

Role Description

Senior Cyber Security Analyst



Role Description Fields	Details
Cluster	Education
Department/Agency	TAFE NSW
Division/Branch/Unit	Digital Solutions Group
Position Description no	10936-01
Classification/Grade/Band	TAFE Manager Level 1
Senior executive work level standards	Not Applicable
OSCA Code	271133
PCAT Code	1226368
Date of Approval	August 2020
Agency Website	www.tafensw.edu.au

Agency overview

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.

Primary purpose of the role

This position 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.

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.

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.

Key relationships

Internal

Who	Why
Line Manager	<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 advice, 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

Who	Why
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.

Role dimensions

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.

Reporting line

Manager Cyber Security

Direct reports

Nil

Budget/Expenditure

TBA

Essential requirements

1. A valid Working with Children Check (required prior to commencement).
2. Degree in relevant discipline or equivalent skills, knowledge and experience.

3. Demonstrated experience in working in a cyber security environment and an awareness of current trends in IT security management.

Capabilities for the role

The [NSW public sector capability framework](#) describes the capabilities (knowledge, skills and abilities) needed to perform a role. There are four main groups of capabilities: personal attributes, relationships, results and business enablers, with a fifth people management group of capabilities for roles with managerial responsibilities. These groups, combined with capabilities drawn from occupation-specific capability sets where relevant, work together to provide an understanding of the capabilities needed for the role.



The capabilities are separated into focus capabilities and complementary capabilities

Focus capabilities

Focus capabilities are the capabilities considered the most important for effective performance of the role. These capabilities will be assessed at recruitment.

The focus capabilities for this role are shown below with a brief explanation of what each capability covers and the indicators describing the types of behaviours expected at each level.

Focus capabilities

Capability group/sets	Capability name	Behavioural indicators	Level
 Personal Attributes	Display Resilience and Courage Be open and honest, prepared to express your views, and willing to accept and commit to change	<ul style="list-style-type: none"> • Remain composed and calm and act constructively in highly pressured and unpredictable environments • Give frank, honest advice in response to 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 and difficult or controversial issues 	Advanced
 Relationships	Work Collaboratively Collaborate with others and value their contribution	<ul style="list-style-type: none"> • Encourage a culture that recognises the value of collaboration • Build cooperation and overcome barriers to information sharing and communication across teams and units • Share lessons learned across teams and units • Identify opportunities to leverage the strengths of others to solve issues and develop better processes and approaches to work • Actively use collaboration tools, including digital technologies, to engage diverse audiences in solving problems and improving services 	Adept



Deliver Results

Achieve results through the efficient use of resources and a commitment to quality outcomes

- Use own and others' expertise to achieve outcomes, and take responsibility for delivering intended outcomes
- Make sure staff understand expected goals and acknowledge staff success in achieving these
- Identify resource needs and ensure goals are achieved within set budgets and deadlines
- Use business data to evaluate outcomes and inform continuous improvement
- Identify priorities that need to change and ensure the allocation of resources meets new business needs
- Ensure that the financial implications of changed priorities are explicit and budgeted for

Adept



Think and Solve Problems

Think, analyse and consider the broader context to develop practical solutions

- Research and apply critical-thinking techniques in analysing information, identify interrelationships and make recommendations based on relevant evidence
- Anticipate, identify and address issues and potential problems that may have an impact on organisational objectives and the user experience
- Apply creative-thinking techniques to generate new ideas and options to address issues and improve the user experience
- Seek contributions and ideas from people with diverse backgrounds and experience
- Participate in and contribute to team or unit initiatives to resolve common issues or barriers to effectiveness
- Identify and share business process improvements to enhance effectiveness

Adept



Technology

Understand and use available technologies to maximise efficiencies and effectiveness












- Champion the use of innovative technologies in the workplace
- Actively manage risk to ensure compliance with cyber security and acceptable use of technology policies
- Keep up to date with emerging technologies and technology trends to understand how their application can support business outcomes
- Seek advice from appropriate subject-matter experts on using technologies to achieve business strategies and outcomes
- Actively manage risk of breaches to appropriate records, information and knowledge management systems, protocols and policies

Advanced

Complementary capabilities

Complementary capabilities are also identified from the Capability Framework and relevant occupation-specific capability sets. They are important to identifying performance required for the role and development opportunities.

Note: capabilities listed as 'not essential' for this role are not relevant for recruitment purposes however may be relevant for future career development.

Capability group/sets	Capability name	Description	Level
 Personal Attributes	Act with Integrity	Be ethical and professional, and uphold and promote the public sector values	Adept
 Personal Attributes	Manage Self	Show drive and motivation, an ability to self-reflect and a commitment to learning	Adept
 Personal Attributes	Value Diversity and Inclusion	Demonstrate inclusive behaviour and show respect for diverse backgrounds, experiences and perspectives	Intermediate
 Relationships	Communicate Effectively	Communicate clearly, actively listen to others, and respond with understanding and respect	Intermediate
 Relationships	Commit to Customer Service	Provide customer-focused services in line with public sector and organisational objectives	Adept
 Relationships	Influence and Negotiate	Gain consensus and commitment from others, and resolve issues and conflicts	Adept
 Results	Plan and Prioritise	Plan to achieve priority outcomes and respond flexibly to changing circumstances	Intermediate
 Results	Demonstrate Accountability	Be proactive and responsible for own actions, and adhere to legislation, policy and guidelines	Adept
 Business Enablers	Finance	Understand and apply financial processes to achieve value for money and minimise financial risk	Intermediate
 Business Enablers	Procurement and Contract Management	Understand and apply procurement processes to ensure effective purchasing and contract performance	Intermediate
 Business Enablers	Project Management	Understand and apply effective planning, coordination and control methods	Intermediate

Occupational Specific Complimentary Capabilities

Capability group/sets	Capability name	Description	Level
-----------------------	-----------------	-------------	-------



Information Strategy,
Information Security

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.

Level 4

Advice & Guidance, Specialist
Advice

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

Level 5

Service Operation, Security
Administration

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.

Level 5
