



Redland City Council Position Description

Date Created	17 MAY 2021
Date Amended	12 October 2026
Probation Period	3 months
Related Positions	
Authority Level Approval	Group Manager
Established Position	Yes

Position Title	Senior Cyber Security Operations Analyst
Position Number	201397
Award	Queensland Local Government Industry Award - State 2017 and applicable Division(s)
EB Agreement	Officers' Certified Agreement
Applicable Agreement/s	
Salary Level	7
Position Employment Type	Permanent
Attendance Type	Full Time
Department / Group	Organisational Services / Corporate Services
Unit / Team	Cyber Security
Standard Hours	36.25
Functional Capacity Assessment	A - Completion of a pre-employment questionnaire

PRIMARY PURPOSE

The Senior Cyber Security Operations Analyst is responsible for leading and coordinating the operational delivery of Council's cyber security capability across Information Technology, Operational Technology, Internet of Things, Closed Circuit Television, cloud platforms and Microsoft 365 services. Reporting to the Principal Cyber Security Adviser, the role operates under limited direction and exercises specialist judgement in coordinating a significant cyber security operations capability, including security monitoring, incident response, threat management, vulnerability management, security assessments, awareness activities, operational assurance and cyber security technologies.

The role will deliver the Cyber Security operations function through:

- Providing operational leadership and specialist advice to internal and external stakeholders on cyber security controls, operational risks, system security and incident response requirements.
- Coordinating the effective operation and continual improvement of cyber security systems and controls including Microsoft 365 security services, identity protection, endpoint protection, email security, vulnerability management, monitoring and response capability.
- Developing and maintaining operational procedures, playbooks, guidance, reporting and assurance practices to support consistent cyber security operations across Council environments.
- Supporting Council's broader cyber security strategy, governance and risk management objectives through operational delivery, expert advice, awareness activities and continuous improvement initiatives.

STATUTORY REQUIREMENTS AND CORPORATE REQUIREMENTS

All aspects of this position will be performed by the incumbent to:

- satisfy all relevant statutory obligations,
- satisfy public sector ethical standards, and Redland City Council (RCC) codes of conduct and values,
- comply with the Information Privacy Principles of the Information Privacy Act 2009,
- contribute to and support the achievement of Redland City Council's Corporate Plan,
- align with authorised RCC policies, guidelines, and procedures,
- support and contribute to customer service that satisfies the RCC Customer Charter, and
- protect the safety of self and other workers through safe work practices as detailed in the Work Health and Safety Management Guideline and associated statements.

For staff who create or receive corporate/business documents (including e-mail), it is a requirement that these documents be registered into the relevant corporate recordkeeping system/s in accordance with approved Policy and Procedures.

ORGANISATIONAL RELATIONSHIPS

Reports to: Principal Cyber Security Adviser (200650)

Supervises: Nil

DELEGATIONS

As described in the Delegations Register.

Key Accountabilities		
1	Lead Cyber Security Operations Delivery Lead and coordinate the operational delivery of Council's cyber security services under the direction of the Principal Cyber Security Adviser. This includes exercising specialist judgement and operational decision-making across security monitoring, threat management, vulnerability management, cyber incident response, Microsoft 365 security services, endpoint protection, identity security, cloud security, email security and related cyber technologies. The role is responsible for operational effectiveness, procedures, control improvement and maturity of Council's cyber security operations capability.	40%
2	Coordinate Incident Response, Threat Management and Operational Readiness Lead and coordinate operational cyber incident response, threat management and readiness activities, including initial incident triage, investigation, containment advice, escalation, recovery support, lessons learned, and response playbooks. Provide expert operational advice during complex or high impact cyber events and ensure response procedures remain current, tested, understood and aligned to Council's escalation requirements.	25%
3	Provide Security Assessments, Risk Advice and Control Assurance Provide specialist cyber security advice, system assessments and risk management support across Council's technology environments, including Information Technology, Operational Technology, Internet of Things, CCTV, cloud platforms, infrastructure, applications and software procurement. Undertake risk assessments, review solution designs, assess supplier and system security risks, contribute to security architecture discussions and recommend practical control treatments to support operational assurance.	20%
4	Coordinate Cyber Awareness, Documentation and Continuous Improvement Coordinate cyber awareness, communication and continuous improvement activities across Council. Develop and maintain cyber security procedures, guidance material, operational documentation, risk records, reporting and assurance evidence. Build effective relationships with business units, technology teams, suppliers, government agencies and industry partners to improve operational cyber security maturity, consistency and resilience.	15%

Selection Criteria

1	Extensive experience in cyber security operations and administration, including Microsoft 365, Microsoft Defender, Microsoft Sentinel, Microsoft Entra ID, Microsoft Purview, Microsoft Azure, Amazon Web Services, firewalls, intrusion prevention systems, web application firewalls, email gateways, endpoint protection, vulnerability management platforms and SIEM capability. Demonstrated ability to lead and coordinate specialist cyber security operations under limited direction and improve operational control maturity.	30%
2	Demonstrated experience in cyber incident response, investigations, threat management and operational cyber security, including phishing analysis, sandboxing or digital forensic tools, threat hunting, root cause analysis, security monitoring, response coordination and the ability to document and present findings, recommendations and lessons learned.	25%
3	High level analytical and problem-solving experience with the ability to undertake cyber security reviews, system assessments and risk assessments across Information Technology, Operational Technology, cloud services, infrastructure, applications, software procurement and technology projects. Proven ability to apply specialist judgement, translate complex security matters into clear business advice and recommend practical operational treatments.	15%
4	Demonstrated understanding and practical application of cyber security frameworks, standards and guidance including ASD ISM, ASD Essential Eight, ISO 27001, NIST Cyber Security Framework and relevant Australian Government cyber security guidance. Knowledge of privacy, supplier assurance and Security of Critical Infrastructure obligations would be highly regarded.	15%
5	Highly developed written, verbal and interpersonal communication skills, including the ability to provide specialist advice, deliver cyber awareness activities, coordinate initiatives, influence operational decisions, prepare reports and build effective relationships with internal stakeholders, suppliers, government partners and industry groups. Demonstrated ability to exercise sound judgement and coordinate a significant specialist operational work area under limited direction.	15%

Mandatory Criteria

Criminal History check prior to appointment

Desirable Criteria

Bachelor's degree or certification in Cyber Security, Information Technology, Information Systems, Risk Management or a related discipline

Relevant industry certifications such as CISSP, CISM, CRISC, CCSP, Security+, Microsoft Security, Azure Security, GIAC or equivalent

Experience using Microsoft Defender, Microsoft Sentinel, Entra ID, Microsoft Purview, Microsoft 365, Azure, AWS, vulnerability management platforms, endpoint protection, email security and SIEM capability

Experience in operational technology, critical infrastructure, water sector environments, supplier assurance, security architecture, risk assessment or local government cyber security

ITIL, project management, incident management, business continuity or cyber awareness program experience

Authorities

This position description meets the capability requirements of the position.

People and Culture Officer / Executive Group

Manager, People, Culture & Org Performance

Date:.....

Group/General Manager/

Chief Executive Officer:.....

Date:.....