## Network Security Engineer

**POSITION DESCRIPTION**

Business Services  
Chief Operating Officer Portfolio

---

### POSITION DESCRIPTION

**POSITION NUMBER**  
0054806

**PROFESSIONAL CLASSIFICATION**  
UOM 9 - $134,320 - $139,749 per annum (pro rata for part-time)  
- negotiable commensurate with qualifications and experience,  
a loading sum may be applied to the salary offered.

**SUPERANNUATION**  
Employer contribution of 17%

**WORKING HOURS**  
Full Time (1 FTE)

**BASIS OF EMPLOYMENT**  
Continuing

**HOW TO APPLY**  
Go to [http://about.unimelb.edu.au/careers](http://about.unimelb.edu.au/careers), under Current staff or Prospective staff, select the relevant option (‘Current Opportunities’ or ‘Jobs available to current staff’) and search for the position by title or number.

**CONTACT FOR ENQUIRIES ONLY**  
Terry Reidy  
Email: terry.reidy@unimelb.edu.au  
*Please do not send your application to this contact*

---

For information about working for the University of Melbourne, visit our website: [about.unimelb.edu.au/careers](http://about.unimelb.edu.au/careers)
ACKNOWLEDGEMENT OF COUNTRY

The University of Melbourne acknowledges the Traditional Owners of the unceded land on which we work, learn and live: the Wurundjeri Woi Wurrung and Bunurong peoples (Burnley, Fishermans Bend, Parkville, Southbank and Werribee campuses), the Yorta Yorta Nation (Dookie and Shepparton campuses), and the Dja Dja Wurrung people (Creswick campus).

The University also acknowledges and is grateful to the Traditional Owners, Elders and Knowledge Holders of all Indigenous nations and clans who have been instrumental in our reconciliation journey.

We recognise the unique place held by Aboriginal and Torres Strait Islander peoples as the original owners and custodians of the lands and waterways across the Australian continent, with histories of continuous connection dating back more than 60,000 years. We also acknowledge their enduring cultural practices of caring for Country.

We pay respect to Elders past, present and future, and acknowledge the importance of Indigenous knowledge in the Academy. As a community of researchers, teachers, professional staff and students we are privileged to work and learn every day with Indigenous colleagues and partners.

THE UNIVERSITY OF MELBOURNE

Established in 1853, the University of Melbourne is a leading international university with a tradition of excellence in teaching and research. The main campus in Parkville is recognised as the hub of Australia’s premier knowledge precinct comprising eight hospitals, many leading research institutes and a wide-range of knowledge-based industries. With outstanding performance in international rankings, the University is at the forefront of higher education in the Asia-Pacific region and the world.

The University of Melbourne employs people of outstanding calibre and offers a unique environment where staff are valued and rewarded.

Find out more about the University’s strategy, ‘Advancing Melbourne’, at https://about.unimelb.edu.au/strategy/advancing-melbourne

CHIEF OPERATING OFFICER PORTFOLIO

The Chief Operating Officer (COO) Portfolio is responsible for the University’s budget and financial performance, and the management of its property and capital. It also delivers efficient and effective shared services in support of all aspects of the University’s business.

The COO Portfolio is comprised of eight sub-portfolios covering all areas of our operations, including the newly established Operational Performance group. This has been established to drive and manage a program of operational improvement and service transformation, underpinned by contemporary business insights, data modelling, predictive analytics, digital tools, and service planning.
• Business Services
• Digital and Data
• Finance
• Legal and Risk
• Operational Performance Group
• Property
• Research, Innovation and Commercialisation
• Student and Scholarly Services

BUSINESS SERVICES
Business Services provides a full range of class leading information technology and facilities management services to all operating entities of the University, and fit for purpose and efficient Finance, HR and OHS services.

EQUAL OPPORTUNITY, DIVERSITY AND INCLUSION
The University is an equal opportunity employer and is committed to providing a workplace free from all forms of unlawful discrimination, harassment, bullying, vilification and victimisation. The University makes decisions on employment, promotion, and reward on the basis of merit.

The University is committed to all aspects of equal opportunity, diversity and inclusion in the workplace and to providing all staff, students, contractors, honorary appointees, volunteers and visitors with a safe, respectful and rewarding environment free from all forms of unlawful discrimination, harassment, vilification and victimisation. This commitment is set out in the Advancing Melbourne strategy that addresses diversity and inclusion, equal employment opportunity, discrimination, sexual harassment, bullying and appropriate workplace behaviour. All staff are required to comply with all University policies.

The University values diversity because we recognise that the differences in our people’s age, race, ethnicity, culture, gender, nationality, sexual orientation, physical ability and background bring richness to our work environment. Consequently, the People Strategy sets out the strategic aim to drive diversity and inclusion across the University to create an environment where the compounding benefits of a diverse workforce are recognised as vital in our continuous desire to strive for excellence and reach the targets of Advancing Melbourne.

ABOUT THE ROLE
Position Purpose:
The Network Security Engineer is a specialist technical role responsible for undertaking the deployment, management and maintenance of a range of networking and cybersecurity technologies, including Palo Alto firewalls, Palo Alto GlobalProtect VPN clients and ExtraHop Network Detection and Response.
This role will work as a bridge between the UoM Cybersecurity team and the UoM Networks and Telephony team in a highly hands-on capacity to ensure the ongoing effectiveness and optimisation of networking cybersecurity controls including monitoring, detection, prevention and response systems.

Reporting line: Cybersecurity Engagement Manager and Networks and Telephony Manager
No. of direct reports: 0
No. of indirect reports: 0
Direct budget accountability: NA

**Key Dimensions and Responsibilities:**

Task level: Significant  
Organisational knowledge: Moderate  
Judgement: Significant  
Operational context: University-wide

OH&S and compliance: All staff are required to take reasonable care for their own health and safety and that of other personnel who may be affected by their conduct. These include general staff responsibilities and those additional responsibilities that apply for managers, supervisors and other personnel. Specific responsibilities for the role are available at [http://safety.unimelb.edu.au/topics/responsibilities/](http://safety.unimelb.edu.au/topics/responsibilities/). Staff must comply with all relevant requirements under the University’s risk management framework including legislation, statutes, regulations and policies.

**Core Accountabilities:**

- Plan, deploy and configure networking and cybersecurity systems, including Palo Alto firewalls and ExtraHop Network Detection and Response, to optimise the ability to monitor, detect, prevent and quickly respond to cybersecurity threats
- Continually review and enhance proposed configuration changes, including firewall policies, DDoS protection policies and client security posture, to maximise the return on investment and network security control effectiveness
- Anticipate and actively lead initiatives to position the use of networking technology to meet the challenge of the evolving cyber landscape
- Provide expert advice and undertake configuration of networking equipment and systems to minimise the University’s attack surface
- Identify opportunities to enhance the University’s network management processes and track and resolve identified issues and exceptions
- Provide regular reporting on the status and effectiveness of the University's network security posture
- Analyse and automate cybersecurity intelligence and research to inform decision making and improve the timeliness of protective network security controls.
Selection Criteria:

Education/Qualifications

1. The appointee will have a tertiary qualification in networking or cybersecurity or an equivalent combination of relevant experience and education/training.

Knowledge and skills:

2. Demonstrate COOP values by acting in the best interest of your employer; displaying service excellence by striving to deliver beyond expectations and taking ownership of the delivery; and value working collaboratively, connecting with people and building relationships in your workplace.

3. Demonstrated experience in the design, deployment, integration, tuning, monitoring, maintenance and technical management of large deployments of enterprise networking and security systems such as
   a. next generation firewall (Palo Alto) technologies and ruleset reviews,
   b. software-defined network security controls,
   c. network attack simulation technologies,
   d. virtual private networks (GlobalProtect),
   e. intrusion prevention systems,
   f. cloud access security brokers,
   g. network detection and response systems,
   h. automation and orchestration platforms,
   i. web content filtering technologies,
   j. web application firewalls
   k. certificate management systems and
   l. packet capture and network analysis systems.

4. High order technical skills, methodical problem-solving skills and an ability to prioritise and work on multiple tasks quickly and effectively under pressure.

5. Experience analysing complex technical configurations and the impact of proposed changes quickly and efficiently.

6. A strong interest in applied network security and cybersecurity and a desire to own and drive continuous innovation in our network security technology stack.

7. Excellent communication skills including the ability to communicate with technical and non-technical audiences.

8. Certifications such as PCNSE (Palo Alto Networks Certified Network Security Engineer) would be preferred.

Desirable

- Personal resilience and experience responding to resistance to change.
- Experience operating effectively in a large-scale, technically complex environment.
- Experience with incident response processes and technologies.
- Experience within the higher education or research sectors.