document

ICT50220 Diploma of Information Technology (Cyber Security)

This qualification comes from a training package created by the Commonwealth Government for Information and Communications Technology (ICT) defining core and elective competency units. We've chosen specific elective units from the training package, based on input from industry experts, to address South Australia's workforce requirements.

The Diploma of Information Technology, specialising in Cyber Security reflects the role of individual 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 skills required for these roles may include, but are not restricted to:

- Protecting sensitive data and information through security architecture.
- Developing disaster recovery and contingency plans
- Manage network security
- Gather, analyse, and interpret threat data
- Undertake penetration testing

Employment Opportunities

- Network security administrator
- Cyber security operations administrator
- Cyber security specialist
- Network security support officer
- Website security support officer
- Information systems security support officer
- Cyber network services administrator
- Cyber security network support administrator

The recommended fulltime study plan will require 12 months of study to complete this qualification.

Program Information Document

Course Admissions Requirement

- Certificate IV in Cyber Security

If you do not have a Certificate IV in Cyber Security but other relevant qualifications or industry experience, you may wish to email admissions@tafesa.edu.au to discuss.

Information on the contents of the 22603VIC Certificate IV in Cyber Security can be found here:

Certificate IV in Cyber Security Program Information Document.

Incidentals Costs

You will be required to provide your own access to the following hardware. This hardware costs approximately $700.00.

- 1TB SSD portable hard drive,
- Webcam,
- Headset with microphone,
- Purchase of a Public Domain Name,
- Raspberry Pi 4 (or higher) Starter Kit with minimum 4GB and minimum 16GB SD card. Accessories required are as following:
  - PIR Motion Sensor (compatible with your Raspberry Pi)
  - Raspberry Pi Camera Module 3 with cable suitable for your Pi
  - Temperature and Humidity Sensor - DHT22 (SEN0137)
  - Fingerprint Sensor - Basic Fingerprint Sensor with Socket Header Cable (ADA4690)
  - 150mm Socket to Socket (F to F) Jumper Leads

Note: Students who have completed the 22603VIC Certificate IV in Cyber Security at TAFESA and have access to the Raspberry Pi Kit with PIR motion sensor and camera module, may need only to purchase the temperature and humidity sensor and fingerprint sensor

Software

All software required to complete this course will be available for students at no additional cost.

Program Information Document

Hardware

Access to computer hardware is provided at certain TAFE SA campuses.

It is important to note that for students studying this course and not able to attend a suitable campus it will be assumed that you have the necessary computer hardware to run the required resources. You will need to have a Windows machine with the following as a minimum.

- Intel i5 CPU (or equivalent AMD), (Intel i7, recommended)
- 16GB of RAM, (32GB, recommended)
- 1Tb SSD

Note: Apple MAC notebooks are not compatible with some of the software required for this course and cannot be supported.

Internet

To study away from a campus, you will be required to have internet access.

This qualification requires students to use virtual machines for learning activities and assessments. Students will be required to obtain these from either their local campus or from the Internet. Virtual machine file sizes can vary but are generally above 20GB in size. The time to download these virtual machines from the Internet may vary depending on your Internet connection speed.

Program Information Document

Required Competencies

Diploma of Information Technology (Cyber Security)
National Code: ICT50220 TAFE SA Code: TP01271

This table shows the units of competency that you must have on your academic record to achieve this qualification. The National Training Package requires 20 units. The units are listed in the sequence that you should complete them. This is particularly important for part-time students. Standard study plans are provided below. The table also provides details of any assumed knowledge and skills for each unit. You must have these skills before attempting these units.

Units of Competency (listed in delivery sequence)

Unit Code	**Unit Title**	**Core/Specialist Elective/Elective**	**Assumed knowledge & skills**
ICTNWK428	Create scripts for networking	Elective	None
BSBXCS402	Promote workplace cyber security awareness and best practices	Core	None
ICTNWK536	Plan, implement and test enterprise communication solutions	Elective	None
ICTSAS526	Review and update disaster recovery and contingency plans	Specialist Elective	None
ICTSAS527	Manage client problems	Core	None
ICTCLD507	Build and deploy resources on cloud platforms	Elective	None
ICTNWK544	Design and implement a security perimeter for ICT networks	Elective	None
ICTCYS407	Gather, analyse and interpret threat data	Specialist Elective	None
ICTSAS524	Develop, implement and evaluate an incident response plan	Specialist Elective	ICTCYS407
ICTICT532	Apply IP, ethics and privacy policies in ICT environments	Core	None
ICTDAT501	Gather, analyse and verify data from different source inputs	Elective	ICTCYS407
VU23300	Detect and respond to cyber security threats	Elective	VU23218
ICTCYS603	Undertake penetration testing for organisations	Elective	None
BSBXTW401	Lead and facilitate a team	Core	None
ICTICT517	Match ICT needs with the strategic direction of the organisation	Core	None
ICTIOT501	Install IoT devices and networks	Elective	None
ICTCYS610	Protect critical infrastructure for organisations	Specialist Elective	None

Program Information Document

ICTCYS613	Utilise design methodologies for security architecture	Specialist Elective	None
ICTNWK546	Manage network security	Elective	None
BSBCRT512	Originate and develop concepts	Core	None

Program Information Document

Study Plan for Full-Time Students (12 months)

The following table shows the recommended study plan for Diploma of Information Technology (Cyber Security). Each stage is one semester (or 6 months) in length. Codes in brackets are the IT Subject names which are described in the Subject Description table below.

Stage 1	
Term 1	**Term 2**
ICTCLD507 (CLD5C2AZA) (4)	
ICTNWK544 (NWK544FGT) (2)	
ICTCYS407 (CYS407SPB) (2)	**ICTSAS526** (SAS526) (2)
ICTICT532 (ICT532) (2) *	**ICTDAT501** (DAT501SPA) (2)
ICTNWK536 NWK536MSO (4)	**ICTNWK428** (NWK428PSS) (4)
BSBXCS402 (XCS402) (2) *	**ICTSAS527** (SAS527) (2) *
ICTSAS524 (SAS524IRP) (2)	
IT Practical (2)	**IT Practical (4)**
20 hours / week	**20 hours / week**

Stage 2	
Term 1	**Term 2**
VU23300 (CVU300CCO) (4)	
ICTICT517 (ICT517) (2) *	
ICTIOT501 (IOT501) (2)	
ICTCYS603 (CYS603) (2)	
ICTCYS610 (CYS610) (2)	**ICTNWK546** (NWK546) (4)
ICTCYS613 (CYS613) (2)	**BSBCRT512** (CRT512) (2) *
BSBXTW401 (XTW401) (2)	
IT Practical (4)	**IT Practical (4)**
20 hours / week	**20 hours / week**

Program Information Document

Please Note: This program structure is subject to change.

Legend:

* Competencies delivered online are marked with an asterisk

( ) The number in brackets after the subject is the number of hours per week that you would expect to attend class for that subject as a campus or virtual student.

IT Practical sessions provide support to complete subject activities and assessments.

NOTE: The study plan is for a full-time student with class-attendance. This is usually 20 hours a week of attendance. It is expected that an additional 12-15 hours would be required outside of class time to complete activities and assessments.

Program Information Document

Study Plan for Part-Time Students (24 months)

The following table shows the recommended study plan for studying the Diploma of Information Technology (Cyber Security) as part-time (half-time). If a half-time plan does not meet your needs, you can study more or less subjects per term/semester, but you must follow the recommended sequence in the Required Competencies table above. Each stage is one semester (or 6 months) in length. Codes in brackets are the IT Subject names which are described in the Subject Description table below.

Stage 1	
Term 1	**Term 2**
ICTCYS407 (CYS407SPB) (2)	**ICTDAT501** (DAT501SPA) (2)
BSBXCS402 (XCS402) (2) *	**ICTSAS526** (SAS526) (2)
ICTNWK536 NWK536MSO (4)	**ICTSAS527** (SAS527) (2) *
IT Practical (2)	**IT Practical (4)**
10 hours / week	**10 hours / week**

Stage 2	
Term 1	**Term 2**
ICTCLD507 (CLD5C2AZA) (2)	
ICTNWK544 (NWK544FGT) (2)	
ICTSAS524 (SAS524IRP) (2)	**(NWK428PSS)** ICTNWK428 (4)
ICTICT532 (ICT532) (2) *	
IT Practical (2)	**IT Practical (2)**
10 hours / week	**10 hours / week**

Stage 3	
Term 1	**Term 2**
VU23300 (CVU300CCO) (4)	
ICTCYS603 (CYS603) (2)	
BSBXTW401 (XTW401) (2)	
IT Practical (2)	**IT Practical (4)**
10 hours / week	**10 hours / week**

Program Information Document

Stage 4	
Term 1	**Term 2**
ICTICT517 (ICT517) (2) *	
ICTIOT501 (IOT501) (2)	
ICTCYS610 (CYS610) (2)	**ICTNWK546** (NWK546) (4)
ICTCYS613 (CYS613) (2)	**BSBCRT512** (CRT512) (2) *
IT Practical (2)	**IT Practical (2)**
10 hours / week	**10 hours / week**

Legend:

* Competencies delivered online are marked with an asterisk

( ) The number in brackets after the subject is the number of hours per week that you would expect to attend class for that subject as a campus or virtual student.

NOTE: The study plan is for a part-time student studying a half-time load. This is approximately 10 hours a week of class time. It is expected that an additional 6-10 hours would be required outside of class time to complete activities and assessments

Program Information Document

IT Studies Subjects

TAFE SA IT Studies uses subject codes to indicate the context that has been chosen for the unit, guided by industry needs in South Australia. For example, **PRG443PYI** indicates that the content for delivery of unit PRG443**PYI** will include coverage of **Python** programming language.

The table below provided information on the context for each unit and provides the subject code that is used. If a subject contains more than one unit delivery and assessment will be done holistically so you will be awarded the same result for all units assessed in that subject that you have enrolled in. Your final official results will refer to the units.

Subject Description

Unit Code	IT Studies subject code	Description
ICTNWK428	**NWK428PSS**	This unit describes the skills and knowledge required to automate **Active Directory** and **Windows services** with **PowerShell scripts**. This subject is taught using Active Directory and services hosted on **MS Windows Server**. It applies to those who are responsible for the maintenance and coordination of database operations. They usually work in an organisation providing daily services as database administrators, database developers, database coordinators, or application developers.
BSBXCS402	**XCS402**	In this unit describes the skills and knowledge required to promote cyber security in a work area. It applies to those working in a broad range of industries who as part of their job role support policies, procedures and practice within an organisation that promote cyber security.
ICTNWK536	**NWK536MSO**	This unit outlines the skills and knowledge required to deploy, configure and manage enterprise communication solutions using **Microsoft 365** as the core platform. It covers services such as email (including remote access), web portals or content management solutions, and enterprise collaboration tools. It applies to ICT professionals responsible for implementing and administering **Microsoft 365 services** to deliver secure, reliable email, messaging and collaboration capabilities that meet the needs of enterprise users.
ICTSAS526	**SAS526**	In this unit you will learn the skills and knowledge required to analyse the impact of the system on the organisation and carry out risk analysis, disaster recovery and contingency planning.
ICTSAS527	**SAS527**	This unit focuses on the skills and knowledge needed to **work closely with clients to help them manage, troubleshoot, and resolve ICT-related problems**. You will learn how to communicate effectively, gather accurate information, provide informed advice, and support clients through the problem-solving process in a professional ICT environment..
ICTCLD507	**CLD5C2AZA**	In this unit describes the skills and knowledge required to configure, deploy and monitor a range of technology resources of core cloud computing service on a cloud platform. The unit applies to cloud engineers, cloud systems administrators and those who work within cloud computing operations to provision, implement and maintain cloud computing solutions for a business with little guidance or supervision. These ICT professionals may work from designs developed by cloud architects and focus on operational concerns, including automation and maintaining cloud resources.
ICTNWK544	**NWK544FGT**	This unit provides a solid working knowledge of the features and capabilities of the **Fortinet FortiGate** platform. You will develop the skills and knowledge required to

Program Information Document

		design and implement a high-performance, secure, and resilient network perimeter for enterprise ICT environments. It applies to individuals with advanced ICT expertise working in roles such as network engineers, security analysts, network technicians, information security managers, or other mid-level ICT and security positions responsible for managing and protecting enterprise networks.
ICTCYS407	**CYS407SPB**	This unit provides the skills and knowledge required to collect data from a range of sources, and to analyse and interpret that data to identify potential cyber security threats, inconsistencies and anomalies. You will develop the ability to ingest and normalise data from systems such as logs, network traffic and security tools, and apply analytical techniques to detect suspicious behaviour and indicators of compromise. The unit emphasises the use of platforms such as **Splunk** to search, correlate and visualise data, enabling effective threat detection and investigation.
ICTSAS524	**SAS524**	This unit provides the skills and knowledge required to develop, implement and manage an effective incident response plan for an organisation. It includes identifying potential security incidents, establishing appropriate response procedures, and coordinating actions to contain, eradicate and recover from cyber security events. You will learn how to assess the effectiveness of incident response activities, including evaluating outcomes against organisational objectives and determining the impact on business operations and mission-critical functions. The unit also covers continuous improvement practices, ensuring that lessons learned from incidents are used to refine response strategies, policies and procedures.
ICTICT532	**ICT532**	In this unit describes the skills and knowledge required to maintain professional and ethical conduct, as well as to ensure that personal information of stakeholders is handled in a confidential and professional manner when dealing with stakeholders in an Information and Communications Technology (ICT) environment. It applies to ICT personnel who are required to gather information to determine the organisation's code of ethics and protect and maintain privacy policies and system security.
ICTDAT501	**DAT501SPA**	This unit provides the skills and knowledge required to collect, analyse, test and validate data from a range of source inputs. It focuses on ensuring data accuracy, integrity and relevance to support informed decision-making within an organisation. You will develop the ability to ingest and process data from multiple sources, apply analytical techniques to identify patterns and anomalies, and verify results to ensure reliability. The unit emphasises the use of industry-standard tools such as **Splunk** to search, correlate and visualise data, enabling effective investigation and reporting.
VU23300	**CVU300CCO**	This unit describes the performance outcomes, skills and knowledge required to detect, analyse and respond to cyber security threats within an organisation. It includes preparing for incidents, understanding how attacks may occur, and applying appropriate processes and procedures to effectively respond. The unit also incorporates the use of core technologies such as SIEM, network security monitoring, endpoint detection and response (EDR), and threat intelligence platforms to analyse data and identify intrusions. The unit aligns with frameworks and best practices developed by the National Institute of Standards and Technology (NIST) and is mapped to the **Cisco CyberOps Associate** course.
ICTCYS603	**CYS603**	In this unit describes the skills and knowledge required to use a range of methodologies to simulate an attack on an organisation's information and security systems and report the results back to the organisation.

Program Information Document

BSBXTW401	**XTW401**	In this unit describes the skills and knowledge required to effectively lead and facilitate a team in a workplace within any industry. In this unit has a specific focus on the teamwork skills required for team leader or supervisor level (depending on organisational structure) workers with responsibility for others or teams.
ICTICT517	**ICT517**	In this unit describes the skills and knowledge required to ensure information and communications technology (ICT) products and systems match the strategic direction of the organisation. It applies to individuals whose responsibilities may include improving, evaluating, acquiring, maintaining and supporting ICT for organisations.
ICTIOT501	**IOT501**	In this unit you will learn the skills and knowledge required to install IoT (Internet of Things) devices and networks, including connecting, programming and testing the networks and devices for functionality against a given performance objective.
ICTCYS610	**CYS610**	This unit provides the skills and knowledge required to analyse an organisation's critical cyber security operations and design, implement and manage a protection strategy tailored to its needs. It focuses on securing **Windows-based network environments** and applying key controls to safeguard critical systems and data. The unit incorporates industry best practices, including the **Essential Eight**, to strengthen organisational resilience against common cyber threats.
ICTCYS613	**CYS613**	In this unit you will learn the skills and knowledge required to design security architecture to organisation requirements, utilising specific design methodologies.
ICTNWK546	**NWK546**	This unit provides the skills and knowledge required to implement and manage security functions across networked environments, with a focus on **Microsoft Windows–based systems**. It includes applying security controls, policies and best practices to protect organisational assets and maintain secure operations. The unit aligns with internationally recognised frameworks and standards, including International Organization for Standardization **ISO 27001** and **ISO 27002**, to ensure effective governance, risk management and information security practices.
BSBCRT512	**CRT512**	In this unit describes the skills and knowledge required to originate and develop concepts for products, programs, processes or services to an operational level. In this unit applies to individuals who develop concepts for any business or community activity or process. This may include marketing and advertising campaigns, staff development programs, information technology and communication systems, radio and television programs and entertainment events. These individuals operate with a high degree of autonomy and also collaborate with others to generate ideas and refine concepts for implementation.