

## CHIEF INFORMATION SECURITY OFFICER

BRANCH/UNIT	Information and Communications Technology (ICT)		
TEAM	Security		
LOCATION	TBA		
CLASSIFICATION/GRADE/BAND	Senior Executive (Equivalent PSSE Band 1)		
POSITION NO.	TBA		
ANZSCO CODE	262112	PCAT CODE	2226368
TAFE Website	<a href="http://www.tafensw.edu.au">www.tafensw.edu.au</a>		

### 1. ORGANISATIONAL ENVIRONMENT

TAFE NSW's purpose is to skill the workforce of the future. It is Australia's leading provider of vocational education and training with over 500,000 annual enrolments and a proud history for setting the benchmark for quality service. As the NSW public provider, it supports the NSW Government's priority to grow skills for the economy and jobs of tomorrow. Critically, TAFE NSW plays a vital role in providing vocational education in rural and regional NSW, and job training pathways for the most vulnerable in the community.

TAFE NSW offers the best of campus-based delivery as well as flexible, online and work-based learning. The TAFE NSW values of Customer First, Collaboration, Integrity and Excellence guide our team in strengthening communities, delivering world-class training for our students and producing job ready graduates for employers. The operating environment for TAFE NSW is dynamic as we leverage our scale, expertise, passion and reputation to meet the rapidly changing VET landscape.

TAFE NSW is committed to its students and customers and the role it plays in changing lives and opening up opportunities through learning.

### 2. POSITION PURPOSE

The Chief Information Security Officer (CISO) is responsible for driving the development, implementation and support of ICT best practice standards and ensuring compliance to deliver secure and reliable systems. The CISO develops and implements TAFE NSW's information technology (IT) security strategy whilst protecting the business from information security breaches and cyber environment threats.

### 3. KEY ACCOUNTABILITIES

1. Identify and analyse TAFE NSW and sector IT security issues to ensure compliance with business, statutory and legislative obligations.
2. Develop, maintain and implement TAFE NSW's ICT security strategy, governance framework, architecture and practice to drive the provision of secure ICT services, which support business outcomes through effective risk management strategies.
3. Lead, develop and communicate innovative ICT cyber and information security policy, standards, training and compliance systems to drive awareness and secure use of information systems.
4. Manage, measure and monitor information security threats, incidents and investigations to ensure the timely response and containment of security issues.
5. Provide expert, authoritative and professional advice to the Chief Information Officer and senior management on ICT security matters to inform and influence decisions that effectively enhance systems security and minimise risk.
6. Ensure alignment of information security strategies with business objectives, collaborating with stakeholders on TAFE NSW's overall business continuity and disaster recovery strategies.
7. Drive implementation of a comprehensive program of security management audits and controls, including vulnerability testing, ensuring proactive identification and assessment of threats, weaknesses and non-conformance to effectively address current and future risks.
8. Manage financial budgeting, reporting and resourcing to achieve service delivery outcomes and savings targets.
9. By example, lead the development of a safe, healthy and inclusive work environment, including implementation and review of appropriate strategies and measures.
10. Place the customer at the centre of all decision making.
11. Build and develop a high performance team, aligned to the core values of integrity, collaboration, excellence and a customer first attitude, through effective leadership, support and feedback.
12. Collaborate with staff to ensure the development and regular review of meaningful individual performance management and development plans that are clearly aligned to strategic objectives and focused to develop the individual.

### 4. KEY CHALLENGES

- Engaging and influencing stakeholders to ensure relevant ICT security governance frameworks and risk management practices are effectively implemented.
- Responding appropriately to threats as they emerge in a context where disciplines around security and risk management are evolving.
- Embedding a consistent and high level of ICT security protection and risk mitigation practice across TAFE NSW as a mainstream operational standard.
- Proactively and responsively managing both the diversity and complexity of security matters and associated risk in a commercially sensitive business delivery context.
- Providing high-level risk informed advice on IT security strategies and solutions that both minimizes threats and business services delivery disruption.

## 5. KEY RELATIONSHIPS

WHO	WHY
<b>Internal</b>	
Chief Information Officer	<ul style="list-style-type: none"> <li>Receive leadership, advice and support.</li> <li>Provide expert strategic and technical advice to influence decisions regarding ICT security initiatives and innovation.</li> <li>Alert to significant issues, providing risk informed advice and options to address.</li> </ul>
Direct reports	<ul style="list-style-type: none"> <li>Provide leadership, advice and support.</li> <li>Guide on decisions and actions regarding implementation of security and risk management strategies.</li> <li>Support with complex issues management and resolutions.</li> </ul>
TAFE NSW Executive and senior management level committees and forums	<ul style="list-style-type: none"> <li>Provide information and reporting on IT security related issues and activities.</li> <li>Build awareness and knowledge on IT security issues, innovations and trends to assist inform business planning, strategies and operational decision making.</li> </ul>
TAFE NSW corporate services and business managers and stakeholders	<ul style="list-style-type: none"> <li>Provide expert advice and guidance on IT security and cyber threat issues.</li> <li>Support with awareness of IT security risks and embedding practical approaches to minimising risk.</li> </ul>
TAFE NSW managers and staff	<ul style="list-style-type: none"> <li>Provide communications and access to documents and resources to build awareness and assist with IT security related policies, processes and practices.</li> </ul>
<b>External</b>	
Specialist contractors and services providers	<ul style="list-style-type: none"> <li>Manage relationships, provide work specifications and oversee performance.</li> </ul>
Whole of government ICT forums	<ul style="list-style-type: none"> <li>Build networks, share learnings and optimise synergies to deliver improved IT security management strategies and practices.</li> <li>Work with central agencies and other clusters to collaborate on initiatives and strategies of benefit to the sector and to TAFE NSW.</li> </ul>

## 6. POSITION DIMENSIONS

**Reporting Line:** Chief Information Officer

**Direct Reports:** x 3

**Indirect Reports:** 11

**Financial delegation:** Up to \$150,000 or as updated by the TAFE NSW Financial Delegations applying at the time.

**Budget/Expenditure:** TBA

TAFENSW.EDU.AU

**Decision Making:**

- Makes decisions on highly complex and sensitive issues where there may be no readily available source of advice and guidance and outcomes may break new ground for the organisation.
- Manage functional expenditure and resourcing within relevant policy and delegation frameworks.
- Matters requiring a higher level of approval are referred to the Reporting Line Manager.

## 7. ESSENTIAL REQUIREMENTS

1. Degree qualification in related field or equivalent significant experience.
2. Demonstrated experience developing and implementing an enterprise level IT security strategy for a large and diverse organisation.
3. Proven record of achievement addressing IT security issues, protecting against cyber threats and effectively managing associated risks.
4. Significant experience providing strategic management advice based on professional knowledge and expertise in ICT security and embedding best practice standards in operations.
5. Ability to address and meet focus capabilities as stated in the Position Description.





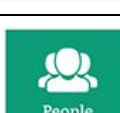
## 8. CAPABILITIES

**NSW Public Sector Capability Framework**

Below is the full list of capabilities and the level required for this role as per the [NSW Public Sector Capability Framework](#). The capabilities **in bold** are the focus capabilities for this role. Refer to the next section for further information about the focus capabilities.

Capability levels are as follows and reflect a progressive increase in complexity and skill:

Foundational > Intermediate > Adept > Advanced > Highly Advanced

CAPABILITY GROUP	NAME	LEVEL
 Personal Attributes	Display Resilience & Courage	Advanced
	Act with Integrity	Advanced
	<b>Manage Self</b>	<b>Highly Advanced</b>
	Value Diversity	Intermediate
 Relationships	Communicate Effectively	Advanced
	Commit to Customer Service	Adept
	<b>Work Collaboratively</b>	<b>Advanced</b>
	<b>Influence and Negotiate</b>	<b>Advanced</b>
 Results	Deliver Results	Advanced
	Plan And Prioritise	Adept
	<b>Think and Solve Problems</b>	<b>Advanced</b>
	<b>Demonstrate Accountability</b>	<b>Advanced</b>
 Business Enablers	Finance	Adept
	<b>Technology</b>	<b>Highly Advanced</b>
	Procurement and Contract Management	Adept
	Project Management	Adept
 People Management	Manage and Develop People	Adept
	Inspire Direction and Purpose	Adept
	<b>Optimise Business Outcomes</b>	<b>Advanced</b>
	Manage Reform and Change	Advanced

### Occupation / profession specific capabilities

Capability Set	Category, Sub-category and Skill	Level and Code
	Strategy and Architecture – Information Strategy Information Governance	Level 5 – IRMG
	<b>Strategy and Architecture – Advice and Guidance Specialist Advice</b>	<b>Level 5 – TECH</b>
	Strategy and Architecture – Business Strategy and Planning Business Risk Management	Level 5 - BURM
	<b>Strategy and Architecture – Information Strategy Information Security</b>	<b>Level 6 – SCTY</b>
	<b>Delivery and Operation – Service Operation Security Administration</b>	<b>Level 6 – SCAD</b>
	<b>Delivery and Operation – Service Operation Penetration Testing</b>	<b>Level 6 – PENT</b>
	Skills and Quality – Quality Conformance Conformance Review	Level 5 - CORE

**FOCUS CAPABILITIES**

The focus capabilities for the Chief Information Security Officer are the capabilities in which occupants must demonstrate immediate competence. The behavioural indicators provide examples of the types of behaviours that would be expected at that level and should be reviewed in conjunction with the position’s key accountabilities.

**NSW Public Sector Focus Capabilities**

NSW Public Sector Capability Framework		
Group and Capability	Level	Behavioural Indicators
<b>Personal Attributes</b> Manage Self	Highly Advanced	<ul style="list-style-type: none"> <li>Promote and model the value of self-improvement and be proactive in seeking opportunities for growth.</li> <li>Actively seek, reflect and integrate feedback to enhance own performance, showing a strong capacity and willingness to modify own behaviours.</li> <li>Manage challenging, ambiguous and complex issues calmly and logically.</li> <li>Model initiative and decisiveness.</li> </ul>
<b>Relationships</b> Work Collaboratively	Advanced	<ul style="list-style-type: none"> <li>Build a culture of respect and understanding across the organisation.</li> <li>Recognise outcomes which resulted from effective collaboration between teams.</li> <li>Build co-operation and overcome barriers to information sharing and communication and collaboration across the organisation and cross government.</li> <li>Facilitate opportunities to engage and collaborate with external stakeholders to develop joint solutions.</li> </ul>
<b>Relationships</b> Influence and Negotiate	Advanced	<ul style="list-style-type: none"> <li>Influence others with a fair and considered approach and present persuasive counter-arguments.</li> <li>Work towards mutually beneficial win/win outcomes.</li> <li>Show sensitivity and understanding in resolving acute and complex conflicts.</li> <li>Identify key stakeholders and gain their support in advance.</li> <li>Establish a clear negotiation position based on research, a firm grasp of key issues, likely arguments, points of difference and areas for compromise.</li> <li>Pre-empt and minimise conflict within the organisation and with external stakeholders.</li> </ul>
<b>Results</b> Think and Solve Problems	Advanced	<ul style="list-style-type: none"> <li>Undertake objective, critical analysis to draw accurate conclusions that recognise and manage contextual issues.</li> <li>Work through issues, weigh up alternatives and identify the most effective solutions.</li> <li>Take account of the wider business context when considering options to resolve issues.</li> <li>Explore a range of possibilities and creative alternatives to contribute to systems, process and business improvements.</li> <li>Implement systems and processes that underpin high quality research and analysis.</li> </ul>
<b>Results</b> Demonstrate Accountability	Advanced	<ul style="list-style-type: none"> <li>Design and develop systems to establish and measure accountabilities.</li> </ul>

TAFENSW.EDU.AU

## NSW Public Sector Capability Framework

Group and Capability	Level	Behavioural Indicators
		<ul style="list-style-type: none"> <li>• Ensure accountabilities are exercised in line with government and business goals.</li> <li>• Exercise due diligence to ensure work health and safety risks are addressed.</li> <li>• Oversee quality assurance practices.</li> <li>• Model the highest standards of financial probity, demonstrating respect for public monies and other resources.</li> <li>• Monitor and maintain business unit knowledge of and compliance with legislative and regulatory frameworks.</li> <li>• Incorporate sound risk management principles and strategies into business planning.</li> </ul>
<b>Business Enablers</b>		
Technology	Highly Advanced	<ul style="list-style-type: none"> <li>• Encourage research and expert advice on the application of emerging technologies to achieve organisational outcomes.</li> <li>• Ensure that effective governance frameworks are in place to enable efficient and effective application of information and communication technology within the organisation.</li> <li>• Establish effective governance to ensure organisational compliance with information and communications security and use policies.</li> <li>• Critically assess business cases supporting the introduction of technology solutions to improve the efficiency and effectiveness of the organisation.</li> <li>• Ensure that effective policy and procedural disciplines are in place for records, information and knowledge management to meet both government and organisational requirements.</li> </ul>
<b>People Management</b>		
Optimise Business Outcomes	Advanced	<ul style="list-style-type: none"> <li>• Develop workforce plans that effectively distribute organisational resources to achieve business goals.</li> <li>• Plan for strategic use of human resources that links to wider organisational aims and goals.</li> <li>• Encourage others to strive for ongoing performance improvement.</li> <li>• Align systems and processes to encourage improved performance and outcomes.</li> </ul>

### Occupation specific capability set (Skills Framework for the Information Age – SFIA 7)

Category and Sub-Category	Level and Code	Level Descriptions
Strategy and Architecture - Advice and Guidance, Specialist Advice	Level 5 – TECH	Actively maintains recognised expert level knowledge in one or more identifiable specialisms. Provides definitive and expert advice in their specialist area(s). Oversees the provision of specialist advice by others, consolidates expertise from multiple sources, including third party experts, to provide coherent advice to further organisational objectives. Supports and promotes the development and sharing of specialist knowledge within the organisation.

Occupation specific capability set (Skills Framework for the Information Age – SFIA 7)		
Category and Sub-Category	Level and Code	Level Descriptions
<b>Strategy and Architecture –</b> Information Strategy Information Security	Level 6 - SCTY	Develops and communicates corporate information security policy, standards and guidelines. Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and pro-actively assesses impact on business strategies, benefits and risks. Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with experts in other functions such as legal, technical support. Ensures architectural principles are applied during design to reduce risk and drives adoption and adherence to policy, standards and guidelines.
<b>Delivery and Operation –</b> Service Operation Security Administration	Level 6 - SCAD	Develops policies, standards, processes, guidelines for ensuring the physical and electronic security of automated systems. Ensures that the policy and standards for security administration are fit for purpose, current and are correctly implemented. Reviews new business proposals and provides specialist advice on security issues and implications.
<b>Delivery and Operation –</b> Service Operation Penetration Testing	Level 6 - PENT	Takes a comprehensive approach to seeking vulnerabilities across the full spectrum of organisation policies, processes, and defences in order to improve organisational readiness, improve training for defensive practitioners, and inspect current performance levels. Determines testing policy, and owns the supporting processes. Takes responsibility for the management of all vulnerability testing activities within the organisation. Assesses and advises on the practicality of testing process alternatives. Initiates improvements to test processes and directs their implementation. Assesses suppliers' development and testing capabilities. Manages client relationships with respect to all testing matters.