POSITION DESCRIPTION

Specialist Network Engineer



POSITION DETAILS

Position Title	Specialist Network Engineer
Classification	HEW 7
Position Number	NEW
School/Office	Digital Services / Security & Digital Operations
Division	Division of Operations

POSITION PURPOSE

This position delivers high-quality network engineering services that support the University's digital infrastructure. It contributes to the design, implementation, and optimisation of secure and scalable network solutions that enable teaching, research, and operational excellence across campuses.
The role also ensures effective capacity planning, supports disaster recovery and continuity arrangements, and provides specialist advice to uplift cyber resilience and network performance.

KEY ACCOUNTABILITIES

- Implement and maintain enterprise network infrastructure to ensure performance, reliability, and security across all campuses.
- Diagnose and resolve complex network issues using advanced troubleshooting techniques and tools.
- Collaborate with internal teams and external vendors to deliver integrated network solutions aligned with strategic objectives.
- Monitor network performance and usage trends, identifying opportunities for optimisation and improvement.
- Ensure compliance with network governance, standards, and protocols, including cybersecurity and regulatory requirements.
- Contribute to network design and planning activities, providing technical input and recommendations.
- Conduct capacity planning to ensure network resources meet current and anticipated demands.
- Contribute to business continuity and disaster recovery processes from a network perspective.
- Document network configurations, procedures, and changes to maintain accurate and accessible records.
- Support the adoption of emerging technologies that enhance network capabilities and user experience.

QUALIFICATIONS, EXPERIENCE AND SKILLS

- Tertiary qualifications in Information Technology, Network Engineering, or a related discipline, or equivalent experience.
- Proven experience in enterprise network engineering, including implementation, maintenance, and troubleshooting.
- Strong understanding of network protocols, architectures, and cybersecurity principles.
- Experience working with network monitoring and diagnostic tools.
- Ability to collaborate effectively with technical and non-technical stakeholders.
- Excellent problem-solving, communication, and documentation skills.
- Requirement to obtain and maintain any clearances necessary to perform the role *(including, but not limited to, a NSW Police Force Professional Suitability clearance).*

Technical Proficiency

- Hands-on expertise with enterprise-grade networking technologies (e.g., Cisco, Juniper, Palo Alto).
- Experience with network monitoring and diagnostic tools (e.g., SolarWinds, Nagios, Wireshark).
- Knowledge of routing, switching, firewalls, VPNs, and wireless solutions in large-scale environments.
- Familiarity with automation and scripting for network configuration (e.g., Python, Ansible).

Desirable

- Relevant certifications such as CCNP, JNCIP, or equivalent.
- Experience in higher education, research, or public sector environments.
- Exposure to cloud networking (Azure, AWS) and hybrid connectivity models.

KEY RELATIONSHIPS

This position reports to: Manager & Architect, Network

This position supervises: None

Key internal relationships:

- Cybersecurity, IT Operations, Digital Infrastructure, Academic and Professional Units

Key external relationships:

- Network vendors, service providers

CHALLENGES

- Managing complex network environments across multiple campuses with diverse user needs.
- Responding to evolving cybersecurity threats and compliance requirements.
- Balancing operational reliability with innovation and continuous improvement.
- Coordinating with vendors and partners to deliver timely and effective solutions.

OCCUPATION SPECIFIC CAPABILITY SET

SFIA

SFIA Capability	Code	Level	Rationale
Network support	NTAS	L4	Applies and maintains enterprise network infrastructure, ensuring operational performance, reliability, and security.
Incident management	USUP	L4	Responds to and resolves complex network incidents, escalating as needed, to maintain continuity.
Network design	NTDS	L4	Contributes technical input into network design and planning, supporting scalable and secure architecture.
Security administration	SCAD	L4	Applies security controls within network operations, ensuring compliance with policies and regulatory standards.
Service management	ITSM	L4	Collaborates with internal teams and vendors to coordinate delivery of integrated network solutions.
Performance management	DEMM	L4	Monitors and analyses network usage and performance trends to recommend improvements.
Capacity management	CPMG	L4	Tracks and plans network capacity to meet current and future demand.
Continuity management	COPL	L4	Supports business continuity and disaster recovery by ensuring network resilience.

UNIVERSITY EXPECTATIONS

The University expects that all employees are aware of, and comply with legislation and Western's policies and procedures relevant to the position, including but not limited to:

- → Code of Conduct
- → Work Health and Safety and Wellbeing Management System
- → Enterprise Agreement or Award
- → Anti-discrimination principles, Equal Employment Opportunity and staff and student equity.

Approved by:
Date: