Government of South Australia
Department for Housing and Urban Development

Role Statement

Position title:	Senior ICT Operations Officer	**Position no:**	P32334/P32507
Classification:	ASO5	**Review date:**	May 2026
Directorate:	Operations		
Business unit:	Information & Technology		

About us

Our department's primary objective is the delivery of homes and housing options for South Australians. In response to the national housing crisis, we are committed to accelerating the build of a diverse range of housing options. We strive to find solutions to the urgent demand for housing security.

Our mission focuses on coordinating various portfolios related to housing, housing infrastructure, urban development, and planning. By ensuring sound decisions and efficient management, we strive to create sustainable, well-planned communities offering safe and affordable housing options.

Join us in our endeavour to address one of the most pressing challenges of our time and make a tangible difference in the lives of our community.

OUR VALUES: Professionalism | Service | Respect | Courage and Tenacity | Collaboration and engagement | Trust | Sustainability | Honesty and Integrity |

About this role

The Senior ICT Operations Officer applies technical expertise across the full range of IT operational services. This role has primary responsibilities for the provision of effective, efficient and timely service delivery, incorporating extensive technical support, triage and incident response (including for cyber security matters), continuous improvement of IT functions and processes, and extensive collaboration with colleagues and managers both within and external to the Agency.

The Senior ICT Operations Officer acts as the first interface between the ICT Team and wider Agency staff for standard day to day, business as usual activities, whilst also maintaining and applying deep technical proficiency across a wide range of operational domains. To achieve success in this expansive role, the Senior ICT Operations Officer works under the broad direction of the ICT Service Delivery Manager to establish, embed and continuously improve operational efficiency, maintaining a high maturity, highly effective ICT operational function that appropriately balances competing demands across a volume of work that spans low complexity / highly automatable processes, through to expert technical and emergent problem solving, and moderate-complexity projects.

The Senior ICT Operations Officer will often demonstrate the highest domain-specific, technically proficient skillsets in the agency related to the administration of ICT Operational Systems and will directly engage external parties to collaboratively escalate issues where necessary. They apply excellent Third-Party relationship management skills in addition to the Customer Service skillsets that they exercise with agency staff on a daily basis.

The Senior ICT Operations Officer provides effective and comprehensive Help Desk services, contributes to ongoing maturity and capability uplift within the IT Operational Services model, promotes and contributes to the maintenance of an effective Operational Cyber Security posture, and delivers projects and initiatives relevant to IT operational services, including proactive internal measures and representing the agency at a technical level in cross-agency forums, working groups, and communities of practice.

Who will you work with

Senior ICT Operations Officer reports to: ICT Service Delivery Manager

The role is required to work with:

- Staff from across the Department.
- Stakeholders from external government agencies, consultants and external service providers, as required
- The position may become a member of a project team, when required, for the duration of the project, including maintaining sound working relationships with representatives from services providers

Conditions

- Some out of hours work may be required.
- Some intra state, international and interstate travel may be required.

- Required to maintain a safe working environment by adopting appropriate hazard management practices consistent with the role.
- Compliance with Government legislation, Code of Ethics for the SA Public Sector, Departmental policies and procedures, including information management, WHS and injury management, risk management, and the access / equity / diversity strategies of the public sector.
- Required to obtain a National Police Check prior to employment. A renewal will be required every 3 years.
- Duties may be limited by eligibility and willingness to obtain and maintain an Australian Government Security Vetting Agency Security Clearance at Baseline or Negative Vetting Level 1.

What you will do

Key responsibilities	Specified duties	Performance indicator/ measurement
Level 1 through level 3 Service Desk Support	1. Provide expert technical support to end-users, resolving complex IT issues and proactive services. 2. Escalate and coordinate support cases when necessary. 3. Ensure timely and effective problem resolution. 4. Efficiently manage prioritise workloads within the ITSM system and adjacent channels. 5. Maintain a user-friendly knowledge base. 6. In consultation with the ICT Service Delivery Manager, lead hardware selection, procurement, and deployment activities.	• Incidents and requests are prioritised and resolved in accordance with approved DHUD ICT priority definitions and Service Level Agreements. • Level 2/3 incidents include appropriate diagnostic detail, resolution steps and root cause analysis, where required by documented procedures. • Knowledge articles are created and maintained in alignment with DHUD knowledge management standards. • Tickets are actively monitored and updated in line with agreed ICT operational reporting and communication standards.
Operational ICT Systems Administration	1. Lead the technical administration of all operational ICT systems. 2. Manage and maintain Active Directory Services and ensure that user accounts and permissions are accurate and secure. 3. Effectively administer and manage operational software licenses.	• User account provisioning, modification and de-provisioning is completed in accordance with approved DHUD ICT procedures. • Periodic access reviews are conducted and remediated as defined in DHUD ICT documentation. • Changes are executed in line with approved change management frameworks and risk tolerances.

Patching, Configuration Item and Asset Management	1. Ensure that patching, Standard Operating Environment (SOE) management, Mobile Device Management and compliance with relevant Standards are all maintained in accordance with targets. 2. Maintain accurate records of physical and intangible IT assets.	• Patching of endpoints, servers and applications is performed in accordance with the DHUD ICT procedures, including risk categorisation and governance. • Urgent and security-related patches are prioritised and implemented within timeframes defined by approved DHUD ICT policy or through documented risk acceptance. • Asset and configuration records are maintained in accordance with DHUD ICT standards.
Local Network and Cloud Infrastructure Administration	1. Administer and troubleshoot local network infrastructure, escalating and collaborating with support partners as necessary. 2. Ensure network reliability and performance. 3. Collaborate with the Architecture function to administer and manage cloud infrastructure effectively.	• Network and cloud infrastructure issues are managed in accordance with approved DHUD ICT practices, including escalation to partners and architecture functions as required. • Recurring or systemic issues are identified, recorded and addressed through documented problem management processes.
Operational Cyber, Triage and Preliminary Incident Response	1. Quickly assess and respond to operational cybersecurity incidents. 2. Conduct initial triage and containment of security threats. 3. Collaborate with the security team to escalate and mitigate incidents. 4. Contribute to the Agency's alignment to the SACSF framework in domains relevant to day-to-day operations.	• Cyber security incidents are triaged, contained and escalated in accordance with the DHUD Cyber Security Procedures and approved playbooks. • Security incidents and vulnerabilities are remediated or risk-accepted in line with DHUD security governance requirements and other cybersecurity obligations. • Required evidence, reporting and post-incident reviews are completed as defined by approved procedures.
Operational Service Design, Configuration, Maturity Uplift and Continuous Improvement	1. Contribute to the design and configuration of operational ICT services and provide those services in a highly effective manner.	• Continuous improvement initiatives are delivered in line with approved DHUD ICT priorities and governance arrangements. • Operational procedures and services are periodically reviewed

	2. Lead and participate in initiatives to improve operational maturity. 3. Drive continuous improvement projects within the ICT department, particularly those associated with streamlining and automating appropriate operational processes to more effectively utilise team capacity. 4. Act as the primary technical representative of the agency in relevant extra-agency working groups and communities of practice, and in whole-of-South Australian Government projects. 5. Share knowledge and contribute to adoption of appropriate industry best practices, including by providing technical skills and process training to junior team members.	and uplifted to maintain alignment with organisational needs, industry good practice and whole-of-government standards. • Repeat incidents are addressed through root cause analysis where required under DHUD ICT processes.
Working with Third-Party Suppliers and Services Providers	1. Collaborate with external vendors, suppliers, and services providers to ensure effective service delivery. 2. Manage relationships effectively.	• Vendor performance is monitored and managed in accordance with applicable contracts, SLAs and DHUD vendor management processes, including identification and escalation of systemic issues.
Writing and Maintaining Operational ICT Procedures	1. Create and update operational procedures, work instructions and similar documentation. 2. Ensure documentation is accurate and accessible. 3. Contribute to administrative processes that facilitate the smooth operations of the ICT team. 4. Participate in invoice processing and assurance activities related to ICT financial operations, ensuring appropriate separation of duties and integrity controls and contributing to successful vendor relationships.	• Operational procedures and work instructions are created, maintained and reviewed in accordance with DHUD documentation, record-keeping and ICT governance standards. • Documentation is published in agreed repositories with clear ownership and accessibility.

The capabilities you will bring

Technical expertise	• Desirable qualifications: Certificate level or above in information technology, or skills gained through study or equivalent workplace experience. • Comprehensive Troubleshooting: Proficient in IT troubleshooting across various domains, including hardware, software, operating systems, and networking, enabling efficient problem resolution within a Microsoft Windows / M365 environment, across cascading levels of complexity. • Triage, prioritisation and incident response: Expertise in quickly and effectively assessing and responding to operational priorities, including cybersecurity events, to ensure timely resolution and mitigation. • Technical Project Execution: Proficient in executing technical projects within IT operational services, particularly focusing on the hands-on implementation and technical execution aspects. This includes deploying and configuring IT systems, tools, and solutions, ensuring their functionality and alignment with operational objectives. Demonstrates expertise in managing smaller, self-contained initiatives efficiently. • Administration Proficiency: High technical proficiency in the administration of operational information technology systems to ensure stability, security, and optimal performance, especially in the management of user accounts and permissions. Moderate proficiency in the administration of infrastructure and networks.
Personal abilities	• Effective Communication and Documentation: Clear communication with end-users and colleagues, including the creation and maintenance of accessible documentation. • Service Excellence and Collaboration: Maintains a strong service ethos even under challenging circumstances, collaborates effectively with internal and external parties, and represents the agency effectively in technical forums. • Resilience and Workload Prioritisation: Demonstrates resilience and excellent workload prioritisation skills tailored to the demands of the role. Adapts well to the fast-paced and dynamic nature of ICT Operations, ensuring that critical tasks, incident responses, and continuous improvement initiatives receive the necessary attention.
Experience	• Substantial experience as a technical practitioner in ICT operations, encompassing frontline and escalated service desk support, incident response, operational cyber security, system administration and infrastructure management, and resolving complex technical challenges. • Significant involvement in continuous improvement initiatives and enhancing maturity capabilities within the context of ICT operations, including initiatives to streamline processes, automate workflows, and optimize time spent on higher value activities. • Knowledge of equal opportunity, equal employment opportunity and occupational health safety and welfare policies and procedures and public sector aims and standards