

Role Description

Cyber Security Analyst



Cluster	Stronger Communities
Agency	NSW State Emergency Service
Division/Branch/Unit	Information and Communications Technology
Location	State Headquarters
Classification/Grade/Band	Clerk Grade 7/8
ANZSCO Code	262112
Role Number	52015358
PCAT Code	1122492
Date of Approval	September 2023
Agency Website	www.ses.nsw.gov.au

Agency overview

Our Mission: NSW SES saving lives and protecting communities.

Our Vision: Be the best volunteer emergency service agency in Australia.

The NSW State Emergency Service (NSW SES) is an emergency and rescue service made up almost entirely of volunteers and supported by a small staff contingent. NSW SES is a key influencer of other emergency service agencies and works closely with these partners to modernise and grow volunteering to save lives and protect communities

While major responsibilities are for flood, storm operations and tsunamis, the NSW SES also provides the majority of general rescue effort in the rural parts of the state. This includes road accident rescue, vertical rescue, bush search and rescue, evidence searches (both metropolitan and rural), other forms of specialist rescue that may be required due to local threats, Urban Search and Rescue and Community First Response.

Primary purpose of the role

The Cyber Security Analyst manages the governance and administration of the organisation's information and data security policies and practices to ensure authorised users can readily access information and that the information is protected in terms of confidentiality, integrity, and availability from internal or external security threats and incidents.

Key accountabilities

- Monitor and report on the performance of network, system and application security solutions to highlight areas of non-compliance and inform the development of improved practices and processes.
- Manage the allocation of access privileges of users to ensure appropriate security settings are applied in accordance with organisation policies and application owner-defined parameters
- Lead the security breach investigation process to ensure minimal disruption to business and to guide the refinement of information security policies and practices

- Manage the periodic maintenance of security systems and applications to ensure new threats are identified and managed and the security of the organisation's assets are maintained
- Develop and maintain the set of policies and procedures that form NSW SES Information Security Management System (ISMS) for systematically managing the organisations sensitive data to ensure compliance with NSW Government Security strategy and policies
- Coordinate ongoing security awareness programs for staff and volunteers to ensure compliance with security policy and procedures

Key challenges

- Maintaining currency of knowledge regarding the information security environment and the range of options available to secure the organisation's assets.
- Exercising judgement, analysing, and interpreting complex security issues and challenges, evaluating impacts and determining responses.

Key relationships

Who	Why
Internal	
Senior Manager	<ul style="list-style-type: none"> ▪ Escalate issues, advise, and receive instructions. ▪ Report on security system performance ▪ Provide input to recommendations for changes and improvements to policy and practice
Work team	<ul style="list-style-type: none"> ▪ Work collaboratively to contribute to achieving organisation's business goals ▪ Participate in meetings to obtain the work group perspective and share information ▪ Provide advice and guidance on security matters
External	
Suppliers/ Vendors	<ul style="list-style-type: none"> ▪ Coordinate security threat analysis and testing ▪ Review threats and vulnerabilities ▪ Review products and services
Security Community	<ul style="list-style-type: none"> ▪ Represent NSW SES at NSW Government security forums

Role dimensions

Decision making

The role;

- Exercises considerable autonomy, judgement and initiative in resolving day-to-day cyber security issues that arise from service provision to the Director and stakeholders.
- Seeks input of others to find and recommend appropriate solutions, considering impacts and risks.

- Defers and escalates decisions to the Senior Manager and/or Director including approval for change, assignment of tasks within directorate, budget expenses, and major decisions related to cyber security.

Reporting line

The role reports directly to the Manager Cyber Security.

Direct reports

Cyber Security Officer

Budget

Nil

Essential requirements

- Relevant tertiary qualification(s) in IT or related field and/or equivalent relevant industry knowledge and experience.
- Demonstrated high level experience, knowledge of, and experience in cyber security functions and procedures.
- Thorough knowledge of AIMS principles and processes, and/or willingness to obtain competence within 12 months.


You may be required to participate in activities to support the agency out of business hours during a cyber security, operational or emergency responses at NSW SES locations in the state, where the requirements are within the scope of your skills, knowledge, and capabilities. You may also be required to participate in an on-call roster.




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

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	Intermediate
	Value Diversity	Intermediate
	Communicate Effectively	Adept
	Commit to Customer Service	Intermediate
	Work Collaboratively	Intermediate

	Influence and Negotiate	Intermediate
	Deliver Results	Intermediate
	Plan and Prioritise	Intermediate
	Think and Solve Problems	Adept
	Demonstrate Accountability	Intermediate
	Finance	Foundational
	Technology	Adept
	Procurement and Contract Management	Foundational
	Project Management	Intermediate

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

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 Be ethical and professional, and uphold and promote the public sector values	Adept	<ul style="list-style-type: none"> Represent the organisation in an honest, ethical and professional way and encourage others to do so Act professionally and support a culture of integrity Identify and explain ethical issues and set an example for others to follow Ensure that others are aware of and understand the legislation and policy framework within which they operate Act to prevent and report misconduct and illegal and inappropriate behaviour
Personal Attributes Manage Self Show drive and motivation, an ability to self-reflect and a commitment to learning	Intermediate	<ul style="list-style-type: none"> Adapt existing skills to new situations Show commitment to achieving work goals Show awareness of own strengths and areas for growth, and develop and apply new skills Seek feedback from colleagues and stakeholders

NSW Public Sector Capability Framework

Group and Capability	Level	Behavioural Indicators
Relationships Communicate Effectively Communicate clearly, actively listen to others, and respond with understanding and respect	Adept	<ul style="list-style-type: none"> Stay motivated when tasks become difficult Tailor communication to diverse audiences Clearly explain complex concepts and arguments to individuals and groups Create opportunities for others to be heard, listen attentively and encourage them to express their views Share information across teams and units to enable informed decision making Write fluently in plain English and in a range of styles and formats Use contemporary communication channels to share information, engage and interact with diverse audiences
Results Think and Solve Problems Think, analyse and consider the broader context to develop practical solutions	Adept	<ul style="list-style-type: none"> 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
Business Enablers Technology Understand and use available technologies to maximise efficiencies and effectiveness	Adept	<ul style="list-style-type: none"> Identify opportunities to use a broad range of technologies to collaborate Monitor compliance with cyber security and the use of technology policies Identify ways to maximise the value of available technology to achieve business strategies and outcomes Monitor compliance with the organisation's records, information and knowledge management requirements

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

Category and Sub-Category	Level and Code	Level Descriptions
Service Management Service Operation	Level 5 SCAD	Security Administration (SCAD) - Drafts and maintains the policy, standards, procedures and documentation for security. Monitors the application and compliance of security operations procedures and reviews information systems for actual or potential breaches in security. Ensures that all identified breaches in security are promptly and thoroughly investigated. Ensures that any system changes required to maintain security are implemented. Ensures that security records are accurate and complete.

NSW Public Sector Capability Framework

Group and Capability	Level	Behavioural Indicators
Strategy & Architecture	Level 5	Information Security (SCTY) - Obtains and acts on vulnerability information and conducts security risk assessments for business applications and computer installations; provides authoritative advice and guidance on security strategies to manage the identified risk. Investigates major breaches of security and recommends appropriate control improvements. Interprets security policy and contributes to development of standards and guidelines that comply with this. Performs risk assessment, business impact analysis and accreditation for all major information systems within the organisation. Ensures proportionate response to vulnerability information, including appropriate use of forensics.
Information Strategy	SCTY	