



POSITION DESCRIPTION

Directorate: Digital Canberra

Position Numbers: P72062, several

Division: Customer Data and Technology

Classification: Information Technology Officer
Grade 2 (ITO2)

Business Unit: Strategic Asset Management

Location: Hybrid working arrangements
(Winyu House, Gungahlin and work
from home)

Position Title: ICT Facilities Officer

Last Reviewed: August 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 Negative Vetting 1 (NV1) 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 as 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.

DIVISION OVERVIEW

The Customer, Data and Technology Group (CDT) enables a modern, digitally empowered ACT Government. By delivering shared services that are efficient, secure, AI-enabled, and customer-focused the group helps ensure that citizens and businesses benefit from responsive, transparent, and innovative public administration.

The group has a wide range of strategy, policy and operational responsibilities across ACT Government including:

- management of Information Communications Technology services
- service integration and management
- program and project management
- cyber, risk and governance
- strategic asset management
- data and artificial intelligence (AI) including digital records.

BUSINESS UNIT OVERVIEW

The Strategic IT Asset Management Program (SAMP) Branch leads the coordination and oversight of ICT asset maintenance and renewal activities across the ACT Government. The branch adopts a whole-of-government portfolio approach to asset lifecycle planning, ensuring technology assets are managed in a structured, prioritised and sustainable manner.

The branch maintains a consolidated view of the ICT asset landscape, including current state maturity, risks, dependencies and investment priorities. This end-to-end visibility enables informed decision-making on asset renewal and supports the reliability, security and performance of critical government systems and services.

The branch is responsible for developing and implementing ICT asset management strategy, standards and governance frameworks, supported by clear reporting and assurance mechanisms. These provide transparency of portfolio performance, enable risk-based prioritisation, and promote consistent delivery outcomes across government.

Working in close partnership with Technology Services Branch, directorates and delivery partners, SAMP ensures asset lifecycle activities are aligned with operational support models, broader ICT strategies and capital investment programs. Through this integrated approach, SAMP reduces operational risk, improves asset management maturity and supports the long-term sustainability of government technology environments.

POSITION OVERVIEW

The ICT Facilities Officers support the Strategic Asset Management Program (SAMP) by undertaking field audit, asset validation, physical installation, replacement, labelling, remediation, decommissioning and completion evidence activities for approved ICT infrastructure refresh works.

The roles attend ACT Government sites to assess communications rooms, cabinets, racks, patching fields, cabling presentation, wireless access point locations and related infrastructure that may affect refresh planning, installation, supportability or handover. They compare field observations with approved records, including ServiceNow, NetBox, CMDB records, asset registers, network inventory, floor plans, rack elevations and deployment records where relevant, and provide evidence to Asset Assurance teams for modelling, discovery validation, asset data quality and lifecycle planning.

The roles also undertake practical physical refresh tasks within approved work scope, including installation support, labelling, decommissioning, post-refresh checks and targeted cabinet or rack remediation where required to support incoming equipment. They work closely with ICT Facilities, Compliance and Delivery staff, Networks, Infrastructure, operational subject matter experts, project managers, vendors and delivery partners.

WHAT YOU WILL DO

Under the general direction of the Assistant Director of ICT Facilities, Compliance and Delivery and Senior Director, Networks and Infrastructure you will:

- a. Conduct structured technical field audits of communications rooms, cabinets, racks, patching fields, fibre terminations, cabling pathways, wireless access points and related physical ICT infrastructure affected by approved SAMP refresh activities.
- b. Validate asset identity, location, rack position, labelling, patching, port information, physical connectivity and site-readiness evidence, and record findings using approved SAMP methods and templates.
- c. Undertake or support approved physical installation, labelling, decommissioning, post-refresh checks and targeted cabinet or rack remediation activities within authorised work scope.
- d. Reconcile field evidence with digital records, including ServiceNow, NetBox, CMDB records, asset registers, network inventory, floor plans, rack elevations and deployment records where relevant, to support delivery planning and Infrastructure Asset Assurance activities.
- e. Capture clear field evidence, including photographs, mark-ups, labels, diagrams, field notes and exception reports, to support planning, modelling, assurance, outage coordination and operational handover.
- f. Identify and escalate data gaps, record inconsistencies, physical constraints, safety issues or site-readiness matters that may affect refresh delivery, asset confidence, completion evidence or operational acceptance.
- g. This position may be required to participate in an after-hours works.
- h. This position does not involve direct supervision of staff; however requires active collaboration, knowledge sharing and support to other team members.

WHAT YOU REQUIRE

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

Capabilities

Professional / Technical Skills and Knowledge

1. Demonstrated practical experience inspecting, validating or supporting physical ICT infrastructure, including communications rooms, cabinets, racks, patching fields, fibre terminations, cabling pathways, wireless access points and related equipment.
2. Demonstrated ability to undertake or support physical installation, replacement, labelling, decommissioning and post-refresh validation activities within approved ICT refresh work scope.
3. Demonstrated ability to identify, validate, document and reconcile asset, connectivity and site-readiness evidence with approved records, including ServiceNow, NetBox, CMDB records, asset registers, network inventory, floor plans, rack elevations and deployment records.
4. Demonstrated ability to prepare accurate field evidence and exception reports, including photographs, mark-ups, diagrams, labels and field notes, to support refresh planning, assurance, outage coordination and operational handover.

Behavioural Capabilities

5. Demonstrated ability to work collaboratively and communicate clearly across technical, project, operational, vendor and stakeholder groups to deliver shared outcomes.
6. Demonstrated ability to exercise sound judgement, manage competing priorities and escalate issues that may affect delivery, safety, quality or operational readiness.

7. Demonstrated behaviours consistent with the ACTPS values of respect, integrity, collaboration and innovation.

Compliance Requirements

- This role is a Position of Trust and requires you to obtain and maintain an Australian Government NV1 security clearance, or be prepared to transfer an existing security clearance, which will be sponsored by the Digital Canberra Directorate. If you are not successful in obtaining a security clearance, your employment in the role will not commence. If already commenced, your employment will be terminated. To be eligible for an NV1 security clearance, you must be an Australian citizen.
- A current driver licence is highly desirable as the role requires travel to multiple ACT Government sites.
- A construction induction card or equivalent site access credential is highly desirable and may be required for construction or controlled work sites.
- ACMA Open Cabling Registration and relevant structured cabling endorsements are highly desirable.
- Experience with ServiceNow, NetBox, CMDB, IT asset management, network discovery tools, Visio, Excel, floor plans or rack elevation records is highly desirable.

WORK ENVIRONMENT DESCRIPTION

The following work environment description outlines the inherent requirements for the roles of ICT Facilities Officer (P72062, several) 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	Frequently
Designated workstation	Occasionally

STANDARD HOURS	FREQUENCY
Flexible working hours (access to flex time)	Frequently
Fixed or specified start/finish times	Occasionally
Expected to work extensive hours over a significant period due to the nature of the duties	Never
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)	Frequently
Working in a call centre environment	Never
Working directly with the public	Never

PHYSICAL DEMANDS	FREQUENCY
Distance walking (large buildings or inter-building transit)	Frequently
Working outdoors	Occasionally

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

TRAVEL	FREQUENCY
Frequent travel – multiple work sites	Frequently
Frequent travel – driving	Frequently
Frequent travel – interstate	Never

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

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