Role Description
Security Operations Officer

Cluster	Transport for NSW
Agency	Transport for NSW
Division/ Branch/ Unit	Corporate Services/ Office of GGM ICT/IT/ Service Assurance and Operations
Classification/ Grade/ Band	USS9
Role Number	Various
ANZSCO Code	262112
PCAT Code	1226492
Date of Approval	July 2020
Agency Website	www.transport.nsw.gov.au

Agency overview

At Transport, we're passionate about making NSW a better place to live, work and visit. Our vision is to give everyone the freedom to choose how and when they get around, no matter where they live. Right now, we're delivering a $51.2bn program – the largest Australia has ever seen – to keep people and goods moving, connect communities and shape the future of our cities, centres and regions. At Transport, we're also committed to creating a diverse, inclusive and flexible workforce, which reflects the community and the customers we serve.

Our organisation – Transport for NSW – is comprised of nine integrated divisions that focus on achieving community outcomes for the greater good and on putting our customers at the centre and our people at the heart of everything we do.

Corporate Services

Corporate Services partner to provide sustainable strategies, solutions and services to enable our clients to deliver with confidence, Transport's vision to make NSW a great place to live, work and play.

Primary purpose of the role

The Security Operations Officer is responsible for providing security operational activities across Transport for NSW IT Service, ensuring secure development and operational practices are in place. This role also undertakes proactive monitoring and coordination of responses to address security alerts and incidents using industry best practice tools and processes.

Key accountabilities

- Develop and implement data security procedures across Solution Design, Development and Runtime to improve Transport for NSW overall security and compliance with data security policies, regulations and best practice.
- Conduct data security assessments, and report on security threats, make recommendations to support security activities across Transport for NSW.

- Implement appropriate end-user controls across TfNSW employee IT devices in consultation with the Security and End User Services Teams to support effective security controls.
- Facilitate security awareness training for all employees involved in Applications Assurance and Operations team and other third party suppliers with information security clearance on the company's information security policies and procedures.
- Participate in compliance and security audits providing evidence of secure processes and procedures in operation.

Key challenges

- Ensuring all technical deliverables are met given the high volume work environment and demands resulting from tight timeframes and competing priorities.
- Establishing and managing relationships with key internal and external stakeholders to ensure the successful delivery of technical deliverables given the complexity that can exist.
- Keeping abreast of current and emerging technologies and best practice in application support.

Key relationships

Who	Why
Internal	
Security Lead	• Escalate issues • Receive guidance and advice • Report on progress against work plans
IT Service Operations and Assurance Team	• Assist with security reviews • Provide security advice • Manage security incidents and risks
Transport Cyber Security Group	• Raise incidents and risks • Represent RDS IT for security incidents • Collaborate and provide insights for security improvement activities
Business Stakeholders	• Provide security advice • Assist with security compliance activities • Provide updates andinformation in regards to security incidents
External	
Application Support and Data Centre Managed Service Providers	• Governance of Security Operations activities and compliance activities • Collaboration on security improvement activities • Security sign-off for changes
Other External Service Providers	• Assist with audit and compliance reviews • Engagement for security services and advice
External Partners such as NSW Cyber Security Group	• Undertake compliance and reporting activities • Attend NSW Cyber Security forums and communities of practice

Role dimensions

Decision making

The Security Operations Officer has some independence in prioritising day to day activities and collaborates with the manager to re-prioritise urgent requests. The role is fully accountable for the quality and integrity of the service provided.

The role defers to the Security Lead complex issues of a technical, legislative or political nature or decisions that will substantially alter the outcome or timeframes, significant issues or conflicts arising in the course duties or matters requiring a higher delegated authority including approval for expenditure or sensitive matters.

Reporting line

The role accounts and reports to the Security Lead

Direct reports

Nil

Budget/Expenditure

Nil

Key knowledge and experience

- Demonstrated experience in adherence to Government data protection regulations and policies in large-scale mission-critical systems.
- Demonstrated experience in ISO 27001 implementations and participating in Compliance and PCI Audits.
- Demonstrated experience in security operations toolsets such as firewalls and intrusion detection/prevention protocols.
- Demonstrated experience in dealing with security aspects of projects in large Corporate or Government organisations.

Capabilities for the role

The NSW Public Sector Capability Framework applies to all NSW public sector employees. The Capability Framework is available at www.psc.nsw.gov.au/capabilityframework

This role also utilises an occupation specific capability set which contains information from the Skills Framework for the Information Age (SFIA). The capability set is available at www.psc.nsw.gov.au/capabilityframework/ICT

Capability summary

Below is the full list of capabilities and the level required for this role. The capabilities in bold are the focus capabilities for this role. Refer to the next section for further information about the focus capabilities.

NSW Public Sector Capability Framework		
Capability Group	**Capability Name**	**Level**
Personal Attributes	Display Resilience and Courage	Intermediate
	Act with Integrity	**Adept**
	Manage Self	**Adept**
	Value Diversity	Intermediate
Relationships	**Communicate Effectively**	**Adept**
	Commit to Customer Service	Intermediate
	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

Focus capabilities

The focus capabilities for the role 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 role's key accountabilities.

NSW Public Sector Capability Framework		
Group and Capability	**Level**	**Behavioural Indicators**
Personal Attributes Act with Integrity	Adept	• Represent the organisation in an honest, ethical and professional way and encourage others to do so • Demonstrate professionalism to support a culture of integrity within the team/unit • Set an example for others to follow and identify and explain ethical issues • Ensure that others understand the legislation and policy framework within which they operate • Act to prevent and report misconduct, illegal and inappropriate behaviour
Personal Attributes Manage Self	Adept	• Look for and take advantage of opportunities to learn new skills and develop strengths • Show commitment to achieving challenging goals • Examine and reflect on own performance

NSW Public Sector Capability Framework		
Group and Capability	**Level**	**Behavioural Indicators**
		• Seek and respond positively to constructive feedback and guidance • Demonstrate a high level of personal motivation
Relationships Communicate Effectively	Adept	• Tailor communication to the audience • Clearly explain complex concepts and arguments to individuals and groups • Monitor own and others' non-verbal cues and adapt where necessary • Create opportunities for others to be heard • Actively listen to others and clarify own understanding • Write fluently in a range of styles and formats
Results Deliver Results	Adept	• 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	• 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 • 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	• 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**
Delivery and Operation Service Operation	Level 5 SCAD	**Security Administration (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.
Strategy and Architecture Information Strategy	Level 5 SCTY	**Information Security (SCTY)** - Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security, and recommends appropriate control improvements. Contributes to development of information security policy, standards and guidelines.