

# Role Description

## Senior Cyber Security Analyst



Cluster	Stronger Communities
Agency	NSW Police Force
Command/Business Unit	Digital Technology & Innovation, Security
Location	Sydney Olympic Park
Classification/Grade/Band	CSO 4
ANZSCO Code	262112
PCAT Code	1226364
NSWPF Role Number	RD 855
Date of Approval	03/02/2022
Agency Website	<a href="http://www.police.nsw.gov.au">www.police.nsw.gov.au</a>

### Agency overview

The NSW Police Force (NSWPF) vision is for *A Safer New South Wales*, which is achieved by police working with the community to prevent, disrupt and respond to crime.

It is one of the largest police forces in the western world, with more than 20,000 NSW Police Force employees, including more than 17,000 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

This role is responsible for operational responses to Cyber Security Threats, Events and Incidents. It is also responsible for data protection, information security engineering and compliance with information security policies and procedures.

## Key accountabilities

- Establish and implement practices for the monitoring of information systems' logical and physical security to minimise the risk of equipment and data loss, theft or tampering.
- Monitoring of and taking appropriate action based on information from Security information and Event Monitoring (SIEM) platforms that perform log collection, analysis, correlation and alerting reviewing detection capabilities.
- Identify and implement counter-measures or mitigating controls for deployment and implementation in the enterprise network environment
- Collect and maintain information pertinent to security investigations and incidents in a format that supports analysis, situational awareness reporting, and investigation efforts
- Undertake investigations and report on security breaches and incidents to guide the refinement of practices and processes and reduce the likelihood and impact of security related incidents
- Detect, Investigate, respond and report cyber security events

## Key challenges

- Work within an environment where technologies are subject to rapid evolution and change and identify technology solutions and platforms that improve the efficiency and effectiveness of the overall service offering for customers and drive improved value.
- Develop and maintain an active culture of security awareness within the organisation
- Understand the threat landscape and how NSW Police Force should respond to current and emerging threats.

## Key relationships

Who	Why
<b>Internal*</b>	
Manager	<ul style="list-style-type: none"> <li>• Escalate issues, advise and receive instructions</li> <li>• Report on security breaches</li> <li>• Make recommendations for changes and improvements to policy and practice</li> </ul>
Clients/customers	<ul style="list-style-type: none"> <li>• Manage expectations, resolve issues and provide solutions to problems</li> <li>• Educate user population regarding relevant practices and processes</li> </ul>
<b>External</b>	
Suppliers / Vendors	<ul style="list-style-type: none"> <li>• Manage external security threat analysis and testing</li> <li>• Review threats and vulnerabilities</li> <li>• Review and recommend products and services</li> </ul>

## Role dimensions

### Decision making

This role has autonomy to plan own work to meet given objectives and processes, making decisions which influence the success of projects and team objectives in liaison with their manager.

### Reporting line

- Team Leader - Cyber Security Operations Centre – CSO 5

### Direct reports

- Nil

### Budget/Expenditure

- Nil

## Key knowledge and experience

- Experience with IT security management processes and systems, ideally SIEM, and understanding of current Australian regulatory environment and related identity management and security / audit compliance.
- Advanced IT knowledge in databases, operating systems, networking and their security.
- Experience with automation tools and development of security playbooks.

## Essential requirements

- Obtain and maintain the requisite security clearances for this position.
- Tertiary qualifications in a relevant Information Technology discipline or demonstrated experience in security operations
- Ability to respond to cyber incidents and provide coverage 24 hour/7 days per week.

## Capabilities for the role

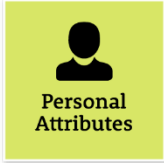

The [NSW public sector capability framework](#) describes the capabilities (knowledge, skills and abilities) needed to perform a role. There are four main groups of capabilities: personal attributes, relationships, results and business enablers, with a fifth people management group of capabilities for 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	<b>Act with Integrity</b> Be ethical and professional, and uphold and promote the public sector values	<ul style="list-style-type: none"> <li>• Represent the organisation in an honest, ethical and professional way and encourage others to do so</li> <li>• Act professionally and support a culture of integrity</li> <li>• Identify and explain ethical issues and set an example for others to follow</li> <li>• Ensure that others are aware of and understand the legislation and policy framework within which they operate</li> <li>• Act to prevent and report misconduct and illegal and inappropriate behaviour</li> </ul>	Adept
	<b>Manage Self</b> Show drive and motivation, an ability to self-reflect and a commitment to learning	<ul style="list-style-type: none"> <li>• Keep up to date with relevant contemporary knowledge and practices</li> <li>• Look for and take advantage of opportunities to learn new skills and develop strengths</li> <li>• Show commitment to achieving challenging goals</li> <li>• Examine and reflect on own performance</li> <li>• Seek and respond positively to constructive feedback and guidance</li> <li>• Demonstrate and maintain a high level of personal motivation</li> </ul>	Adept
 Relationships	<b>Communicate Effectively</b> Communicate clearly, actively listen to others, and respond with understanding and respect	<ul style="list-style-type: none"> <li>• Focus on key points and speak in plain English</li> <li>• Clearly explain and present ideas and arguments</li> <li>• Listen to others to gain an understanding and ask appropriate, respectful questions</li> <li>• Promote the use of inclusive language and assist others to adjust where necessary</li> <li>• Monitor own and others' non-verbal cues and adapt where necessary</li> <li>• Write and prepare material that is well structured and easy to follow</li> <li>• Communicate routine technical information clearly</li> </ul>	Intermediate

FOCUS CAPABILITIES			
Capability group/sets	Capability name	Behavioural indicators	Level
 Results	<b>Plan and Prioritise</b> Plan to achieve priority outcomes and respond flexibly to changing circumstances	<ul style="list-style-type: none"> <li>Consider the future aims and goals of the team, unit and organisation when prioritising own and others' work</li> <li>Initiate, prioritise, consult on and develop team and unit goals, strategies and plans</li> <li>Anticipate and assess the impact of changes, including government policy and economic conditions, on team and unit objectives and initiate appropriate responses</li> <li>Ensure current work plans and activities support and are consistent with organisational change initiatives</li> <li>Evaluate outcomes and adjust future plans accordingly</li> </ul>	Adept
	 Business Enablers	<b>Technology</b> Understand and use available technologies to maximise efficiencies and effectiveness	Adept
	<b>Procurement and Contract Management</b> Understand and apply procurement processes to ensure effective purchasing and contract performance	<ul style="list-style-type: none"> <li>Understand and comply with legal, policy and organisational guidelines and procedures relating to purchasing</li> <li>Conduct delegated purchasing activities in line with procedures</li> <li>Work with providers, suppliers and contractors to ensure that outcomes are delivered in line with time and quality requirements</li> </ul>	Intermediate
	<b>Project Management</b> Understand and apply effective planning, coordination and control methods	<ul style="list-style-type: none"> <li>Perform basic research and analysis to inform and support the achievement of project deliverables</li> <li>Contribute to developing project documentation and resource estimates</li> <li>Contribute to reviews of progress, outcomes and future improvements</li> <li>Identify and escalate possible variances from project plans</li> </ul>	Intermediate

Occupation / profession specific capabilities		
Capability Set	Category, Sub-category and Skill	Level and Code
	Delivery and Operation, Security Service, Security Operations	Level 5 - SCAD
	Strategy and Architecture, Security and Privacy, Information Security	Level 4 - SCTY
	Strategy and Architecture, Security and Privacy, Information Assurance	Level 5 - INAS







NSW Government employees can access the ICT set through the [Skills Framework for the Information Age](#) Foundation website by registering as a corporate user via their NSW Government email address.

## 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.

COMPLEMENTARY CAPABILITIES			
Capability group/sets	Capability name	Description	Level
 Personal Attributes	Display Resilience and Courage	Be open and honest, prepared to express your views, and willing to accept and commit to change	Intermediate
	Value Diversity and Inclusion	Demonstrate inclusive behaviour and show respect for diverse backgrounds, experiences and perspectives	Adept
 Relationships	Commit to Customer Service	Provide customer-focused services in line with public sector and organisational objectives	Adept
	Work Collaboratively	Collaborate with others and value their contribution	Foundational
	Influence and Negotiate	Gain consensus and commitment from others, and resolve issues and conflicts	Intermediate
 Results	Deliver Results	Achieve results through the efficient use of resources and a commitment to quality outcomes	Adept
	Think and Solve Problems	Think, analyse and consider the broader context to develop practical solutions	Intermediate
	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	Not Essential

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

Category, Sub-category	Skill and Level Description	Level and Code
<b>Delivery and Operation, Security Service</b>	<b>Security Operations</b>  Monitors the application and compliance of security operations procedures.  Reviews actual or potential security breaches and vulnerabilities and ensures that they are promptly and thoroughly investigated. Recommends actions and appropriate control improvements.  Ensures that security records are accurate and complete and that requests for support are dealt with according to agreed procedures.  Contributes to the creation and maintenance of policy, standards, procedures and documentation for security.	<b>Level 5 - SCAD</b>
<b>Strategy and Architecture, Security and Privacy</b>	<b>Information Security</b>  Provides guidance on the application and operation of elementary physical, procedural and technical security controls.  Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems.  Identifies risks that arise from potential technical solution architectures. Designs alternate solutions or countermeasures and ensures they mitigate identified risks.  Investigates suspected attacks and supports security incident management.	<b>Level 4 - SCTY</b>



NSW Government employees can access the ICT set through the [Skills Framework for the Information Age](#) Foundation website by registering as a corporate user via their NSW Government email address.

## Version Control

Version	Summary of Changes	Date
V1.0	New Role Description created for new role	16.09.2021

## Roles attached

Position Number	Region	Position Number	Region	Position Number	Region	Position Number	Region
51294949	DTI	51294950	DTI	51294951	DTI	51295328	DTI
51295329	DTI	51295330	DTI	51295331	DTI		