Government of South Australia
Department of Treasury and Finance

Role Statement

Role title	Cloud Mobility Specialist	**Classification**	ASO7
Branch	Office of the Chief Information Officer	**Type of Appointment**	Ongoing
Section	Cloud Services	**Position Number**	P68380
Approved by	Director, Digital Strategy, Technology and Architecture	**Date**	2 May 2026

Department of Treasury and Finance

The Department of Treasury and Finance is the lead agency for economic, digital and financial policy outcomes.

We play a vital role in providing financial services to the community and economic and fiscal policy advice as well as digital services to the Government of South Australia.

The Department of Treasury and Finance actively promotes flexible working arrangements and values diversity in the workplace.

Our Purpose

We are *the Government's trusted fiscal, economic, digital and policy advisor*.
We work to ensure *South Australia is a thriving, prosperous State now and in the future*.

Who we are

Talented, Clear Eyed and Curious

We are analytical, evidence based, innovative and creative.

High Performing

We are known for achieving successful and timely outcomes.

Trusted Partner

We work better together. We lead, partner, and collaborate to help solve the big challenges.

Agile

We organise around opportunities critical to our state and are flexible in responding to challenges.

Fulfilled and Fun

We take the work seriously and ourselves less so - we support each other in the pursuit of excellence and make Treasury a great place to work.

What we are known for

A world class Treasury and Finance.
A high performing agency that *seizes opportunities*, addresses the *big challenges*,
and is a *destination employer* providing *rewarding careers*.

Branch/Section

The Office of the Chief Information Officer (OCIO) enables a more connected, secure and digitally capable South Australian Government, empowering agencies to better serve the community. OCIO leads whole-of-government technology, cyber security and digital strategies, delivering resilient, trusted and innovative ICT platforms and services at scale. These include policy leadership, architecture, security governance, and the delivery of critical shared platforms that underpin government service delivery.

OCIO operates in accordance with the SA Public Sector Code of Ethics and is guided by principles that are customer-centric, collaborative, growth-minded, and accountable.

Flexible working arrangements are actively supported. OCIO operates an activity-based work environment designed to balance collaboration, focused work, and operational delivery.

Cloud Services, in OCIO, supports SA Government agencies by delivering whole of government cloud-based applications, software, infrastructure, and platforms including identity management services, the Microsoft 365 central tenancy platform, the Integration Platform as a Service, SMS and eFax Services to enhance collaboration, drive innovation and provide economies of scale that enable agencies to focus efforts on delivering services that meet customer needs.

What this role is responsible for

The Cloud Mobility Specialist is accountable to the Deputy Director, Cloud Services and acts as the principal technical specialist for Microsoft 365 mobility and endpoint security services across the South Australian Government central tenancy.

The role provides senior technical leadership across the design, governance, and continuous improvement of Microsoft Intune, Conditional Access, Windows Autopilot, and Microsoft Defender services. It is responsible for ensuring these services are secure, resilient, scalable, and aligned with whole-of-government ICT and cyber security strategies.

The position exercises delegated design and configuration authority for mobility and endpoint security controls; provides authoritative technical advice to agencies and senior stakeholders; and leads the strategic planning and evolution of M365 mobility services to support secure digital transformation outcomes across government.

Key responsibilities include:

- Providing specialist advice to the technical strategy, design and governance of Microsoft 365 mobility and endpoint security services, including Intune, Conditional Access, Autopilot and Microsoft Defender for Endpoint.
- Providing expert input to, and approval of, technical architectures and configuration standards impacting device, application and identity-based access controls.
- Designing and governing Zero Trust and least-privilege security models, including device compliance, identity-driven access and attack surface reduction.
- Providing authoritative advice and impact analysis on Conditional Access and device security policy changes.
- Leading the technical lifecycle of mobility services, including roadmap development, service enhancements, and continuous security posture improvement.
- Providing senior technical leadership during critical incidents and service disruptions, including complex system recovery and post-incident reviews.
- Supporting and mentoring team members to build organisational capability and promote consistent engineering and operational standards.
- Establishing and maintaining operational frameworks, standards and procedures to ensure compliance with policy, security and service management requirements.
- Leading engagement with SA Government agencies, ICT suppliers and strategic partners in relation to mobility and endpoint security services.
- Supporting audit readiness and compliance assurance activities by ensuring services are defensible, well-documented, and aligned with governance obligations.
- Contributing to briefings, papers and advice on emerging mobility, endpoint and identity security issues relevant to the Cloud Services portfolio.
- Championing continuous improvement, automation and innovation in the delivery of mobility and endpoint security services.
- While the primary focus of the role is Microsoft 365, a working knowledge of Azure and AWS is required to support broader cloud integration, identity, networking and security considerations in a multi-cloud environment.

Who this role reports to

The Cloud Mobility Specialist reports to the Deputy Director, Cloud Services.

Key Relationships/Stakeholders

- Has significant working relationships with external and internal Service Providers.
- Provides direction, advice and mentoring to members of the Cloud Services team to ensure a harmonious well motivated working environment.

Special Conditions

- Applicants will be required to undergo the appropriate and relevant Employment Screening Assessment(s) required for this role. This role requires:
  ☒ National Police Check
  ☒ Security Clearances - Negative Vetting Level 1
- Work within a confidential, commercially orientated and at times politically sensitive environment.
- The incumbent will be required to participate in the Departmental Performance Management Program.
- The incumbent may be required to be assigned to other positions at the same remuneration level across the department.
- Some out of hour's work may be required. Intrastate and interstate travel may be required.
- A current driver's licence, participation in an on-call roster and participation in an Incident Management Team will be required.
- The State Emergency Management Plan details a requirement for a Control Agency for Cyber Crisis. OCIO personnel will participate in Control Agency responsibilities as required subject to appropriate training and induction.

Essential Expertise

- Demonstrated senior-level experience providing technical leadership and specialist advice across Microsoft 365 mobility services, including Microsoft Intune, Conditional Access, Windows Autopilot and Microsoft Defender for Endpoint.
- Proven experience designing, implementing and governing least-privilege and Zero Trust security models in complex enterprise environments.
- Strong experience performing Conditional Access design, impact analysis, and policy optimisation to balance security and user experience.
- Demonstrated expertise in endpoint security controls, including Defender for Endpoint, security baselines, device compliance and attack surface reduction.
- Experience administering and troubleshooting Microsoft Entra ID, including hybrid identity and Entra ID Connect configuration and support.
- Experience integrating third-party or platform services within Azure environments to support mobility, identity or security outcomes.
- Ability to automate and maintain configurations using scripting tools such as PowerShell and APIs.
- Working knowledge of Azure, with awareness of AWS to support multi-cloud integration and security considerations.
- Knowledge of ITIL-aligned service management practices for planning, delivering and improving ICT services.
- Demonstrated ability to operate effectively under pressure, manage competing priorities and lead technical responses in complex environments.
- Highly developed analytical, documentation and problem-solving skills, with the ability to evaluate options and formulate sound, defensible solutions.

- Well-developed written and verbal communication skills, including the ability to provide clear, authoritative advice to senior stakeholders.
- Demonstrated ability to work independently and collaboratively, maintaining high standards of accuracy, accountability and professionalism.
- Understanding of, and commitment to, relevant legislation, policies and procedures including the Code of Ethics, WHS obligations, cultural inclusion and risk management principles (AS ISO 31000:2018).

Desirable Expertise

- N/A

Professional / Technical ICT Capabilities (Skills Framework for the Information Age – SFIA):

- Emerging Technology Monitoring: Monitors the market to gain knowledge and understanding of currently emerging technologies. Identifies new and emerging mobility trends and operational based security adaptable across a complex eco system with multiple subscribed agencies, assesses their relevance and potential value to the organisation, contributes to briefings of staff and management.
- Technical Specialism: Maintains deep specialist knowledge of mobility and endpoint security platforms and provides expert technical leadership and consultancy across the organisation. Exercises independent judgement in complex technical matters and supervises specialist technical activities where required.