Role Description
Manager Cyber Security Operations Centre

NSW Police Force

Cluster	Stronger Communities
Agency	NSW Police Force
Command/Business Unit	Digital Technology & Innovation
Location	Parramatta
Classification/Grade/Band	CSO 6
ANZSCO Code	262112
PCAT Code	1236492
NSWPF Role Number	
Date of Approval	00/00/0000
Agency Website	www.police.nsw.gov.au

Agency overview

The NSW Police Force (NSWPF) vision is for a *Safe and Secure New South Wales*, which is achieved by police working with the community to reduce violence, crime and fear.

It is one of the largest police forces in the western world, with more than 20,000 NSW Police Force employees, including more than 16,000 sworn officers providing a range of law and order services 24 hours a day, seven days a week to the socially, geographically and culturally diverse community of NSW.

The organisation has four function lines, based across a number of locations. Metropolitan Field Operations and Regional NSW Field Operations provide frontline services directly to the community. Investigations & Counter Terrorism provides investigative, technical and counter terrorism expertise. Corporate Services, provides business support services such as technology and communication, education and training and corporate human resources functions.

The NSW Police Force is a proud employer of a diverse range of people. This includes, but is not limited to, people who identify as Aboriginal or Torres Strait Islander, LGBTIQ, people, with disability, people who come from a variety of cultural, religious or ethnic backgrounds, and workers of all ages. The NSWPF is committed to reflecting the diverse community we serve and creating an inclusive and respectful workplace for all employees, where difference is embraced, contributions are valued, and everyone has a sense of connection and belonging. This enables the growth and development of a talented and diverse workforce across the state, in a wide range of roles, at all levels.

The NSWPF *Statement of Values* and *Code of Conduct & Ethics* outlines appropriate behaviour for all NSW Police Force staff. All employees of NSWPF are expected to ensure ethics are incorporated into all aspects of their work making ethical behaviour, practices and decision making a part of daily routine. This further extends to ensuring confidentiality and information security is maintained at all times.

Work, Health and Safety legislation requires all employees to have specific responsibilities. This role is responsible for ensuring that the work for which their position is responsible is carried out in ways which safeguard the health and safety of all workers.

Primary purpose of the role

The Manager Cyber Security Operations Centre will provide direction and support to a team responsible for operational responses to Cyber Security Threats, Events and Incidents. This role will be key to ensure the

NSW GOVERNMENT

appropriate policies, procedures and technology are in place to ensure that NSWPF is effectively delivering against Events, Alerts and Actions as a feed for the Security Event & Incident Management (SIEM) process. Through the collation of External Threat Intelligence, Vulnerability & Threat assessments, appropriate Security Benchmarking and Research will assist in Managing & Resolving cyber Events and Incidents.

Key accountabilities

- Engage with key stakeholders to ensure the needs of the NSWPF are met in line with Threat Intelligence & Threat Response, compliance with prudential standards and practice guides in relation to cybersecurity and information management
- Assisting Cyber Security to appropriately manage risk profiles, whilst ensuring the control environment is maintained
- Analysis of trends, identify critical threats and opportunities, diagnose problems and issues and recommend appropriate actions
- Identify and resolve network operational and service issues working in partnership with other Telco Authority staff and service providers
- Provide tactical knowledge and advice to the team
- Coordinate, monitor and assure the quality of consolidated performance and status reports
- Provide after-hours response as required for support management activities and actively support management of the performance of the network in a Cyber Event or major incidents

Key challenges

- Demonstrated ability to build trust and strong cross-functional relationships across an organisation to achieve common goals
- Organisational agility and the ability to read the subtle nuances of a situation and react/plan accordingly.

Key relationships

Who	Why
Internal*	
Manager	• Provide expert strategic and technical advice to the CISO to influence decisions regarding ICT initiatives and innovation
Clients/customers	• Provide strategic advice for business improvement • Provide information regarding agency sector wide rules and standards • Ensure compliance with agency and sector rules and standards
Work team	• Represent work group perspective and share information • Lead discussions and decisions regarding implementation of innovation and best practice
External	
Vendors/Service Providers and Consultants	• Communicate needs and resolve issues • Engage with vendors, service providers & consultants

Role dimensions

Decision making

- Carries a high level of autonomy in setting own priorities

- Maintains a degree of independence to develop a suitable approach in managing the workload and provision of advice and recommendations
- Determines own actions undertaken, within government and legislative policies, and for ensuring quality control in the implementation of own workload.
- Ensures recommendations are based on sound evidence, but at times may be required to use their judgment under pressure or in the absence of complete information or as a source of expert advice to internal stakeholders
- As necessary, consults with management on a suitable course of action in matters that are sensitive, high-risk or business-critical

Reporting line

- Chief Information Security Officer (CISO)

Direct reports

- Team Leader Threat Response
- Team Leader Threat Intelligence

Budget/Expenditure

- Nil

Essential requirements

- Obtain and maintain the requisite security clearances for this position.
- Minimum of 5 years in an information security manager role
- Demonstrated experience in information security strategy and policy management
- Strategic acumen and problem-solving skills with the ability to turn findings into executable plans

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**
	Display Resilience and Courage	Adept
	Act with Integrity	**Advanced**
	Manage Self	Adept
	Value Diversity	Adept

NSW Public Sector Capability Framework		
Capability Group	**Capability Name**	**Level**
	Communicate Effectively	Advanced
	Commit to Customer Service	Adept
	Work Collaboratively	Adept
	Influence and Negotiate	**Adept**
	Deliver Results	Adept
	Plan and Prioritise	Adept
	Think and Solve Problems	**Advanced**
	Demonstrate Accountability	**Advanced**
	Finance	Intermediate
	Technology	Adept
	Procurement and Contract Management	**Intermediate**
	Project Management	Intermediate
	**Manage and Develop People**	**Adept**
	Inspire Direction and Purpose	Intermediate
	Optimise Business Outcomes	Adept
	Manage Reform and Change	Adept

Occupation / profession specific capabilities		
Capability Set	**Category, Sub-category and Skill**	**Level and Code**
SFIA	**Strategy and Architecture – Information Strategy** **Information Management**	**Level 5 - IRMG**
	Strategy and Architecture – Business Strategy and Planning **Business Risk Management**	**Level 5 - BURM**
	Strategy and Architecture – Information Strategy **Information Security**	**Level 6 - SCTY**
	Business Change – Relationship Management **Stakeholder Relationship Management**	**Level 5 - RLMT**

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	Advanced	• Model the highest standards of ethical behaviour and reinforce them in others

NSW Public Sector Capability Framework		
Group and Capability	**Level**	**Behavioural Indicators**
		• Represent the organisation in an honest, ethical and professional way and set an example for others to follow • Ensure that others have a working understanding of the legislation and policy framework within which they operate • Promote a culture of integrity and professionalism within the organisation and in dealings external to government • Monitor ethical practices, standards and systems and reinforce their use • Act on reported breaches of rules, policies and guidelines
Relationships Influence and Negotiate	Adept	• Negotiate from an informed and credible position • Lead and facilitate productive discussions with staff and stakeholders • Encourage others to talk, share and debate ideas to achieve a consensus • Recognise and explain the need for compromise • Influence others with a fair and considered approach and sound arguments • Show sensitivity and understanding in resolving conflicts and differences • Manage challenging relations with internal and external stakeholders • Pre-empt and minimise conflict
Results Think and Solve Problems	Advanced	• Undertake objective, critical analysis to draw accurate conclusions that recognise and manage contextual issues • Work through issues, weigh up alternatives and identify the most effective solutions • Take account of the wider business context when considering options to resolve issues • Explore a range of possibilities and creative alternatives to contribute to systems, process and business improvements • Implement systems and processes that underpin high quality research and analysis
Results Demonstrate Accountability	Advanced	• Design and develop systems to establish and measure accountabilities • Ensure accountabilities are exercised in line with government and business goals • Exercise due diligence to ensure work health and safety risks are addressed • Oversee quality assurance practices • Model the highest standards of financial probity, demonstrating respect for public monies and other resources • Monitor and maintain business unit knowledge of and compliance with legislative and regulatory frameworks • Incorporate sound risk management principles and strategies into business planning

NSW Public Sector Capability Framework		
Group and Capability	**Level**	**Behavioural Indicators**
Business Enablers Procurement and Contract Management	Intermediate	• Understand and comply with legal, policy and organisational guidelines and procedures in relation to procurement and contract management • Conduct delegated purchasing activities, complying with prescribed guidelines and procedures • Work with providers, suppliers and contractors to ensure that outcomes are delivered in line with time and quality requirements
People Management Manage and Develop People	Adept	• Define and clearly communicate roles and responsibilities to achieve team/unit outcome • Negotiate clear performance standards and monitor progress • Develop team/unit plans that take into account team capability, strengths and opportunities for development • Provide regular constructive feedback to build on strengths and achieve results • Address and resolve team and individual performance issues, including unsatisfactory performance in a timely and effective way • Monitor and report on performance of team in line with established performance development frameworks

Occupation specific capability set (Skills Framework for the Information Age – SFIA)		
Category, Sub-category	**Level and Code**	**Skill and Level Description**
Strategy and Architecture Information Strategy	Level 5 RMG	**INFORMATION MANAGEMENT (IRMG) –** Drafts and maintains the policy, standards and procedures for compliance with relevant legislation. Understand the implications of information, both internal and external, that can be mined from business systems and elsewhere. Make business decisions based on that information, including the need to make changes to the systems. Reviews new business proposals and provides specialist advice on information management, including advice on and promotion of collaborative working and assessment and management of information-related risk. Creates and maintains an inventory of information assets, which are subject to relevant legislation. Prepares and reviews the periodic notification of registration details and submits it to the relevant regulatory authorities. Ensures that formal information access requests and complaints are dealt with according to approved procedures
Strategy and Architecture Business Strategy and Planning	Level 5 BURM	**BUSINESS RISK MANAGEMENT (BURM) –** Carries out risk assessment within a defined functional or technical area of business. Uses consistent processes for identifying potential risk events, quantifying and documenting the probability of occurrence and the impact on the business. Refers to domain experts for guidance on specialised areas of risk, such as architecture and environment. Co-ordinates the development of countermeasures and contingency plans

Occupation specific capability set (Skills Framework for the Information Age – SFIA)		
Category, Sub-category	**Level and Code**	**Skill and Level Description**
Strategy and Architecture Information Strategy	Level 6 SCTY	**INFORMATION SECURITY (SCTY) –** Provides leadership and guidelines on information assurance security expertise for the organisation, working effectively with strategic organisational functions such as legal experts and technical support to provide authoritative advice and guidance on the requirements for security controls. Provides for restoration of information systems by ensuring that protection, detection, and reaction capabilities are incorporated
Business Change Relationship Management	Level 5 RLMT	**STAKEHOLDER RELATIONSHIP MANAGEMENT (RLMT) –** Develops and maintains one or more defined communication channels and/or stakeholder groups, acting as a single point of contact. Gathers information from the customer to understand their needs (demand management) and detailed requirements. Facilitates open communication and discussion between stakeholders, using feedback to assess and promote understanding of need for future changes in services, products and systems. Agrees changes to be made and the planning and implementation of change. Maintains contact with the customer and stakeholders throughout to ensure satisfaction. Captures and disseminates technical and business information

Version Control

Version	Summary of Changes	Date
V1.0	Position Description translated into Role Description template	09.05.2018

Roles attached

Position Number	Region	Position Number	Region	Position Number	Region	Position Number	Region
50662968							