

Position Title: Cybersecurity Analyst

Campus: Ballarat

Directorate: Chief Financial Officer

Department: Digital Health

Reporting to: Direct: Director of Cybersecurity

Appointment Terms/Conditions:

Classification and Code: Administration Grade 6 (HS6)

Enterprise Agreement: Victorian Public Health Sector (Health Professionals, Health & Allied Services, Managers & Administrative Officers) Multiple Enterprise Agreement.

ORGANISATIONAL INFORMATION

Grampians Health was established on 1 November 2021. Drawing on a regional history of over 150 years, we provide service to over 250,000 Victorians, operate across 21 campuses and sites, and employ more than 7,000 dedicated professionals. Our values reinforce our commitment to providing high-quality, accessible healthcare services close to home. Our mission is to serve the communities of the Grampians region with comprehensive care, ensuring every individual receives the attention they deserve. For more information, visit www.grampianshealth.org.au

Collaboration	Compassion	Accountability	Respect	Innovation
<i>We are stronger together.</i>	<i>We show that we care.</i>	<i>We do what we say and say what we do.</i>	<i>We appreciate and value all people.</i>	<i>We adapt and innovate to achieve best outcomes.</i>
Recognising and utilising strengths to share knowledge, solve problems, build relationships, and deliver the best outcomes possible.	All people deserve to be treated with compassion, kindness, and empathy.	Openness, honesty, and transparency support us to be courageous, take responsibility for our actions and follow through on our commitments	Our actions and words reflect our commitment to a safe and fair health service for all.	Every day, we apply expertise and integrity to make responsible choices, always striving for continuous improvement.

POSITION PURPOSE

The Cybersecurity Analyst role will support the Cybersecurity and Digital Health activities to ensure secure commissioning of technology solutions at Grampians Health, particularly in relation to the Ballarat Base Hospital Redevelopment (BBHR) program of works.

The Cybersecurity Analyst will collaborate closely with the Digital Health teams, BBHR project teams, Grampians Health and Grampians Rural Health Alliance (GRHA) stakeholders, and vendors to determine cybersecurity requirements for technology implementations for BBHR and provide expert recommendations in alignment with our cybersecurity frameworks.

The role will conduct security assessments (such as reviewing system architecture diagrams) to ensure cybersecurity requirements are not overlooked, negotiate outcomes that meet modern cybersecurity requirements, and coordinate risk identification and management activities. This role will offer expert advice in designing enhancements to the organisation's cybersecurity controls, policies, and procedures, thereby strengthening ongoing cybersecurity governance. The role will also consider any uplift requirements of existing technologies to meet overall security requirements.

The role will further ensure through testing and auditing (e.g. vulnerability scans), that the prescribed cybersecurity configurations are effective, that processes are in place to ensure systems security is maintained, and any residual risk is managed.

About the Ballarat Base Hospital Redevelopment (BBHR) Program

The Victorian Government is investing \$655 million for the redevelopment and expansion of the Ballarat Base Hospital. The Victorian Health Building Authority (VHBA) and Grampians Health (GH) will supervise this redevelopment and expansion. This project will include the creation of a new emergency department, a women and children's hub, a state-of-the-art theatre suite, and an additional 100 inpatient and short stay beds. Furthermore, the project entails a new and expanded critical care floor that will consolidate operating theatres, procedure rooms, an expanded intensive care unit, endoscopy suites, and consulting rooms. The final stage of construction is anticipated to be completed by late 2027. Once completed, the hospital will have the capacity to treat at least 18,000 more emergency patients, an extra 14,500 inpatients per year, and support an extra 4,000 surgeries every year.

The BBHR and Operational Commissioning (OCx) programs deliver and transition digital clinical environments for the new hospital tower. The BBHR program team will work with clinical, operational, capital works, technology, and change stakeholders to plan and deliver required service and infrastructure changes, including associated ICT deliverables and operational readiness activities.

Delivery will be undertaken collaboratively with internal and external partners to ensure design, build, transition, and go-live readiness activities align with program timelines and Grampians Health standards.

Knowledge and Understanding

- Working knowledge of information systems security policies, standards and practices (e.g., access control and system hardening, system audit and log file monitoring, security policies, and incident handling) in an enterprise environment
- An understanding of current and emerging cybersecurity threats
- An understanding of modern cybersecurity solutions
- Broad knowledge of current operating systems, modern networks, server infrastructure, identity and access management principles, M365 ecosystem, security management systems, web and application servers and database management systems
- A sound understanding of firewall and endpoint policies in an enterprise environment

Skills

- Strong working knowledge of modern cybersecurity solutions
- Applying cybersecurity tools and procedures within mission-critical environments
- Ability to co-ordinate 3rd parties to provide input to the design process for security configuration and hardening, log events, alerts and analysis
- Advanced problem-solving and analytical skills
- Highly developed verbal communication and interpersonal skills
- Ability to work autonomously and contribute effectively to a team environment
- Ability to anticipate situations and plan accordingly
- Ability to work in an environment of rapid change and development

KEY ACCOUNTABILITIES

Systems Management and Administration

- Assist in ensuring a high standard of cybersecurity by supporting that work undertaken incorporates the appropriate security controls in alignment with our cybersecurity frameworks
- Identify systems vulnerabilities and make appropriate recommendations
- Contribute to day-to-day operations of the cybersecurity team, and ensure consistency in the design and implementation of cybersecurity controls and procedures
- Monitor and maintain key diagnostic cybersecurity systems
- Support the secure provisioning of vendors, contractors, and new staff as required
- Prioritise and action cybersecurity tickets and alerts

Teamwork

- Assist the Digital Health team and BBHR project resources by providing guidance and leadership on cybersecurity matters

Documentation, Planning & Policy Development

- Assist with maintenance of IT Disaster Recovery Plan, and Incident Response Plans
- Assist the Systems Administrators in defining and implementing standard server operating environments
- Assist the Desktop/Endpoint engineers in secure configuration of endpoints including Virtual Desktop Infrastructure (VDI)
- Assisting in the design, implementation, and maintenance of policies, procedures, documentation, and tools in support of the above
- Maintain internal documentation and procedures
- Coordinate policy amendments as required

Management

- Participate in meetings and user groups as requested and required
- Liaise with Digital Health management to contribute to a co-ordinated and cohesive strategy
- Undertake other duties as directed within Digital Health and GRHA teams

Work environment

- Work on-site with the ability to work flexibly if required
- Availability to travel to other GH and partner sites as required

KEY SELECTION CRITERIA

Essential

- Tertiary degree in information technology, computer science or computer systems engineering discipline,
or
Relevant Industry Certifications such as MCSE, MCITP:EA, CEH, CompTIA Security+, CISSP, CISM, CISA, CRISC, CASP+, etc.
or
5+ Years relevant industry experience
- Knowledge and experience Cybersecurity systems and tooling, such as SIEM and EDR
- Understanding of Cybersecurity Governance, Risk and Compliance activities and associated frameworks
- Knowledge and experience in Systems Administration in High Availability environments
- Working knowledge and experience in Networking and security infrastructure
- Experience in delivering IT services in enterprise size organisations
- Have excellent analytical and problem-solving abilities combined with exceptional communication and presentation skills

Desirable

- Knowledge and experience in the Health Sector, including IoMT and Biomedical devices
- Working knowledge of ITSM, M365 Products, cloud offerings/solutions and emerging technologies
- Experience in programming and scripting languages

Personal attributes

- Excellent attention to detail, with demonstrated high level analytical, conceptual, and problem-solving skills.
- **Adaptability:** Maintaining effectiveness when experiencing major changes in work responsibilities or environment; adjusting effectively to work within new work structures, processes, requirements, or cultures.
- **Initiating Action:** Taking prompt action to accomplish objectives; taking action to achieve goals beyond what is required; being proactive.
- **Work Standards:** Setting high standards of performance for self and others; assuming responsibility and accountability for successfully completing assignments or tasks; self-imposing standards of excellence rather than having standards imposed.
- **Stress Tolerance:** Maintaining stable performance under pressure or opposition (such as time pressure or job ambiguity); handling stress in a manner that is acceptable to others and to the organisation.

Interpersonal Skills

- **Building Strategic Working Relationships:** Developing and using collaborative relationships to facilitate the accomplishment of work goals.
- **Communication:** Clearly conveying information and ideas through a variety of media to individuals or groups in a manner that engages the audience and helps them understand and retain the message.
- **Negotiation:** Effectively exploring alternatives and positions to reach outcomes that gain the support and acceptance of all parties.

ORGANISATIONAL REQUIREMENTS

- Grampians Health is committed to a consumer centred approach in the provision of health care and services, consistent with our values, purpose, and vision. It is expected that team members demonstrate the core values of consumer centred care in every interaction.
- All team members of Grampians Health are responsible for supporting the safety, participation, wellbeing, and empowerment of children.
- Quality care is a strategic and operational priority at Grampians Health, achieved through our Governance Framework.
- Participation in the Grampians Health integrated quality improvement and risk management systems by being aware of responsibilities to identify, minimise and manage risks and identifying opportunities for continuous improvement in your workplace through communication and consultation with managers and colleague.
- You must ensure that the affairs of Grampians Health, its patients, clients, and staff remain strictly confidential and are not divulged to any third party except where required for clinical reasons or by law. Such confidentiality shall extend to the commercial and financial interests and activities of Grampians Health.
- In accordance with current legislation and organisational policy, employees must be willing to undertake and maintain a police check, working with children check and where necessary an NDIS Worker screening check. Ongoing employment will be dependent on the provision of satisfactory checks.

OTHER RELEVANT INFORMATION

- At Grampians Health we recognise and respect diversity. Each person has a right to high-quality health care and opportunities regardless of diversity factors which might include aspects such as cultural, ethnic, linguistic, religious background, gender, sexual orientation, age, and socioeconomic status. Inclusiveness improves our service to our community and promotes engagement amongst Grampians Health employees.
- All Grampians Health employees are required to take reasonable care of their own health and safety in the workplace as well as take reasonable care for the health and safety of others who may be affected their acts or omissions. Persons with delegated management functions have an additional duty to provide and maintain a working environment that is safe and free of risks to health, so far as is reasonably practicable in areas where they have management or control. All employees have a duty to report issues they cannot rectify, follow all existing Grampians Health policies and protocols relating to health, safety, wellbeing, and injury management and cooperate with any action taken by Grampians Health to comply with the OHS Act or Regulations.
- Statements included in this Position Description are intended to reflect in general the duties and responsibilities of this position and are not to be interpreted as being all inclusive.
- Management may alter this Position Description if and when the need arises. Any such changes will be made in consultation with the affected employee(s).
- An annual performance review will occur with your Manager. Your performance review is intended to be a positive discussion, outlining the key roles and responsibilities outlined in this Position Description. The performance review discussion provides an opportunity to clarify your role, revise key performance activities and identify any objectives or goals for the year ahead.