

Position Description – Network Administrator

Position Number:	1060
Directorate:	Services
Business Unit:	Information Technology
Hours Per Week:	35
Award:	Local Government (State) Award
Grade (SAS):	24
Location:	Civic Centre
Position Reports to:	Manager – Information Technology
Positions Reporting Direct to this One	Nil

Our Values



Customer focus

We listen to the needs and wants of our customers and provide exceptional customer service



Integrity

We are fair and consistent in our actions, and we act ethically, honestly, responsibly and respectfully



Consultation

We seek to understand before acting and are sensitive to residents' needs and situations



Leadership

We focus attention on what is really important, lead by setting a good example and seek to improve outcomes, processes and relationships



Equity

We deal equally and honestly with customers and each other

Position Overview

This Position Description is not a complete statement of all the Accountabilities, Responsibilities, Tasks and Outcomes etc. associated with the role. It is intended only to be indicative and descriptive of the role with the incumbent required to undertake any and all tasks requested that are within their skills, competence and training.

The nature of the work means that some tasks and projects will be required to be undertaken outside of normal work hours so as to minimise impact to the network environment and applications.

Responsible for the management of Council's Information Technology infrastructure and resources, to ensure the efficient planning, implementation and application of information technology to support Council's service delivery.

Work with the Senior Cyber Security and IT Infrastructure Administrator to provide cyber security, risk and relevant technical expertise to support Council's cyber security posture, including providing cyber security guidance and performing assessments to identify risks and develop controls for the Essential 8 and other cyber security frameworks.

Principal Accountabilities

- Manage and administer Council's network infrastructure and virtual servers, including acquisitions, upgrades, operations and maintenance of the virtual environment, servers, SAN, firewalls, routers, switches and other networking equipment and infrastructure.
- Troubleshoot network and connectivity issues and provide solutions to minimise disruptions to business operations.
- Manage and administer Council's information technology equipment and software, including the installation, configuration, maintenance and support for personal computers, software, and peripherals such as phones, printers, scanners, and modems.
- Liaise with external suppliers for procurement, maintenance and repairs when necessary.
- Ensure the integrity and security of Council's data, and data backup and recovery of corporate information system and network.
- Ensure Council's IT disaster recovery plan is current and periodically tested to ascertain its effectiveness.
- Manage and administer access controls, user accounts, and permissions for network and cloud resources and services.
- Develop and maintain network and security documentation such as diagrams, inventories, and procedures to ensure accuracy and completeness.
- Perform system monitoring and analysis, including network performance tuning and troubleshooting, and deploying measures to enhance network speed, reliability, and availability.
- Provide technical advice and assistance to IT team members to achieve the team's business outcomes, including helpdesk support and training for users.
- Work with the Senior Cyber Security and IT Infrastructure Administrator to plan, develop, implement and maintain security measures to protect Council's digital assets against cyber threats and unauthorised access and meet required outcomes.
- Assist the Senior Cyber Security and IT Infrastructure Administrator to undertake incident response, threat and vulnerability management, logging and monitoring, technical assurance and compliance monitoring activities.
- Assist with the risk management of information assets by performing threat and risk assessments for various platforms, applications and cloud services, as well as providing guidance on security controls for risk treatment.
- Assist with the implementation of actions to respond to the cyber security internal audit findings and/or recommendations.
- Oversee the hardware and software maintenance contracts, including that the contracts are current and in place, for all computer equipment, including networking and critical infrastructure.

Key Organisational Accountabilities

- Abide by the principles of Council's Code of Conduct – and other Council policies and procedures – in the carrying out of all Council duties: integrity, leadership, selflessness, objectivity, accountability, openness, honesty and respect.
- Contribute to improved customer service and organisational effectiveness, by acting ethically, with honesty and fairness.
- Provide exceptional customer service by listening to the needs of each customer and action in a prompt, professional and courteous manner at all times.
- Foster innovation through seeking to improve outcomes, processes and relationships.
- A commitment to ensuring the organisation is child safe.
- Identify, assess and manage all risks associated with the function.
- A commitment to Council's Fraud and Corruption prevention strategy.
- Report injuries, accidents, incidents and near misses in the work area and on the corrective actions taken to prevent reoccurrence.
- Always ensure your actions contribute to a safe and healthy workplace.
- Use and properly maintain appropriate safety clothing and personal protective equipment.
- Ensure EEO, the principles for a culturally diverse society, and Council policies are complied with at all times.

Selection Criteria

Essential

Qualifications

- Tertiary Qualifications in Information Technology or equivalent.

Skills/Experience

- Experience in computer and networking infrastructure, firewalls, operating systems, virtual technologies and cloud technologies.
- Knowledge of network security infrastructure including, but not limited to, wide area networks, firewalls, routers and switches.
- Understanding of cyber security governance risk and compliance.
- Demonstrated ability to analyse information, solve problems and make sound judgments with the appropriate security controls in place.
- Well-rounded in-depth technical skills with attention to detail.
- Demonstrated ability to provide quality customer service.
- Demonstrated record of achievement in Information Technology.
- Excellent oral and written communication, interpersonal and negotiation skills.
- Ability to meet time project deadlines, manage constraints and competing deadlines.
- Previous experience in a similar role in either the public or private sector.

- Ability to maintain confidentiality.
- Highly motivated self starter.
- Team based approach.
- Current Class C Driver Licence.

Desirable

- Cyber security related certification.

Other

- Position Holder in this position will be subject to relevant and ongoing probity checks as determined by Council.

Signature

Position Holder: _____ Date: _____

Reviewed and Finalised

Date: July 2026