Eastern Health

POSITION DESCRIPTION

Position Title:	**Cyber Security Operations Manager**
Award Classification:	**HS4**
Award / Agreement Name:	Administrative Officers (10) Health and Allied Services, Managers and Administrative Workers (Victorian Public Sector) (Single Interest Employers) Enterprise Agreement 2021-2025
Position Reports to:	**Chief Technology Officer**

EASTERN HEALTH – HEALTHIER TOGETHER

Eastern Health is one of Melbourne's largest metropolitan public health services. We provide a comprehensive range of high quality acute, sub-acute, palliative care, mental health, drug and alcohol, residential care, community health and statewide services to people and communities that are diverse in culture, age and socio- economic status, population and healthcare needs

1. POSITION PURPOSE

The Cyber security operations Manager role reporting to the Chief Technology Officer is a hands-on role responsible for managing day to day operations of the extensive security tools and systems whilst leading a team of skilled security engineers.

This role will be responsible for in-depth technical analysis and risk assessment of all security events and incidents including coordination and execution of mandatory security tasks including auditing, reporting, penetration testing and simulation events.

The role demands an in-depth hands-on technical knowledge of security systems and practices including technologies such as EDR, Vulnerability management, Firewalls, Cloud Security, risk control and standards frameworks.

Expertise in leading operational teams and system management is essential for success in this role. In addition to supporting the CIO and CTO Cyber security strategies, roadmap and policies, the Cyber security operations Manager must be able to prioritise work efforts and balance operational tasks and risks

2. MAJOR DUTIES AND/OR RESPONSIBILITIES

The Cyber security operations Manager's job is composed of a variety of activities, including managing operational and technical cyber security program initiatives

- Partner across all IT Teams to ensure that technologies are developed and maintained according to security policies and guidelines.
- Coordinate security communication, awareness and training for audiences, which may range from senior leaders to field staff.
- Work with vendors and the legal and purchasing departments to establish mutually acceptable contracts and service-level agreements.
- Manage production issues and incidents and participate in problem and change management forums.
- Serve as an active and consistent participant in the information security governance process.
- Work with IT and business stakeholders to define metrics (KPI) and reporting strategies that effectively communicate successes and progress of the security program.

- Manage cyber security architecture by working with IT and security staff to ensure that security is factored into the evaluation, selection, installation and configuration of hardware, applications and software.

- Recommend and coordinate the implementation of technical controls to support and enforce defined security policies.
- Research, evaluate, design, test, recommend or plan the implementation of new or updated information security hardware or software, and analyse its impact on the existing environment; provide technical and managerial expertise for the administration of security tools.
- Work with the enterprise architecture team to ensure that there is a convergence of business, technical and security requirements; liaise with IT management to align existing technical foundations and skills with future architectural requirements.
- Develop a strong working relationship with the security engineering team and Department of Health (DoH) cyber team to develop and implement controls and configurations aligned with security policies and legal, regulatory and audit requirements.
- Coordinate, measure and report on the technical aspects of security management and establishment of cyber security working groups
- Manage outsourced vendors that provide information security functions for compliance with contracted service-level agreements.
- Manage and coordinate operational components of incident management, including detection, response and reporting.
- Maintain cyber security playbooks and knowledgebase comprising a technical reference library, security advisories and alerts, information on security trends and practices, and laws and regulations.
- Manage the day-to-day activities of threat and vulnerability management, identify risk tolerances, recommend treatment plans and communicate information about residual risk.
- Manage security projects and provide expert guidance on security matters for other IT projects.
- Assist and guide the disaster recovery planning team in the selection of recovery strategies and the development, testing and maintenance of disaster recovery plans.
- Ensure audit trails, system logs and other monitoring data sources are reviewed periodically and are compliant with policies and audit requirements.
- Design, coordinate and oversee security testing procedures to verify the security of systems, networks and applications, and manage the remediation of identified risks.
- Support the CIO and CTO with cyber security executive and board-level reporting on cyber security performance, governance and risks
- Perform afterhours duties when required.

3. SAFE PRACTICE AND ENVIRONMENT

Occupational Health and Safety

Eastern Health is committed to providing and maintaining a working environment for all staff that is safe and without risk to health. All staff are to take care of their own health and safety and the health and safety of any other person who may be affected by your acts or omissions at the workplace. Understand responsibilities and accountabilities to yourself and others in accordance with OH&S legislation and Eastern Health policies and promote a working environment that is congruent with these guidelines. This includes staff reporting of all clinical and OHS incidents and near misses, particularly those related to Occupational Violence, Manual Handling and Slips, trips and falls.

Staff are required to comply with all state legislative requirements in respect to the Occupational Health and Safety Act 2004 and the Workplace Injury Rehabilitation and Compensations (WIRC) Act 2013.

4. TRAINING AND DEVELOPMENT

Relevant, practical and timely education should direct, facilitate, enhance and support the professional growth and practice of employees in a health environment characterised by change. All programs should endeavour to promote evidence-based practice, a problem-solving approach and to be competency based.

You are expected to participate in the personal development process on an annual basis.

5. QUALITY

As a staff member of Eastern Health staff are required to comply with Eastern Health performance standards and participate in continuous monitoring and improvement as part of your role. You are also required to comply with legislation, professional standards and accreditation standards.

As a staff member employed by Eastern Health services you must have and maintain the appropriate skills and knowledge required to fulfil your role and responsibilities within the organisation. In addition, you must ensure that you practice within the specifications of this position description, and where applicable within the agreed scope of practice.

You are responsible for ensuring safe high-quality care in your work. This will include complying with best practice standards, identifying and reporting any variance to expected standards and minimising the risk of adverse outcomes and patient harm. In addition, you will ensure that service and care is consistent with the EH approach to patient and family centered care.

6. CONFIDENTIALITY

Any information obtained in the course of employment is confidential and should not be used for any purpose other than the performance of the duties for which the person was employed. Staff are bound by the Information Privacy Act 2000 and the Health Records Act 2001.

7. EQUAL EMPLOYMENT OPPORTUNITY

You agree to adhere to the Equal Employment Opportunity policies and practices of the Health Service. Discriminatory practices, including sexual harassment, are unlawful. The Health Service will not tolerate discriminatory behaviour, and any such conduct may lead to the invoking of the Disciplinary Policy and Procedure, which may result in termination of employment.

8. PERFORMANCE DEVELOPMENT

A Performance Review, that includes agreed targets, will occur three (3) months from commencement and then annually on the basis of the duties and responsibilities outlined in this position description. This is an opportunity to review personal and the allocated work unit's service performance, facilitated by the setting of objectives/goals and ongoing evaluation of performance and achievement. Objectives will be developed annually, documented, discussed and agreed with the immediate line manager, who will act as the assessor. The incumbent is expected to demonstrate and show evidence annually of on-going self and allocated work unit's service development.

9. EASTERN HEALTH'S PROMISE

Our promise to our communities, patients, consumers and staff is that we will be **HEALTHIER TOGETHER**. Bolder than a vision for the future, our promise calls us to action. We know that working together is the only way we can achieve what is necessary for a healthier future.

Our values are ones in action and are the behaviours that matter most.

- Respect for all
- Safe always
- Partnering in care
- Learning and improving everyday

Learning from the challenges of the past and looking to the future, we understand that we are building towards a more engaged, more reliable, always safe health service in partnership with our people to improve every day.

10. ATTACHMENTS

- Attachment 1 Key Selection Criteria

11. NOTE

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.

Prior to accepting any offer of employment, prospective employees will be required to read and commit to the Eastern Health Code of Conduct, including (but not limited to) issues of Occupational Health and Safety, Equal Opportunity and Confidentiality.

Vaccination against infectious disease is a mandatory requirement of this role. An offer of employment is conditional on you providing evidence that you are currently vaccinated against COVID-19, prior to commencing employment.

Signed: _____ Date: ____/____/____

Manager

INCUMBENT STATEMENT

I _____(Incumbent Name) have read, understood and accepted the above Position Description and associated Attachments.

Signed: _____ Date: ____/____/____

ATTACHMENT 1

KEY SELECTION CRITERIA

Position Title:	**Cyber Security Operations Manager**
Award Classification:	**HS4**
Award / Agreement Name:	Administrative Officers (10) Health and Allied Services, Managers and Administrative Workers (Victorian Public Sector) (Single Interest Employers) Enterprise Agreement 2021-2025
Position Reports to:	**Chief Technology Officer**

Essential

- Degree in computer science, engineering, or a related field; A minimum of Five years of IT experience, with three to four years in a Senior operational / technical security role with supervisory experience.
- Extensive knowledge and hands-on experience in managing and maintaining
    - EDR Solutions
    - Vulnerability and patch Management systems
    - Cloud security experience
    - Next Generation Firewalls
    - Email protection technologies
    - Cisco Security and SDA network technologies
- Knowledge of security, risk and control frameworks and standards such as ACSC Essential 8, ISO 27001 and 27002, NIST, MITRE ATT&CK, Professional certifications, such as a SSCP, CCSP, GSEC
- The ability to interact with Eastern Health personnel, build strong relationships at all levels and across all business units and organizations, and understand business imperatives.

- A strong understanding of the business impact of security tools, technologies and policies.
- Strong leadership abilities, with the capability to develop and guide information security team members and IT operations personnel, and work with minimal supervision.
- Excellent verbal, written and interpersonal communication skills, including the ability to communicate effectively with the IT organization, project and application development teams, management and business personnel; knowledge and understanding of information risk concepts and principles as a means of relating business needs to security controls; an understanding of information security concepts, protocols, industry best practices and strategies.
- Exposure to developing and maintaining policies, procedures, standards and guidelines.
- Experience in performing risk, business impact, control and vulnerability assessments, and in defining treatment strategies.
- Strong analytical skills to analyze security requirements and relate them to appropriate security controls.
- An understanding of operating system internals and network protocols.
- Experience in system technology security testing (vulnerability scanning and penetration testing).

Desirable

- Experienced with contract and vendor negotiations.
- Experience in identifying cyber risk for regulated entities.
- Previous experience working in a health environment

Aboriginal & Torres Strait Islander Candidates

Eastern Health's Aboriginal Workforce Plan 2023 – 2026 has recently been released. With a strong focus on cultural safety and belonging, actions included in the Workforce Plan provide practical supports for all Aboriginal and/or Torres Strait Islander staff.

An Aboriginal Employment Coordinator is available to ensure each person has culturally safe and positive employee experiences which foster belonging and access to diverse experiences and career pathways.

Should you require further information regarding this positon or support to complete an application, please contact the Recruitment Manager for this position or Eastern Health's Aboriginal Employment Coordinator at Aboriginal.Workforce@easternhealth.org.au