PSCareers

Position description

Your role at PSC

Cyber Analyst

Section: People, Process and Technology

Salary point: 15

Position number: PSC747

Last updated: May 2026

Position objectives

To effectively monitor, assess and respond to cyber security risks that impact the business needs of Council and its staff. By pro-actively maintaining controls and investigating events, the Cyber Analyst delivers cyber security services that are reliable, fit for purpose and evolving with the threat landscape facing Council. The Cyber Analyst also supports the development and delivery of cyber security uplift initiatives.

PSC values

Respect: Creating a unique, open and trusting environment

Integrity: Being honest and taking responsibility for our actions

Teamwork: Working together as one Council to support each other

Excellence: Improving the way we work, to meet future challenges

Safety: Providing a safety focused workplace culture

Key responsibilities

Management of Council's Cyber Security controls and services (Security Operation):

- Operational management of Council's on-premises and cloud cyber security environment (including configuration, tuning, alert triage and investigation, monitoring and reporting of security controls)
- Ensuring that Council's information and systems are protected against unauthorised access, disclosure and disruption for our customers
- Ensuring operational effectiveness of Council's cyber security monitoring and detection capability, including regular review of alert rules, log sources and coverage, as outlined in the Information Security Management System

- Assess and recommend improvements to security controls and services that align to the wider Digital Strategy and Roadmap, including Essential Eight uplift, identity protection, endpoint security, data protection and threat detection
- Completion of scheduled control review and assurance tasks (that may be outside business hours) which includes the validation of policy enforcement, signature and content updates, and configuration baselines.
- Maintaining accurate and accessible documentation of Council's cyber security controls and audit evidence
- Maintain a high level understanding of Council's security architecture and control environment

Incident and threat management (Security Operation):

- Investigation and containment of cyber security incidents in a way that minimises impact to Council and its customers
- Identifying threat and event patterns based on alerts, user reports and intelligence sources, leading in the identification of underlying causes and the development of effective long-term mitigations
- Implement effective long term solutions to problems through the ICT Change Management process
- Participating in the "After-Hours On-Call Infrastructure Support Service" rostering system

Project Delivery (Service Design & Service Transition):

- Contribute to the service strategy by analysing, developing and evaluating alternative security technologies, platforms and configuration through the service design phase
- Completion of assigned tasks through the service transition phase

Assist the ICT Operations Lead when requested:

- Performing the forensic and information discovery activities in support of staff management, legal or GIPA investigations
- Completion of tasks assigned by the ICT Operations Lead, at all Council sites across the Port Stephens Local Government Area

Key accountabilities

The role of a Cyber Analyst is critical to the secure and audit-defensible operation of Council's ICT environment. Tasks are technical and investigative in nature, requiring detailed analysis and structured judgement to ensure that security controls are consistently enforced, evidenced and reviewed across the device, identity and data estate.

It plays a proactive role in monitoring the threat landscape, investigating events, maintaining control evidence and supporting the broader cyber uplift program. Productive interactions with the ICT Operations team, managed service providers, vendors and external assessors are critical to the success of this role.

Cyber security operational and assurance functions in an enterprise environment include:

- Administering mail flow protections across Council's M365 environment

- Operating network security and intrusion prevention controls in line with approved policy
- Responding to security incidents in accordance with Council's Incident Response plan
- Administering Council's firewall estate including rule lifecycle and change management
- Operating Microsoft 365 security suite, including Defender, across the device estate
- Maintaining Council's security monitoring and detection platform
- Administering data protection controls including sensitivity labelling and DLP
- Applying cyber security fundamentals across identity, endpoint, encryption and secure configuration
- Conduct vulnerability assessments and remediate within agreed timeframes
- Collecting and retaining control evidence demonstrating consistent enforcement of security frameworks
- Producing audit-facing reporting on posture, incidents, control performance and remediation progress for both internal and external audits.
- Maintaining the cyber security exception register and supporting documents as controlled audit artefacts
- Supporting the secure operation of Council's on-premises data centre and communications rooms

Extent of authority

- This position is required to use high level of initiative and problem solving and has the autonomy to make decisions that can have a high impact across work areas and the organisation
- Sometimes decisions needs to be made quickly, independent of peer review and advice or manager approval
- Tasks are allocated under the direction of the ICT Operations Lead and/or the CTO and are to be performed in accordance with Council's processes and procedures
- Where existing processes or procedures do not cover the situation faced, the incumbent may be required to develop and/or modify current processes in consultation with the ICT Operations Lead and/or the CTO

Judgement and decision making

- A high level of investigative skill is required to undertake detailed analysis and identify and develop solutions before choices can be made when solving problems
- A high level of judgement and initiative is required to make decisions in time pressure situations, often outside business hours (throughout the night or on weekends) independent of peer review, advice and autonomous alignment within the agreed escalation pathways
- Decisions made will often affect the work and activities of all groups of the Council to the extent of functions for which the position is responsible
- There is a need to negotiate and determine work priorities

Skills, knowledge and capacity

Organisational

- Demonstrated commitment to a customer service culture and delivery of quality service
- Understanding of the Australian Business Excellence philosophy
- Conduct that demonstrates to others Council's commitment to Respect, Integrity, Teamwork, Excellence and Safety

Interpersonal

- Proven ability to consult and negotiate effectively with internal and external customers and suppliers
- Good organisational skills and the ability to prioritise workload to meet tight deadlines whilst paying attention to detail
- Demonstrated initiative, flexibility and assertiveness with demonstrated ability to act independently
- Well-developed interpersonal and verbal communication skills and a demonstrated ability to work co-operatively as part of a team
- Commitment to ongoing learning and development
- Demonstrated ability to handle highly sensitive information, respecting confidentiality and disclosure regulations
- Ability to research, quickly identify and correct unusual problems

Qualifications and experience

- Tertiary or industry qualifications that demonstrates expertise and competency in the ICT discipline
- Experience that demonstrates expertise and competency in the ICT security discipline
- Experience operating enterprise cyber security tooling including endpoint protection, SIEM, firewall and data protection platforms to deliver on the key accountabilities
- Experience supporting a secure environment operating on the Microsoft Windows platform
- Sound knowledge of networking technologies and principles
- Working knowledge of the Australian Signals Directorate Essential Eight and the NSW Cyber Security Policy, including the evidence and reporting expectations of each
- Experience creating and maintaining Information Management systems documentation
- A current "Class C" NSW driver's licence and ability to safely operate a Council passenger carrying vehicle

Capability Framework level: Adept

Personal attributes	Relationships	Results	Resources
• Manage self • Displays resilience and adaptability • Act with integrity • Demonstrate accountability	• Communicate and engage • Community and customer focus • Work collaboratively • Influence and negotiate	• Plan and prioritise • Think and solve problems • Create and innovate • Deliver results	• Finance • Assets and tools • Technology and information • Procurement and contracts

Position description approval

Employee

Date