Student Program Information 2020

Certificate IV in Cyber Security (22334VIC)

The Certificate IV in Cyber Security is a technician level qualification that will provide graduates with the knowledge and a comprehensive set of technical skills that enables them to:

- monitor the risk of cyber security attacks
- implement appropriate software
- use a range of tools and procedures to mitigate cyber security threats
- protect an organisation from insider security breaches
- develop systems to minimise network vulnerabilities and risks.

Graduates of the course will be able to seek employment as cyber security practitioners in a range of commercial enterprises/organisations and government bodies.

The recommended study plan will require 12 months of study to complete

Subsidised Training

- You may be eligible for government subsidised training based on your employment and training level.
- For full details, including visa eligibility, please see the Skills SA website
- While this course may attract government subsidies, there may also be upfront fees, depending on any required underpinning knowledge and skills.
- **ALL STUDENTS, IRRESPECTIVE OF PREVIOUS STUDIES, WILL BE REQUIRED TO DO THE CORE SKILLS PROFILE FOR ADULTS (CSPA) BEFORE THEY ARE ELIGIBLE FOR GOVERNMENT SUBSIDY.**

Student Program Information 2020

IT Studies Subjects

This qualification was developed in close collaboration with a range of industry partners, including NBN Co, Cisco Australia and New Zealand, BAE Systems, Telstra, Deloitte, TAFEs and others. The information below refers to the TAFE SA IT Studies subjects and outlines the competencies that makes up those subjects. Your final official results will refer to the competencies listed below.

Course Admission Requirements

- Satisfactory demonstration of reading, writing and numeracy skills by undertaking the Core Skills Profile for Adults (CSPA)
- Current Working with Children Check and Police Checks will be required if a student undertakes work placement, work experience or employment in this field

Assumed Skills and Knowledge

Participants would be best equipped to achieve the course outcomes if they have the learning, reading, writing and literacy, and numeracy competencies to Level 3 of the Australian Core Skills Framework (ACSF). See http://education.gov.au/search/site/ACSF. Applicants who have a lower level of language, literacy and numeracy skills may require additional support to successfully complete the course.

This qualification assumes basic computer literacy skills.

Incidentals

This course also has an incidental cost of $400.00 for 512Gb SSD portable hard drive, headset with microphone, National Police Clearance and a Raspberry Pi for use in subjects requiring an IoT device.

Hardware & Software

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

It is important to note that for students studying this course online (externally) it will be assumed that you have the hardware required to run the required resources. It is recommended that you have the following as a minimum;

- Intel i5 CPU (or equivalent AMD)
- 16GB of RAM
- 1Tb SSD
- Internet Access

Internet

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. Downloading these virtual machines from the Internet may vary depending on your Internet connection speed.

Student Program Information 2020

Required Competencies

Certificate IV in Cyber Security

National Code: 22334VIC TAFE SA Code: AC00088

This table shows the competencies that you must have on your academic record to achieve this qualification and the IT subjects you would complete.

IT Studies Subject	National Code	Unit Name	Assumed Knowledge and Skills
4CYNET	**Networking Fundamentals for Cyber Security**		
	VU21988	Utilise basic network concepts and protocols required in cyber security	
4CYACI	**Analyse and Communicate Information**		
	BSBRES401	Analyse and present research information	
	RIICOM301D	Communicate information	
4CYCSF	**Cyber Security Fundamentals**		
	VU21990	Recognise the need for cyber security in an organisation	
4CYBCS	**Basic IT Skills for Cyber Security**		
	VU21993	Secure a networked personal computer	
4CYWHS	**WH&S for Cyber Security**		
	BSBWHS401	Implement and monitor WHS policies, procedures and programs to meet legislative requirements	
4CEP	**Copyright, Ethics and Privacy**		
	ICTICT418	Contribute to copyright, ethics and privacy in an ICT environment	
4CYITS	**Introduction to Scripting**		
	ICTPRG407	Write script for software applications	
4CYDAT	**Introduction to Data collection and Analysis**		
	VU21994	Perform basic cyber security data analysis	
4CYSEC	**Network Security**		4CYNET
	VU21991	Implement network security infrastructure for an organisation	4CYCSF
4CYMAN	**Manage System Security**		
	VU21995	Manage the security infrastructure for the organisation	
4CYTST	**System Testing Procedures**		
	VU21989	Test concepts and procedures for cyber security	
4CYWEB	**Website Security**		
	VU21997	Expose website security vulnerabilities	

4CYIRP	**Incident Response Plan**		
	VU21996	Evaluate and test an incident response plan for an enterprise	
4CYPRO	**Cyber Security Industry Project**		4CYITS 4CYNET 4CYTST 4CYCSF
	VU21992 ICTSAS409	Develop a cyber security industry project Manage risks involving ICT systems and technology	

Student Program Information 2020

Subject Descriptions

Subject	Description
4CYNET	This subject introduces the skills and knowledge required to comprehend how data transmits through a network, covering the function and operation of protocols such as the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and the devices that facilitate this transmission.
4CYACI	This subject provides the skills and knowledge required to gather, organise, analyse and present workplace information, including identifying research requirements and sources of information, applying information to a set of facts, evaluating the quality of the information, and preparing and producing reports.
4CYCSF	This subject provides introductory knowledge and skills to recognise threats, risks and vulnerabilities to cyber security in an organisation. It includes vulnerabilities an organisation is exposed to for networks, computers, applications, data, users and infrastructure. This will include an introduction to common cyber security attack mechanisms and an introduction to identity and threat management as well as security issues surrounding Internet of Things (IOT) devices.
4CYBCS	This subject provides the skills and knowledge to configure an operating system on a personal computer, adding security, setting user level passwords and privileges to limit and identify user access. There will also be an overview of Internet Of Things (IOT) devices, an introduction to computer networking virtualisation and base level Linux commands, using both KALI and UBUNTU.
4CYWHS	This subject describes the skills and knowledge required to implement and monitor an organisation's work health and safety (WHS) policies, procedures and programs in the relevant work area in order to meet legislative requirements.
4CEP	This subject involves maintaining 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.
4CYITS	This subject introduces the skills and knowledge required to plan, design and build scripts, using PYTHON as the scripting language that is highly sort after in the cyber security field. This will include use of libraries such as python-nmap to automate functions such as the identification of open ports and services available on a network host thus helping to build a map of a network to identify potential security vulnerabilities.
4CYDAT	This subject introduces knowledge and skills necessary for cyber security professionals to detect and recognise patterns by performing data analysis. Learn how to look for vulnerabilities using SPLUNK an industry leading Security Information and Event Management (SIEM) solution which is used in many Security Operation Centers (SOC).
4CYSEC	This subject will provide a sound working knowledge of the features of the Fortinet product FortiGate that will support the network security for an organisation. This includes threat inspection and mitigation techniques, network security architectures, introduction to firewall setup and configuration, intrusion prevention system (IPS) setup and operation as well as internetworking operating system (IOS) software features to harden routers and switches. The unit also investigates proxy server vulnerabilities, Wireless Lan (WLAN) security vulnerabilities and the application of Virtual Private Networks (VPN's) and cryptography fundamentals.
4CYMAN	This subject provides the basic knowledge and skills required to manage the implementation of the security infrastructure for an organisation. It includes assessing risk, control implementation, monitoring effectiveness, organisation policy for storage of audit data and reporting, monitor and evaluate physical security infrastructure of the organisation and implement a regular security maintenance program.
4CYTST	This subject provides introductory skills and knowledge required to implement testing procedures for systems in an organisation. These involve application layer testing tools as defined by the Open Web Application Security Project (OWASP), network testing and monitoring tools. The subject examines

	common threats, ethical hacking principles and introduction to penetration testing, social engineering security issues, enumeration, port scanning, sniffers, footprinting, traffic sniffers and wireless LAN vulnerabilities and contains a solid treatment of intrusions.
4CYWEB	This subject provides the knowledge and skills required to ensure and maintain the security of an organisation's website by utilising the outcomes of the Open Web Application Security Project (OWASP). Current penetration testing tools are also utilised to determine the vulnerabilities of a web site. Vulnerabilities are assessed and reported to appropriate personnel to minimise risk.
4CYIRP	This subject provides the basic knowledge and skills for a cyber security practitioner to examine, as part of a team, an organisation's existing incident response plan (IRP) and expand it as necessary to more thoroughly deal with incidents. The unit includes forming the team, clarifying roles, interpreting an incident response plan (IRP), using red and blue teams to test the IRP, implementing an incident, evaluating the IRP for its effectiveness and developing improvement.
4CYPRO	Students will then undertake a project that simulates a real cyber security environment. The project may include using a Cyber Security Operations Centre (CSOC) sandbox or equivalent laboratory environment. This environment allows the participant to demonstrate configuring and testing of firewalls, implementing Intrusion Detection System (IDS) and evaluating and identifying any traffic anomalies. The use of Red & Blue teaming exercises to identify security breaches and apply mitigation strategies to minimise further risk should be included as part of the exercise. This subject will also describe the skills and knowledge required to implement procedures that identify, analyse, evaluate and monitor risks involving information and communications technology (ICT) systems and technology. This includes the development and management of contingency plans.

Student Program Information 2020

Choosing a Study Plan

TAFE SA Study Plan for Full-Time Students (12 months)

Option 1

The following table shows the optional study plan for the Certificate IV of Cyber Security (22334VIC) which allows students to complete 3 months earlier. Each stage is one semester (or 6 months) in length for Full-Time student*.

These are eligible for subsidy under WorkReady

Stage 1		Stage 2	
Term 1	**Term 2**	**Term 1**	**Term 2**
Subjects required to complete the Certificate IV qualification			
4CYNET (4) 4CYBCS (4) 4CYITS (2)		4CYSEC (4) 4CYMAN (2) 4CYPRO (4)	
4CYCSF (4) 4CEP (2) Tutorial (4)	4CYWHS (2) 4CYDAT (2) 4CYACI (4) Tutorial (2)	4CYWEB (4) 4CYTST (4) Tutorial (2)	4CYIRP (4) Tutorial (2)
(20)	(20)	(20)	(18)

Please Note: This program structure is subject to change.

Legend:

* The length of time for Part-Time students will depend on the number of subjects studied in each semester.

( ) The number in brackets after the subject is the indicative number of contact hours per week that you expect to study at a TAFE SA campus for that subject.

NOTE: The study plan is for a full-time student with class-attendance.

Student Program Information 2020

TAFE SA Study Plan for Full-Time Students (15 months)

Option 2

The following table shows an alternate study plan for the Certificate IV of Cyber Security (22334VIC), that will give a reduced study load per term, while still enabling you to remain a Full-Time student*.

These are eligible for subsidy under WorkReady

Stage 1		Stage 2		Stage 3
Term 1	**Term 2**	**Term 1**	**Term 2**	**Term 1**
Subjects required to complete the Certificate IV qualification				
4CYNET (4) 4CYBCS (4) 4CYITS (2)		4CYSEC (4) 4CYMAN (2)		4CYPRO (4) 4CYWHS (2) 4CYIRP (4) Tutorial (6)
4CYCSF (4) Tutorial (4)	4CYDAT (2) 4CYACI (4) Tutorial (2)	4CYWEB (4) 4CYTST (4) Tutorial (2)	4CYPRO (4) 4CEP (2) Tutorial (4)	
(16)	(18)	(18)	(16)	(16)

Please Note: This program structure is subject to change.

Legend:

* The length of time for Part-Time students will depend on the number of subjects studied in each semester.

( ) The number in brackets after the subject is the indicative number of contact hours per week that you expect to study at a TAFE SA campus for that subject.

NOTE: The study plan is for a full-time student with class-attendance.

Click here to apply for this qualification