

| POSITION DESCRIPTION | |
|-----------------------|---|
| Title | Lead Cybersecurity |
| Super Stream | Cyber Resilience & Architecture |
| Department | Digital Innovation |
| Classification | AO8 |
| Agreement | Health and Allied Services, Managers and Administrative Workers Single Enterprise Agreement 2021-2025 |
| Reports to | Manager Resilience & Architecture |
| Accountable to | Director, Cyber Resilience & Architecture |

Organisational Overview

The Royal Women's Hospital (**the Women's**), The Royal Melbourne Hospital (**RMH**), and Peter MacCallum Cancer Centre (**Peter Mac**) are leading Victorian public health services located within the Parkville precinct.

The **Women's** is Australia's foremost specialist hospital for women and newborns, delivering primary and tertiary care through a workforce of more than **2,500 staff**, and is internationally recognised for excellence in care, teaching, and research.

The **RMH** is one of Victoria's largest tertiary health services, providing world-class medical, surgical, and mental health programs. Supported by over **12,000 staff**, RMH is a designated trauma centre and leader in neurosciences, nephrology, oncology, cardiology, and virtual health.

The **Peter Mac** is a global leader in cancer research, education, and treatment, with more than **3,900 staff**, including over **700 researchers**, driving innovation in cancer prevention, diagnosis, and care.

Together, these organisations deliver integrated, research-driven, and patient-centred healthcare to local, state, and international communities.

Department Overview – Digital Innovation Service

The Digital Innovation Service (DI), hosted by the Women's, provides a unified ICT capability across the Parkville Local Health Service Network. DI supports the Women's, RMH, and Peter Mac by delivering shared digital infrastructure, systems, and innovation services critical to their clinical and operational performance.

Between July 2024 and June 2025, DI managed over 139,000 support tickets, supporting than 19,000 staff across the health services, highlighting its essential role in enabling safe, reliable, and connected care across the precinct.

In addition, DI provides services under Service Level Agreements to the Parkville Youth Mental Health and Wellbeing Service (PYMHWS) and limited legacy support to Northern Health and Western Health.

Position Purpose

The Lead, Cybersecurity is responsible for advancing the organisation's cybersecurity strategy, strengthening capability, and overseeing operational security functions to safeguard critical information, systems, and digital services. This role provides expert leadership in managing security risks, mitigating threats, addressing vulnerabilities, and embedding secure-by-design practices across the enterprise.

Operating within the Cyber Resilience & Architecture stream, the position directs the implementation of cybersecurity controls, monitoring, incident response, and continuous improvement initiatives. It ensures that cybersecurity frameworks, standards, and practices are consistently applied across technology teams and digital programs, supporting compliance with regulatory requirements and industry best practices.

The Lead collaborates closely with the Manager, Resilience & Architecture, the Director, technology teams, and business units to strengthen the organisation's cybersecurity posture, anticipate emerging threats, and deliver secure, resilient, and reliable digital environments

Key Responsibilities

Cyber Resilience & Architecture

- Lead the development, implementation and continuous improvement of cybersecurity frameworks, controls and standards.
- Oversee security operations activities including monitoring, detection, vulnerability management and incident response.
- Provide expert advice on secure-by-design principles, ensuring cybersecurity is embedded across solution designs, projects and platforms.
- Conduct security risk assessments and support remediation activities to address identified risks and vulnerabilities.
- Monitor emerging threats, industry trends and regulatory requirements, ensuring proactive adaptation of cybersecurity strategies.
- Support the integration of cybersecurity practices within enterprise architecture and resilience frameworks.

Strategic Leadership

- Contribute to the development and execution of cybersecurity strategies aligned to organisational priorities and the Director's strategic plan.
- Lead the uplift of cybersecurity maturity through capability development, guidance, governance and continuous improvement.
- Influence technology direction by providing authoritative advice on cyber risks, controls, and security technologies.
- Drive adoption of innovative approaches to threat detection, automation and security resilience.

Operational Performance

- Ensure effective operation of cybersecurity tools, processes and services, maintaining high levels of availability, reliability and responsiveness.
- Oversee incident response activities, coordinating investigations, mitigations and post-incident reviews.
- Ensure timely completion of risk assessments, threat modelling and security assurance tasks.
- Develop and monitor performance indicators and reporting to track the effectiveness of security operations.

People and Culture

- Provide day-to-day guidance and support to triage analysts and frontline support staff.
- Assist with onboarding of new staff by ensuring consistency in triage practices, system use, and customer service expectations.
- Contribute to capability development through coaching, knowledge sharing, and uplift of analysis skills across the team.
- Model professional, customer-focused behaviours and support a culture of teamwork, responsiveness, and continuous improvement.
- Support staff wellbeing and contribute to change adoption within the team by reinforcing clear communication and expectations.
- Uphold organisational values and support a safe, inclusive, and respectful workplace.
- Encourage behaviours aligned with organisational values and operational excellence.
- Provide digital services support for all hospital sites supported by the Digital Innovation.
- Participate in daily duty roster support across all supported health service sites as required and scheduled.
- Be available for after-hours on-call support duties across all supported hospital sites as required and rostered.

- Participate in off-site support roster as scheduled.
- Contribute to coordinated teamwork and information sharing.
- Request planned leave promptly and maintain excess leave balances in line with hospital guidelines.
- Submit timesheets and leave requests in accordance with maximum leave balances and attendance requirements.
- Engage in performance management, professional training, and development opportunities as required.
- Complete all mandatory hospital training requirements within specified timeframes.
- Consistently demonstrate hospital values in all interactions and activities.

Stakeholder and Relationship Management

- Build strong relationships with internal stakeholders to promote cybersecurity awareness and support secure delivery of technology initiatives.
- Clearly communicate cybersecurity matters, risks and recommendations to technical and non-technical audiences.
- Represent cybersecurity interests in governance groups, design forums and project discussions.
- Engage with external vendors, industry partners and government bodies to ensure alignment with best practice and emerging standards.

Financial and Risk Management

- Support planning and prioritisation of cybersecurity investments, ensuring value for money and alignment with risk priorities.
- Ensure compliance with relevant security, risk and audit requirements across systems and processes.
- Oversee risk identification, assessment and mitigation activities related to cybersecurity tools, platforms and services.
- Monitor and report on cybersecurity risks, ensuring appropriate controls and actions are implemented.

Key Relationships

| Internal: | External: |
|---|--|
| Chief Digital Information Officer | Victorian Department of Health |
| Partner organisation Board, Chief Executives and Executives | Technology vendors and service providers |
| Directors and Managers within Digital Innovation | Partner health services and universities |
| Clinical, Research, and Corporate Leaders | Research collaborators and innovation partners |

Organisational Relationships

- Number of employees that are consumers of the DI service: **19,000+**

Performance and Accountability

Performance objectives are set annually with the CDIO, focusing on:

- Delivery of strategic digital outcomes
- Service reliability and cybersecurity
- Financial sustainability
- Workforce capability
- Innovation and precinct collaboration

Key Selection Criteria

- Bachelor's degree (or higher) in Business, Healthcare Administration, Information Technology, Digital Health, or a related discipline, or equivalent experience.
- Experience in process improvement, operations, or digital transformation within healthcare or similarly regulated environments.
- Working knowledge of RPA, AI, and intelligent automation, with the ability to evaluate tools and platforms.
- Understanding of healthcare operations, patient workflows, and regulatory requirements.

- Leadership in ICT or digital health, including leading multidisciplinary teams and delivering transformation programs.
- Stakeholder engagement and influence across internal and external groups.
- Strategic thinking in complex service environments.

Inherent Requirements

There are a number of critical work demands (inherent requirements) that are generic across all positions. The generic inherent requirements for this position are detailed below. These may be added to with more specific inherent requirements, if required, by your manager and Occupational Health and Safety.

| Physical Demands | Frequency |
|--|----------------------------------|
| Shift work – rotation of shifts – day, afternoon and night | Occasional |
| Sitting – remaining in a seated position to complete tasks | Frequent |
| Standing- remaining standing without moving about to perform tasks | Occasional |
| Walking – floor type even, vinyl, carpet, | Occasional |
| Lean forward / forward flexion from waist to complete tasks | Rare |
| Trunk twisting – turning from the waist to complete tasks | Rare |
| Kneeling – remaining in a kneeling position to complete tasks | Rare |
| Squatting / crouching – adopting these postures to complete tasks | Rare |
| Leg / foot movement to operate equipment | Not Applicable |
| Climbing stairs / ladders – ascending and descending stairs, ladders, steps | Rare |
| Lifting / carrying – light lifting and carrying less than 5 kilos | Frequent |
| – Moderate lifting and carrying 5–10 kilos | Rare |
| – Heavy lifting and carrying – 10–20 kilos. | Not Applicable |
| Push/Pull of equipment/furniture – light push/pull forces less than 10 kg | Frequent |
| – moderate push / pull forces 10–20 kg | Rare |
| – heavy push / pull forces over 20 kg | Not Applicable |
| Reaching – arm fully extended forward or raised above shoulder | Not Applicable |
| Head / Neck Postures – holding head in a position other than neutral (facing forward) | Not Applicable |
| Sequential repetitive actions in short period of time | |
| – Repetitive flexion and extension of hands wrists and arms | Prolonged/Constant |
| – Gripping, holding, twisting, clasping with fingers / hands | Prolonged/Constant |
| Driving – operating any motor-powered vehicle with a valid Victorian driver's license. | Rare |
| Sensory demands | Frequency |
| Sight – use of sight is integral to most tasks completed each shift | Prolonged/Constant |
| Hearing – use of hearing is an integral part of work performance | Prolonged/Constant |
| Touch – use of touch is integral to most tasks completed each shift. | Prolonged/Constant |
| Psychosocial demands | Frequency |
| Observation skills – assessing / reviewing patients in /outpatients | Prolonged/Constant |
| Problem Solving issues associated with clinical and non-clinical care | Prolonged/Constant |
| Attention to Detail | Prolonged/Constant |
| Working with distressed people and families | Not Applicable |
| Dealing with aggressive and uncooperative people | Rare |
| Dealing with unpredictable behaviour | Rare |
| Exposure to distressing situations | Rare |
| Definitions used to quantify frequency of tasks / demands as above | |
| Prolonged / Constant | 70–100 % of time in the position |
| Frequent | 31–69 % of time in the position |
| Occasional | 16–30% of time in the position |
| Rare | 0–15% of time in the position |
| Not Applicable | |

Employee Responsibilities and Accountabilities

- Be aware of and work in accordance with Hospital policies and procedures, as amended from time to time, including:
 - Code of Conduct
 - Confidentiality
 - Data Accountability Framework
 - Infection Control
 - Occupational Health and Safety
 - Patient Safety
 - Performance Development Management
 - Respectful Workplace Behaviours
 - Risk Management
 - Be respectful of the needs of patients, visitors and other staff and maintain a professional approach in all interactions, creating exceptional experiences.
 - Undertake other duties as directed that meet relevant standards and recognised practice.
 - Our vision is a future free from violence in which healthy, respectful relationships are the norm. Expect all staff to contribute to a culture that promotes gender equity, respect and a safe working environment.
 - The Women's provides pregnancy termination services as part of its public health responsibility to provide safe health care to Victorian women.
 - Data integrity is an essential element of clinical and corporate governance and a key performance indicator. The management of data influences and directly affects patient care, patient decisions, and ultimately the quality and reputation of our service delivery.
- As a consequence all staff are responsible and accountable to ensure that (within their area of work):
- Data recording and reporting, is timely, accurate (ie error free) and fit for purpose.
 - Data management system policies and control processes are complied with on all occasions.
 - Where data issues and/or problems become apparent these matters are immediately referred and reported to supervisors/managers.
- Agree to provide evidence of a valid employment Working with Children Check and provide the necessary details to undertake a national Police check.
 - Expect staff to identify and report incidents, potential for error and near misses and supports staff to learn how to improve the knowledge systems and processes to create a safe and supportive environment for staff and patients.
 - Contributes to a positive and supportive learning culture and environment for health professional students and learners at all levels.

Statutory Responsibilities

- OHS Act 2004
- Freedom of Information Act 1982
- The Victorian Public Sector Code of Conduct

Declaration

I have read, understood and agree to abide by responsibilities and accountabilities outlined in this position description.

Employee Name:

Employee Signature:

Date:

| | |
|-----------------------------|-----------------------------------|
| Developed Date: | December 2025 |
| Developed by: | Chief Digital Information Officer |
| Date of next Review: | December 2026 |
