



POSITION DESCRIPTION

Directorate: Digital Canberra

Position Number: P72079

Division: Customer, Data and Technology

Classification: Senior Officer Grade C

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: Assistant Director, AI Services

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 and AI enablement.

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 leads the enablement, adoption and lifecycle management of WhoG AI services, ensuring services are trusted, secure, well-governed and deliver measurable value. The position oversees AI service design and delivery, including user engagement, licensing and access management, use case coordination, vendor management, service performance monitoring and benefits realisation across government.

Working closely with policy, technical, security and governance teams, and directorate partners, the role implements and embeds privacy, ethical, security and compliance controls into AI services. It provides evidence-based advice to senior stakeholders on service performance, risks and opportunities, supports system security assurance activities in partnership with Digital Canberra Cyber Security, and contributes to the evolution of the WhoG AI services portfolio through standardisation, reuse and continuous improvement.

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:

- Lead Solution Architecture for WhoG AI Implementation including representing AI in relevant Architecture Governance Groups.
- Translate governance and policy priorities into AI-enabled service transformation opportunities
- Manage 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
- Own a WhoG AI register with input from directorates

- Support stakeholders with AI implementation planning, delivery, continuous improvement and review.
- Deliver 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.
- Run AI product lifecycle management
- Lead 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:

This role focuses on system security assurance for AI and data platforms, rather than operational cyber security. Working closely with the Digital Canberra Cyber Security team, you will:

- Provide assurance over security controls and compliance for AI-enabled services and associated data environments, working in partnership with platform owners and cyber security specialists.
- Ensure alignment with ACT Government and Australian Government security standards (e.g. ISM, PSPF where applicable).
- Implement and maintain proportionate security and assurance controls across data, models and AI services including access control, logging, data protection, monitoring and incident response arrangements.
- Support security risk assessments, accreditation processes and audits in partnership with Digital Canberra Cyber Security.
- Identify, assess and mitigate AI-specific risks (e.g. data leakage, model misuse, prompt injection) through sound design and controls.
- Maintain documentation, artefacts and evidence to support ongoing assurance, compliance and audit readiness.

Culture and Leadership

- Actively contribute to a positive, inclusive and collaborative culture within the branch by modelling respectful behaviours, supporting colleagues and fostering constructive ways of working.
- Build and maintain strong working relationships with senior executives, agency leaders and key stakeholders to support effective adoption, trust and continuous improvement of Whole-of-Government AI services.
- Encourage learning, openness and continuous improvement across analytics and AI services.
- Provide clear, evidence-based advice to senior stakeholders on service performance, emerging risks, adoption challenges and opportunities for improvement.

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:

- Demonstrated experience leading and owning complex digital, data or AI services from concept through to production, operation and continuous improvement.
- Strong conceptual understanding of data and AI platforms, integration and modern delivery approaches, with the ability to provide technical leadership and assurance.
- Demonstrated experience in system security assurance including System Security Plans, supporting accreditation, audits and assurance in partnership with cyber specialists.
- Ability to provide sound, pragmatic technical advice on AI tools, platforms and emerging technologies.

Behavioural Capabilities:

- Deliver high-quality outcomes in complex environments while managing competing priorities.
- Work collaboratively across government, influencing outcomes and negotiating priorities with senior stakeholders without direct line management authority.
- Communicate clearly, translating complex technical concepts into business-friendly language.
- Apply sound judgement to translate strategy and policy into practical delivery outcomes in ambiguous and emerging technology contexts.
- Demonstrate integrity by embedding governance, risk and compliance into all aspects of service delivery.

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 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