

SENIOR CYBER SECURITY ANALYST

BRANCH/UNIT	Systems Group		
TEAM	Security		
LOCATION	Negotiable		
CLASSIFICATION/GRADE/BAND	TAFE Manager Level 1		
POSITION NO.	TBA		
ANZSCO CODE	262112	PCAT CODE	1226368
TAFE Website	www.tafensw.edu.au		

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 Senior Cyber Security Analyst is responsible for developing and implementing cyber security strategy, frameworks, policies and guidelines; governing compliance with TAFE cyber security policies and NSW Government Cyber Security Policy; and providing cyber security advice, conducting assessments and reviews, ensuring that TAFE NSW successfully manages its compliance, legal and regulatory obligations.

3. KEY ACCOUNTABILITIES

1. Provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls and performs security risk, vulnerability assessments, and business impact analysis for medium complexity information systems to ensure the risk of cyberattacks are identified and control measures are implemented.
2. Develops cyber security strategy/ policies / standards / guidelines in order to ensure the physical and electronic security of automated systems.
3. Conduct regular research and evaluation including the use of forensics, emerging cyber security threats and assess the most appropriate strategies and techniques to manage risks.
4. Reviews new business proposals and provides specialist advice and support for planning disaster recovery initiatives to ensure business continuity in the event of any security breaches.
5. Provides technical insight to inform the development of policies, standards and guidelines that contribute to a culture that supports system and network protection in order to ensure that policy and standards for security are fit for purpose.
6. Monitors the application and compliance of security administration procedures and reviews information systems for actual or potential breaches in security.
7. Ensures that security records are accurate and complete to ensure requests for support are dealt with according to set standards and procedures.
8. Performs internal and coordinates external security audits, identifying areas at risk and recommending on solutions to ensure systems integrity.
9. Provides technical guidance and advice to security analysts relating to more complex security investigations to ensure robust and technically informed outcomes are determined.
10. Govern and monitor vendors to ensure cyber security controls are implemented, monitored, measured and audited.
11. Reflect TAFE NSW's values in the way you work and abide by policies and procedures to ensure a safe, healthy and inclusive work environment.
12. Place the customer at the centre of all decision making.
13. Work with the Line Manager to develop and review meaningful performance management and development plans.

4. KEY CHALLENGES

- Maintain a contemporary knowledge of developments in cyber security and technology developments.
- Maintain an advanced knowledge of complex analytic tools to determine emerging threat patterns and vulnerabilities.
- Maintain a strong focus on continuous improvement in an environment driven by technology development and tight deadlines.
- Ensuring architectural principles are applied during design to reduce risk and drive adoption and adherence to policy, standards and guidelines.

5. KEY RELATIONSHIPS

WHO	WHY
Internal	
Manager Cyber Security	<ul style="list-style-type: none"> • Receive leadership direction and advice • Escalate contentious or issues that require high level intervention. • Consult on sensitive matters that require immediate response.
Stakeholders/Internal Clients	<ul style="list-style-type: none"> • Liaise in relation to cyber security issues and provide future recommendations. • Consult on the development of new approaches and policy development to support network and system security. • Provide cyber security advise, conduct assessment and reviews. • Engage with cyber security operations team to ensure security investigations and recommendations are fully informed and address all associated business implications. • Engage with IT commercial team to govern vendors and assure cyber security controls are implemented, monitored, measured and audited.
Work Team	<ul style="list-style-type: none"> • Collaborate across the team and participate in team meetings. • Share knowledge and experience in a security awareness and early intervention environment.
External	
Clients/Vendors	<ul style="list-style-type: none"> • Build and maintain relationships to ensure products and advice support TAFE's security policies and procedures. • Participate in external forums and build partnerships that minimise risks to Systems Group security. • Establish governance procedures ensuring vendors comply with TAFE cyber security policies and procedures, including Essential 8 security mitigation strategies.
NSW Department of Customer Service and Cyber Security Community of Practice	<ul style="list-style-type: none"> • Participate in NSW Cyber Security Community of Practice to help improve information sharing, reporting and threat intelligence with key stakeholders. Ensure compliance with NSW Government Cyber Security Policy.

6. POSITION DIMENSIONS

Reporting Line: Manager Cyber Security

Direct Reports: Nil

Indirect Reports: Nil

Financial delegation: TBA

Budget/Expenditure: TBA

TAFENSW.EDU.AU

Decision Making:

- Makes decisions on complex and sensitive issues that are based on professional judgment, evaluating risks and in the context of a complex and changing environment.
- Matters requiring a higher level of approval are referred to the Reporting Line Manager.

7. ESSENTIAL REQUIREMENTS





1. Degree in relevant discipline or equivalent skills, knowledge and experience.
2. Demonstrated experience in working in a cyber security environment and an awareness of current trends in IT security management.
3. 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	Adept
	Manage Self	Adept
	Value Diversity	Intermediate
 Relationships	Communicate Effectively	Intermediate
	Commit to Customer Service	Adept
	Work Collaboratively	Adept
	Influence and Negotiate	Adept
 Results	Deliver Results	Adept
	Plan And Prioritise	Intermediate
	Think and Solve Problems	Adept
	Demonstrate Accountability	Adept
 Business Enablers	Finance	Intermediate
	Technology	Advanced
	Procurement and Contract Management	Intermediate
	Project Management	Intermediate

Occupation / profession specific capabilities		
Capability Set	Category, Sub-category and Skill	Level and Code
	Strategy & Architecture, Information Strategy, Information Security	Level 4 – SCTY
	Strategy & Architecture, Advice & Guidance, Specialist Advice	Level 5 – TECH
	Delivery & Operation, Service Operation, Security Administration	Level 5 – SCAD

FOCUS CAPABILITIES

The focus capabilities for the Senior Cyber Security Analyst 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
Personal Attributes Display Resilience and Courage	Advanced	<ul style="list-style-type: none"> Stay calm and act constructively in highly pressured and unpredictable environments. Give frank, honest advice in the face of strong, contrary views. Accept criticism of own ideas and respond in a thoughtful and considered way. Welcome new challenges and persist in raising and working through novel and difficult issues. Develop effective strategies and show decisiveness in dealing with emotionally charged situations, difficult and controversial issues.
Relationships Work Collaboratively	Adept	<ul style="list-style-type: none"> Encourage a culture of recognising the value of collaboration. Build co-operation and overcome barriers to information sharing and communication across teams/units. Share lessons learned across teams/units. Identify opportunities to work collaboratively with other teams/units to solve issues and develop better processes and approaches to work.
Results Deliver Results	Adept	<ul style="list-style-type: none"> Take responsibility for delivering on intended outcomes. Make sure team/unit staff understand expected goals and acknowledge success. Identify resource needs and ensure goals are achieved within budget and deadlines. Identify changed priorities and ensure allocation of resources meets new business needs. Ensure financial implications of changed priorities are explicit and budgeted for. Use own expertise and seek others' expertise to achieve work outcomes.
Results Think and Solve Problems	Adept	<ul style="list-style-type: none"> Research and analyse information, identify interrelationships and make recommendations based on relevant evidence. Anticipate, identify and address issues and potential problems and select the most effective solutions from a range of options.

NSW Public Sector Capability Framework

Group and Capability	Level	Behavioural Indicators
		<ul style="list-style-type: none"> Participate in and contribute to team/unit initiatives to resolve common issues or barriers to effectiveness. Identify and share business process improvements to enhance effectiveness.
Business Enablers Technology	Advanced	<ul style="list-style-type: none"> Show commitment to the use of existing and deployment of appropriate new technologies in the workplace. Implement appropriate controls to ensure compliance with information and communications security and use policies. Maintain a level of currency regarding emerging technologies and how they might be applied to support business outcomes. Seek advice from appropriate technical experts to leverage information, communication and other technologies to achieve business outcomes. Implement and monitor appropriate records, information and knowledge management systems protocols, and policies.

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

Category and Sub-Category	Level and Code	Level Descriptions
Strategy & Architecture, Information Strategy, Information Security	Level 4 – SCTY	Explains the purpose of and provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls. Performs security risk, vulnerability assessments, and business impact analysis for medium complexity information systems. Investigates suspected attacks and manages security incidents. Uses forensics where appropriate.
Strategy & Architecture, Advice & 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
Delivery & Operation, Service Operation, Security Administration	Level 5 – SCAD	Monitors the application and compliance of security administration procedures and reviews information systems for actual or potential breaches in security. Ensures that all identified breaches in security are promptly and thoroughly investigated and that any system changes required to maintain security are implemented. Ensures that security records are accurate and complete and that request for support are dealt with according to set standards and procedures. Contributes to the creation and maintenance of policy, standards, procedures and documentation for security.

