



Position Description

Position title:	Senior Security Engineer
Entity:	Austroads
Division:	Data & Technology
Job Type:	Full-time (1.0 FTE)
Location:	Austroads Melbourne or Sydney Offices
Reports to:	Head of IT Operations
Responsible GM:	Chief Data & Technology Officer
Direct reports:	N/A
Date reviewed:	September 2025

Organisational Context

Austroads is the association of Australian and New Zealand transport agencies.

We provide authoritative, practical and impartial advice, information, tools and services to help our members to deliver safe, efficient and reliable mobility to their customers.

We also deliver value to a range of other key stakeholders across government, industry and communities, where there is a demonstrated societal benefit to do so.

Austroads comprises several business activities, including the core Austroads work program, the National Exchange of Vehicle and Driver Information System (NEVDIS), and Transport Certification Australia (TCA).

Our teams are located across Australia and New Zealand. We work in an integrated and collaborative way, along with external consultancies and other partners, to ensure our products and services are delivered successfully and maximise value.

Austroads promotes a culture of professionalism, innovation, and integrity, with a commitment to accountability, quality, and excellence in the delivery of all of our programs and services. Austroads values continuous improvement, and all staff are expected to engage in their work in a spirit of curiosity, collaboration, and proactivity.

We recognise the unique skills and abilities of each individual, who come from a wide range of disciplines and backgrounds. We support our people through ongoing development and learning opportunities and create a supportive team environment for all our staff. We strive to be an employer of choice.

Austroads takes inclusion and diversity seriously. We embrace difference and diversity of identity, experience and thought, and actively strive for inclusive behaviours across our company and our work.

The Role

Team Purpose

The Data and Technology team focuses on harnessing the power of data and technology to support our member organisations to deliver improved outcomes for roads and transport users.

Our mission is to enable data-driven decision-making, enhance operational efficiency, and create value for our stakeholders. We do this through the proactive development and implementation of contemporary D&T standards and systems.

Here are some key points that encapsulate our purpose:

1. **Data Stewardship:** We treat data as a valuable corporate asset. Our team aims to deliver its completeness, quality, security, and accessibility, allowing us to derive meaningful insights and drive informed actions.
2. **Technology Enablement:** We leverage state-of-the-art technologies; and we use the best systems for the task. Our goal is to empower our organization with scalable, reliable, and agile solutions.
3. **Cross-Functional Collaboration:** We collaborate closely with business units, ensuring alignment between data/technology strategies and organizational goals. By bridging the gap between technology and business, we drive holistic transformation.
4. **Innovation Hub:** Our group serves as an innovation hub, constantly exploring emerging trends and experimenting with novel solutions. We foster a culture of curiosity, experimentation, and continuous learning.

Remember, our Data and Technology team is not just about bits and bytes; it's about unlocking the full potential of data/technology to propel our organisation forward.

Position Purpose

The Senior Security Engineer will play a key role in strengthening Austroads' security posture by implementing cloud-native and third-party security solutions, supporting operational teams, and ensuring that technical controls are effective, scalable, and aligned with business and compliance requirements.

Major Responsibilities/ Accountabilities

The role is responsible for:

- **Cloud Security Engineering**
 - Designing, implementing, and managing security controls in Azure and AWS environments, such as IAM, network security, logging, and monitoring.
 - Ensuring cloud configurations align with best practices and compliance frameworks (e.g., CIS, Essential Eight, ISO 27001).
 - Supporting application and infrastructure teams with secure architecture and deployment guidance.
- **Security Controls Implementation and Support**
 - Deploying and maintaining technical security tools such as XDR, Zero Trust, vulnerability scanners, and cloud security posture management (CSPM) platforms.
 - Implementing and maintaining endpoint, network, and identity security controls across the organisation.
 - Integrating security tools and controls with existing infrastructure and ensure effective alerting, logging, and reporting.
 - Troubleshooting and resolving issues related to security tooling and configurations.
 - Conducting configuration reviews and hardening of systems, applications, and cloud services.

- Supporting technical assurance activities including penetration testing and remediation tracking.
- **Operational Support**
 - Collaborating with security operations, risk and compliance teams to support incident response, forensic investigations, risk assessments, and compliance initiatives.
 - Provide technical expertise and backfill support during peak operational periods or resource gaps.
 - Identifying opportunities to enhance security tooling, automation, and control effectiveness.
 - Staying current with emerging threats, technologies, and best practices in cloud and enterprise security.
 - Supporting the automation of security processes.
- **Supporting the Information Security Team**
 - Collaborating with technology and business teams to achieve information security outcomes.
 - Contributing to continuous improvement, identifying ways to enhance value for our members and the public
 - Maintaining Quality Systems processes and procedures associated with the function
 - Other duties as directed

Key Stakeholder Interfaces

Internal

- Chief Data & Technology Officer
- Head of IT Operations
- Head of Information Security & Policy
- Data & Technology team
- Project Directors and Managers
- All staff

External

- Austroads approved contractors and service providers
- Industry solutions providers

The Person

Qualifications, Knowledge, and Experience

The Senior Security Engineer will possess:

- Significant experience in cybersecurity engineering, with strong hands-on experience in Azure and AWS.
- Proven experience implementing and managing security tools and platforms.
- Strong understanding of cloud-native security controls, identity and access management, and infrastructure hardening.
- Familiarity with security frameworks such as ISO 27001, NIST, CIS and ACSC Essential Eight.
- Desirable:
 - Certifications such as CISSP, AWS Certified Security – Specialty, Microsoft Certified: Azure Security Engineer Associate, or equivalent.
 - Experience with scripting or automation (e.g., PowerShell, Python, Terraform).
 - Exposure to container security, CI/CD pipelines, and DevSecOps practices.
 - Exposure to regulatory compliance requirements and technical audit support.

Personal Qualities

The incumbent will need to present a professional image and build a strong relationship across the enterprise. Specifically, the role requires:

- Excellent leadership, initiative, innovativeness and drive, and the ability to work independently to deadlines and within time constraints, to handle tasks with discretion, confidentiality, reliability and flexibility, and to set priorities
- Demonstrated high level organisational and administrative ability.
- Highly developed interpersonal and communication skills, both oral and written, including the ability to deal tactfully and effectively with people at all levels.
- Comfortable working in a fast-paced environment
- A service focused approach
- Sound judgement and problem-solving ability
- Strong networking and teamworking skills
- Strong attention to detail
- Commitment to ongoing professional development and learning
- Professional ethics and integrity
- Comfort working in an environment which is constantly evolving

Capability Profile

Resilience and Courage	Is open and honest, prepared to express views, and willing to accept and commit to change. Maintains a positive attitude in the face of challenging situations.	Intermediate
Critical Thinking and Problem Solving	Objectively analyses and evaluates available data, points of view, needs of stakeholders and potential solutions before recommending relevant actions or decisions.	Intermediate
Digital and Technology Proficiency	Integrates digital and technological developments in the design and delivery of relevant policies, programs and services.	Advanced
Drive Accountability and Outcomes	Is proactive and responsible for own actions to ensure desired organisational objectives are achieved.	Intermediate
Communicating with Impact	Uses various communication media to convey information, ideas, and insights in ways that maximises understanding of key messages. Possesses good written and verbal communication skills.	Intermediate
Working Collaboratively	Collaborates with others, demonstrating an understanding of their value to the organisation.	Intermediate
Project/Work Delivery and Management	Defines work activities required to deliver against outcomes intended, in line with agreed timeframes, resources, and ways of working. Understands and applies effective project planning, coordination and control methods.	Intermediate