

Position Description – Network Engineer

Core Detail

Title	Senior Network Engineer
Role	The Network Engineer designs, implements, operates and improves secure, reliable and cost-effective network and communications services across TriCare's corporate offices, residential aged care facilities, retirement living locations and cloud-connected environments. The role provides end-to-end technical management of business networking, including LAN, WAN, internet, wireless, network security, remote access, cloud connectivity, core network services, voice connectivity and the network dependencies of clinical, building and operational systems. Responsibilities span design, deployment and configuration, monitoring, troubleshooting, recovery, documentation, automation, supplier coordination and asset lifecycle planning. The position supports resident care, business continuity and workforce productivity. The role works within approved architecture, security policy and delegated authority; enterprise strategy, risk acceptance, expenditure approval and application ownership remain with the relevant accountable owners.

Position Parameters

Employment	Full time, permanent
Reporting to	CIO.
Location	TriCare Head Office – Mt Gravatt

Detailed Description of the Position

Network design and business connectivity	• Translate business, care-service and site requirements into documented network designs, options, costs, risks and implementation plans within approved standards. • Design and implement campus, branch and data-centre LANs, routing, switching, VLANs, IP addressing, IPv4/IPv6, WAN, SD-WAN and internet connectivity. • Engineer enterprise Wi-Fi, including RF surveys, coverage, capacity, roaming, interference management and separate corporate, resident, guest and device access. • Implement private and public cloud network connectivity, virtual networks, routing, private endpoints, site-to-site connections and secure access to SaaS services in consultation with other teams. • Maintain network components of DNS, DHCP, IP address management, NTP, certificates and authentication integrations in conjunction with the relevant service owners. • Plan quality of service and bandwidth for business applications, real-time communications and critical care-service dependencies. • Provide designs and connectivity for new facilities, refurbishments, relocations and acquisitions, including structured copper/fibre cabling, racks, patching, optics and PoE capacity.
Network operations, performance and resilience	• Configure, administer and maintain routers, switches, access points, wireless controllers, firewalls and network-management platforms across physical, virtual and cloud environments. • Monitor availability, utilisation, latency, jitter, packet loss, interface errors, wireless experience and device health using actionable alerts, flow data, logs and dashboards. • Provide specialist escalation support; diagnose complex faults using traffic-path analysis and structured testing, coordinating carriers, vendors and internal teams through to restoration. • Maintain incident records, business-impact assessments and stakeholder updates; perform root-cause analysis and implement preventive actions for recurring problems. • Forecast capacity, identify bottlenecks and recommend upgrades or optimisation based on service demand, growth, performance and cost. • Manage firmware, supported software versions, configuration backups, secure recovery copies, spares and end-of-support risks through controlled maintenance. • Coordinate network dependencies on rack power, UPS, cooling and physical access with facilities and infrastructure teams; escalate environmental risks.

Network security and secure access	• Implement approved firewall, ACL, segmentation, routing and network-access controls using least privilege and separation of corporate, resident, guest, clinical, IoT and operational environments. • Administer secure remote and third-party connectivity, VPN, zero-trust network access and SASE/SSE network integrations where deployed, with time-limited and approved vendor access. • Maintain secure device administration, AAA/RADIUS/TACACS+ integrations, 802.1X/NAC, administrative MFA where supported, encrypted management and protected credentials. • Review firewall rules, exposed services, device hardening, certificates and network vulnerabilities; implement approved remediation and retain evidence of changes and exceptions. • Integrate network logs and security telemetry with central monitoring/SIEM; investigate network indicators and support authorised containment and recovery. • Apply approved DNS, web-filtering, intrusion-prevention and denial-of-service protections where supported; validate that security controls preserve authorised business services. • Maintain network control evidence for privacy, security and audit requirements; escalate residual risks to accountable owners rather than accepting risk independently.
Business communications and connected systems	• Engineer network connectivity and quality of service for voice, SIP trunks, unified communications, Teams calling integrations, video and meeting-room systems in collaboration with telephony providers. • Support resilient network dependencies for nurse call, clinical and medication systems, CCTV, access control, building management, printers, IoT and other approved connected services. • Coordinate mobile/cellular services, fixed wireless, carrier circuits and backup connectivity where used; maintain service inventories and escalation paths. • Agree device connectivity, discovery, multicast, segmentation, remote support and availability requirements with service owners and vendors, and validate end-to-end operation after changes. • Own the network contribution, not clinical application functionality, building-system operation or telecommunications policy; coordinate specialist owners and approved maintenance windows to protect care continuity.
Delivery, governance and lifecycle management	• Maintain current topology and data-flow diagrams, IP address plans, circuit and asset registers, configuration records, standards, operating procedures and support runbooks. • Plan and deliver network work packages with dependencies, risk assessments, approvals, communications, implementation steps, rollback plans and post-change validation. • Define and execute network acceptance, coverage, performance, security and failover tests; support business UAT and provide a documented service handover.

	• Automate repeatable configuration, backup, compliance checks and reporting using version-controlled scripts, APIs and infrastructure-as-code practices, with testing and credential protection. • Coordinate carriers, managed-service providers, cabling contractors and equipment vendors; track faults, service commitments, renewals, licensing, warranties and delivery quality. • Provide technical specifications, option comparisons, cost estimates and lifecycle forecasts for procurement and budgets; identify unused circuits, licences and services for approved rationalisation. • Contribute to network roadmaps and continuous improvement; transfer knowledge to the service desk, infrastructure and security teams and guide colleagues within the role's expertise. • Escalate material design deviations, service risks, funding decisions and contractual commitments to the relevant delegated authority.
	•
Location and Condition of Service	• Located at TriCare Head Office, 250 Newnham Road, Mt Gravatt QLD 4122. • Normal office hours, with additional hours as required for agreed deadlines and maintenance windows to minimise business disruption. • Travel to TriCare facilities when necessary. • Willingness to undertake occasional work outside normal business hours for planned deployments, critical incidents or maintenance. • Ability to maintain confidentiality when accessing systems containing resident, health, workforce, payroll and commercially sensitive information. •

Skills and Knowledge

Essential

- Demonstrated ability to design, implement and troubleshoot enterprise routing, switching, VLANs, subnetting, TCP/IP, IPv4/IPv6, WAN/SD-WAN and resilient internet services.
- Practical enterprise wireless skills covering RF design, surveys, capacity, roaming, authentication and guest/resident access.
- Hands-on capability with firewalls, NAT, VPNs, segmentation, secure administration, network access control and network security monitoring.
- Knowledge of DNS, DHCP, IPAM, NTP, network authentication, certificates, QoS, voice/video traffic and hybrid/cloud networking.
- Ability to interpret packet captures, flow records, network logs and performance metrics to resolve complex faults and identify root causes.
- Working knowledge of structured cabling, fibre, optics, racks, PoE, carrier services and physical infrastructure dependencies.
- Disciplined incident, problem, change and configuration practices, including risk assessment, testing, rollback, recovery and accurate documentation.
- Clear business and technical communication, supplier coordination and prioritisation based on care continuity, impact, urgency, security and cost.

Desirable

- Experience with enterprise SD-WAN, B-WAN, SASE/SSE, zero-trust access and cloud-native network services.
- Experience with dynamic routing such as BGP and OSPF, high-availability designs, load balancing and application delivery networking.
- Experience with wireless survey tools, network automation platforms, infrastructure as code and centralised configuration compliance.
- Knowledge of SIP, unified communications and connectivity for nurse call, CCTV, access control, building systems and other IoT/operational technology.
- Familiarity with Microsoft Azure and Microsoft 365 connectivity and identity integrations.
- Experience translating security frameworks and audit requirements into practical network controls and evidence.
- Hands on experience with Aruba switches, AP's and Aruba Central.
- Working knowledge of cyber security principals and frameworks.
- Experience working within Aged Care environments.

Personal/Other Attributes

- Patient and respectful
- Calm under pressure
- Customer focused
- Reliable and accountable
- Methodical and organised
- Comfortable working independently or as a part of a team
- Able to communicate with users at different levels of technical ability

- Comfortable working in care environments
- Sensitive to privacy and confidentiality
- Willing to take ownership of issues
- Able to balance urgency with appropriate process and security controls
- Committed to learning and continuous improvement

Experience / Qualifications

- Demonstrated experience delivering network engineering and operational support in a multi-site business environment, including complex troubleshooting and controlled production changes.
- Practical experience across switching, routing, wireless, firewalls and WAN/internet services, with evidence of delivering reliable business connectivity.
- Experience coordinating carriers, vendors and internal service owners through deployments, outages and service improvements.
- Relevant tertiary or vocational qualification in networking, information technology or a related discipline, or equivalent demonstrated professional experience.
- Working understanding of ITIL/service-management principles and practical application of incident, problem, change and configuration controls.

Highly Regarded

- Experience in aged care, healthcare, community services or another regulated, operationally critical environment.
- Relevant networking, wireless, firewall, cloud-networking or security vendor certifications, or equivalent demonstrated capability.
- Experience delivering network refreshes, site openings, WAN migrations, wireless improvements and recovery/failover testing.
- Experience supporting the network dependencies of Epicor, Ecase, nurse call and comparable business or care systems, in partnership with application owners.

Employment Eligibility and Mandatory Requirements

- Be legally entitled to work in Australia and provide evidence of their current work rights before commencing employment.
- Maintain valid Australian work rights for the duration of their employment and promptly advise the organisation of any change to their work entitlement or visa conditions.
- Hold a current Australian driver licence appropriate for operating a standard passenger vehicle.
- Satisfy the organisation's pre-employment screening requirements, which may include identity verification, employment history and reference checks, qualification verification and a national criminal history check.
- Ability to perform occasional physical tasks, including moving, installing and collecting standard ICT equipment, subject to safe manual-handling practices.
-

Work Health and Safety

The incumbent has the responsibility to comply with and meet all obligations contained in:

- a) Work Health and Safety (WHS) legislation;
- b) Related WHS responsibilities; and
- c) TriCare's Risk Management (RM) standards.

Performance Measures

Annual Quality Performance Improvement Review (QPIR).

Service outcomes and targets are to be agreed with the manager, reflecting site criticality, approved service levels and shared supplier responsibilities. Measures include network availability and user experience; incident restoration and repeat-fault reduction; change success and rollback readiness; timely vulnerability and firmware remediation; configuration-backup and recovery-test coverage; documentation and inventory accuracy; capacity headroom; project acceptance; and lifecycle, carrier

and licence cost visibility. SFIA-aligned development objectives should address the role's required technical skills, autonomy, communication and knowledge sharing.