



POSITION DESCRIPTION

Directorate: Digital Canberra

Position Number: P55384

Division: Customer, Data and Technology

Classification: ASO6

Branch: Data, AI and Digital Records

Location: Gungahlin (Winyu House) with flexible working arrangements agreed with the supervisor

Business Unit: Data and AI Services

Position Title: AI Services Officer

Last Reviewed: May 2026

Position Requirements:

The successful applicant must be an Australian citizen and possess or acquire and maintain an Australian Government Security Vetting Agency (AGSVA) security clearance at the Baseline level as an eligibility qualification. If AGSVA screening is not successful, your employment will not commence or, if already commenced, your employment will be reassessed.

The Australian Capital Territory Public Service (ACTPS) is a values-based organisation where all employees are expected to embody the prescribed core values of respect, integrity, collaboration and innovation, as well demonstrate the related signature behaviours.

DIRECTORATE OVERVIEW

Digital Canberra leads the ACT Government's technology, digital, data, and cyber security services. We strive to improve the lives of Canberrans through delivering and supporting digital government services that are easy to access, save time, and are safe to use. We achieve this while also looking to the future – making technology investment decisions that will transform Canberra into a genuinely connected city.

Digital Canberra leads the implementation of the [ACT Digital Strategy](#) and [ACT Digital Health Strategy](#), manages ICT infrastructure for our hospitals, schools, and public service, and represents the ACT at national digital, data, and cyber security forums. Digital Canberra has a diverse workforce across many functions and sites. We have an inclusive culture, and we ensure our people are respected, valued, and involved.

BRANCH OVERVIEW

The ACT Data, AI and Digital Records Branch (DAIDR) leads Whole-of-Government (WhoG) efforts to maximise the value of data and digital information across the ACT Public Service. It oversees the

strategic direction, governance, and operational management of critical systems such as the ACT's data lake, open data portal and EDRMS (Electronic Digital Records Management System), while driving safe and effective use of data and AI through policy, capability building, and cross-sector collaboration. DAIDR plays a pivotal role in shaping data and AI maturity across the jurisdiction, supporting national data integration priorities, and fostering a culture of safe data sharing.

BUSINESS UNIT OVERVIEW

The Data and AI Services business unit supports the ACT Public Service to manage, share and use government data and AI tools in a safe, consistent and strategically aligned manner. The unit provides leadership and practical support to ensure that data is recognised and treated as a critical public asset. Data and AI Services works across directorates to enhance the quality, accessibility and governance of ACT Government data and AI, supporting improved policy design, regulatory effectiveness, service delivery and organisational performance. The unit contributes to WhoG data stewardship by strengthening the frameworks, processes and capabilities that enable responsible use of information.

POSITION OVERVIEW

The role supports the enablement, adoption and ongoing delivery of WhoG AI services in line with agreed service models, governance arrangements and priorities. It contributes to the day-to-day operation of AI services, including licensing and access administration, coordination of AI use cases, service monitoring, incident support and continuous improvement to ensure reliable, secure and effective service delivery.

The position works collaboratively with technical, policy, security and governance teams to support pilots and proofs of concept, assist with transitioning successful initiatives into production, and implement governance, assurance and compliance controls within operational services. The role assists with security assurance activities, risk identification, vendor and delivery partner coordination, and the maintenance of service and assurance documentation. It also contributes to a positive team culture and capability development by working constructively with stakeholders and building skills in AI, data and digital service delivery.

The AI is an ever-changing domain that will mean that roles and responsibilities in this position may need to change over time to support new technologies, strategies as well as governance and policy directions.

WHAT YOU WILL DO

AI Service Delivery:

- Provide Solution Architecture support for WhoG AI Implementation.
- Support the management of WhoG AI use cases including:
 - Collaborating with relevant stakeholders to define and track AI use cases across government
 - Prioritisation as well as approval processes.
 - Providing design support and feasibility assessment
- Maintain a WhoG AI register with input from directorates

- Assist in AI implementation planning, delivery, continuous improvement and review.
- Assist in the delivery of AI services such as:
 - Management of current AI tools (eg: Copilot licenses)
 - Identification, testing and approval of new WhoG AI tools (incl new LLMs) in collaboration with other stakeholders including TSB and Cyber Security
 - Support business areas progress AI adoption through use-cases such as: AI-assisted case management, document summarisation/classification, citizen-facing chatbots.
 - Model, Agent and other AI Development
- Support in embedding AI into business processes.
- Support AI product lifecycle management
- Support the provision of advice on data quality readiness. process redesign for AI integration, risk and ethical considerations in operational contexts, and AI Solution Architecture

Security and System Assurance:

- Support the application and operation of security and assurance controls for AI-enabled services and associated data environments.
- Assist in ensuring AI services align with ACT Government and relevant Australian Government security standards and requirements.
- Maintain documentation, evidence and artefacts to support security assurance activities, audits and accreditation processes.
- Support security risk assessments and reviews in collaboration with platform owners and cyber security specialists.
- Assist in identifying and escalating AI-specific risks, issues or control weaknesses for remediation.

Culture and Leadership

- Contribute positively to a collaborative, inclusive and respectful team culture.
- Work constructively with colleagues, stakeholders and service partners across government.
- Demonstrate a willingness to learn and build capability in AI, data and digital service delivery.
- Communicate clearly and professionally, escalating issues and risks as appropriate.

WHAT YOU REQUIRE

The information below describes the capabilities that are required to perform the duties and responsibilities of the position.

Professional / Technical Skills and Knowledge:

- Experience supporting digital, data or AI services in an operational or delivery-focused environment.
- Foundational understanding of AI, data and digital technologies and how they are applied in service contexts.
- Experience supporting service coordination, vendor engagement or contract administration activities.
- Ability to follow governance, security and assurance requirements and operate within established frameworks and controls.

Behavioural Capabilities:

- Contribute effectively to team and service outcomes in a dynamic and evolving environment.
- Work collaboratively with stakeholders and take direction from senior officers.
- Communicate technical or service-related information clearly to a range of audiences.
- Demonstrate sound judgement, professionalism and integrity in service delivery activities.

Compliance Requirements / Qualifications

- This position requires an Australian Government Security Vetting Agency (AGSVA) security clearance at the Baseline level as an eligibility qualification.

WORK ENVIRONMENT DESCRIPTION

The following work environment description outlines the inherent requirements of the role (P55384) and indicates how frequently each of these requirements would be performed. Please note that ACTPS is committed to providing reasonable adjustment and ensuring all individuals have equal opportunities in the workplace.

ADMINISTRATIVE	FREQUENCY
Telephone use	Frequently
General computer use	Frequently
Extensive keying/data entry	Frequently
Graphical/analytical based	Frequently
Sitting at a desk	Frequently
Standing for long periods	Occasionally
Designated workstation	Frequently

**Note: the position works in an Activity Based Work (ABW) environment. Under ABW arrangements, staff do not have a designated workstation/desk.*

STANDARD HOURS	FREQUENCY
Flexible working hours (access to flex time)	Frequently
Fixed or specified start/finish times	Occasionally
Access to Accrued Days Off (ADO's)	Never
Peaks and troughs	Occasionally
Frequent overtime	Occasionally
Rostered shift work	Never

SOCIAL DEMANDS	FREQUENCY
Work with others towards shared goals in a team environment	Frequently
Work in isolation from other staff (remote supervision)	Never
Working in a call centre environment	Never
Working directly with the public	Never

PHYSICAL DEMANDS	FREQUENCY
Distance walking (large buildings or inter-building transit)	Occasionally
Working outdoors	Never

MANUAL HANDLING	FREQUENCY
Lifting 0 – 5kg	Frequently
Lifting 5 – 10kg	Never
Lifting 10kg+	Never
Climbing	Never
Reaching	Never
Bending/squatting	Never
Push/pull	Never
Sequential repetitive movements in a short amount of time	Occasionally

TRAVEL	FREQUENCY
Frequent travel – multiple work sites	Occasionally
Frequent travel – driving	Occasionally
Frequent travel – interstate	Occasionally

SPECIFIC HAZARDS	FREQUENCY
Working at heights	Never
Exposure to extreme temperatures	Never
Operation of heavy machinery e.g. forklift	Never
Confined spaces	Never
Excessive noise	Never
Low lighting	Never
Handling of dangerous goods/equipment	Never
Working with asbestos	Never
Potential to encounter agitated customers	Never
Exposure to potentially distressing case material	Occasionally

OTHER	FREQUENCY
Uniform required	Never
Personal Protective Equipment (PPE) required	Never