



POSITION DESCRIPTION

Directorate: Digital Canberra

Position Number: P69891

Division: Digital Health Group

Classification: SITOB

Business Unit: Technology Operations – Security Hub

Location: 2-6 Bowes St, Phillip

Position Title: Director, Cyber Project Lead

Last Reviewed: June 2026

Position Requirements: Note: The position requires the successful applicant to be an Australian citizen and possess or acquire and maintain a security clearance at the Negative Vetting 1 (NV1) level as an eligibility qualification for the position. If 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.

DIVISION OVERVIEW

Digital Health Group provides high-level leadership, management and strategic advice in relation to technology capabilities across the ACT public health system.

We are responsible for:

- implementation and support of the [Digital Health Strategy](#)
- management of technology services and projects
- management of the relationship and services delivery by technology vendors
- development, implementation and maintenance of technology policies and procedures
- information management
- protective security.

BUSINESS UNIT OVERVIEW

Technology Operations

The Technology Operations Branch is responsible for the delivery and operation of technology services to Canberra Health Services and Health and Community Services Directorate, our patients, stakeholders, and partners. We are also together with outsourced service providers responsible for managing the Health Enclave which hosts digital health systems in the ACT. Our services cater to all types of health-related technology including patient monitoring equipment, clinical business applications and critical communications and infrastructure.

POSITION OVERVIEW

The Cyber Technical Project Lead will provide technical and cyber governance expertise across a range of cybersecurity initiatives within a cyber security program. The role will work to achieve broad program outcomes across a range of tasks as required. This will include working with stakeholders to facilitate the uplift of applications and infrastructure, including development of requirements and procurement plans, designing and implementing cyber security solutions and controls, working with internal resources, external consultants and vendors on penetration testing services and development of system security plans.

WHAT YOU WILL DO

Under the broad direction of the Senior Director – Digital Health Security, you will be responsible for:

- Providing leadership and direction to staff and multidisciplinary teams, with demonstrated experience acting in or operating at a Director-level capacity, including proven experience managing teams, managing vendor, and effectively balancing competing priorities in a complex Healthcare ICT and cyber security environment. This position may involve direct supervision of program staff.
- Researching, design and implementation of appropriate security controls and cloud platform technologies to meet compliance requirements for managing risk across infrastructure and business systems hosted on-premises and in internally managed cloud environments, with a focus on continuous improvement.

- Performing the role of project lead by providing specialist security advice, reviewing technical solution design and security controls, and ensuring alignment with ACSC Essential Eight and ACT Government security standards, policies and frameworks.
- Possessing relevant and current experience in conducting security risk assessments within a healthcare service delivery context, and implementation of risk treatment strategies, along with a proven track record in driving the uplift of cyber security risk management, governance frameworks, and compliance processes across the Directorate.
- Facilitating workshops, executive briefings, and stakeholder engagement meetings effectively translating complex cyber security and operational technology risks into clear, actionable insights for clinical, technical, and executive audiences to support informed decision-making.
- Undertaking other duties appropriate to this level of classification that contribute to the Directorate.

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 acting in or operating at a Director-level capacity within large-scale healthcare ICT and cyber security environments, with a strong understanding of the ACSC Essential Eight, cyber security risks, technologies, and their impact on clinical systems, operational technology, and patient service delivery is highly advantageous.
- A sound understanding of ICT service management frameworks such as ITIL would be advantageous.

Behavioural Capabilities

- Ability to liaise effectively with a variety of stakeholders internally, within the business and externally (vendors/external auditors).
- Ability to plan and organise activities well in advance, prioritise workloads and meet set deadlines, considering changing circumstances.
- Well-developed verbal and written communication skills with high level attention to detail, including the ability to accurately clarify, check, and present information.
- Demonstrated commitment to Work, Health and Safety (WH&S) and display behaviours that are consistent with the ACTPS values of Respect, Integrity, Collaboration and Innovation.

Compliance Requirements / Qualifications

The position requires the successful applicant to be an Australian citizen and possess or acquire and maintain a security clearance at the Negative Vetting 1 (NV1) level as an eligibility

qualification for the position. If screening is not successful, your employment will not commence or, if already commenced, your employment will be reassessed.