

# Eastern Health

## POSITION DESCRIPTION

<b>Position Title:</b>	<b>Senior Cyber Security Engineer</b>
<b>Award Classification:</b>	<b>HS3</b>
<b>Award / Agreement Name:</b>	Administrative Officers (10) Health and Allied Services, Managers and Administrative Workers (Victorian Public Sector) (Single Interest Employers) Enterprise Agreement 2021-2025
<b>Position Reports to:</b>	<b>Cyber Security Operations Manager</b>

### 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 Senior Cyber Security Engineer will provide expert technical guidance to Eastern Health's cyber security function. Leading by example, to support, investigate and respond to alarms and threats reported to Eastern Health ICT.

**2. MAJOR DUTIES AND/OR RESPONSIBILITIES**

The Senior Cyber Security Engineer role is responsible for the following:

- Respond to security related incidents, either via resolution or escalation to appropriate resolvers and other colleagues and technical resources internal or external to Eastern Health.
- Triage security incidents as they arise, undertakes initial investigations and provides required security incident support and tracking.
- Performs daily and weekly security checks of key systems.
- Monitors security alerts and assesses them for applicability and priority.
- Monitors, and conducts frequent periodic reviews of, security monitoring tools.
- Support the design and implementation of cyber security monitoring frameworks, ensuring advanced threat detection capabilities and real-time analytics.
- Develop and maintain incident response procedures, ensuring Eastern Health ICT is prepared to respond swiftly and efficiently to security events.
- Create, update and maintain Eastern Health Policies, Standards and Guidelines within the review schedule.
- Conduct post-incident analysis to identify lessons learned, refine response strategies, and implement improvements to our controls to prevent future security events, for this TTP (Tactics, Techniques and Procedures)
- Lead proactive threat-hunting activities to identify threats, assess system vulnerabilities and make recommendations to mitigate vulnerabilities before they can be exploited.
- Guide and mentor team members on threat detection and incident response, ensuring effective escalation procedures are in place to promote a positive security culture with a goal of continuous improvement.
- Oversee the vulnerability management process, using existing platforms to develop advanced threat models and prioritising remediation efforts based on business impact.
- Proactively identify and communicate security concerns during system and solution architecture design, application development and infrastructure deployment activities, where we are engaged.
- Provide strategic input to organisational projects, ensuring that security is aligned with the business goals and operational needs.
- Other reasonable tasks to support the cyber security function.

**3. SAFE PRACTICE AND ENVIRONMENT****Occupational Health and Safety**

Eastern Health is committed to provide and maintain 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, in particular 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 centred 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**

<b>Position Title:</b>	<b>Senior Cyber Security Engineer</b>
<b>Award Classification:</b>	<b>HS3</b>
<b>Award / Agreement Name:</b>	Administrative Officers (10) Health and Allied Services, Managers and Administrative Workers (Victorian Public Sector) (Single Interest Employers) Enterprise Agreement 2021-2025
<b>Position Reports to:</b>	<b>Cyber Security Operations Manager</b>

**Essential**

Candidates will be evaluated based on their ability to perform the duties listed above while demonstrating the skills and competencies necessary to be highly-effective in the role. These skills and competencies include:

- 3+ years of experience in a dedicated cyber or information security role
- 5+ years of experience in information technology, preferably supporting large enterprise in a network, cloud, infrastructure or business support role.
- Knowledge of security, risk and control frameworks and standards such as ACSC Essential 8, ISO 27001 and 27002, NIST, MITRE ATT&CK & ITIL.
- Technical understanding of network security knowledge, to include VPN, Firewall, network monitoring, intrusion detection, web server security, and wireless security.
- Strong working knowledge of Microsoft Windows Operating Systems, Active Directory & Group Policy
- Knowledge of common vulnerabilities and exploitation techniques and how to research them to keep abreast of.
- Understanding of database security, content filtering, vulnerability scanning, and anti-malware.
- An understanding of business needs and commitment to delivering high-quality, prompt, and efficient service to the business.
- An understanding of organizational mission, values, and goals and consistent application of this knowledge.
- Excellent written and verbal communication skills. Ability to present information clearly and accurately.
- Strong attention to detail. Ability to analyse and use complex data and information to find trends, solve complex problems and inform reporting.
- Strong Microsoft Office skills and abilities particularly in Excel, Word, PowerPoint and SharePoint.
- Knowledge of and experience with Microsoft SQL and other structure data storage products.
- Demonstrates an ability to clearly communicate to others to modify their opinions, plans, or behaviours.
- Self-motivation and a self-starter, able to look for tasks to undertake with limited direction or supervision.
- High customer service skills, be motivated to develop winning solutions.

**Desirable**

- Working knowledge of Linux/Unix operating systems.
- Previous experience working in a health environment .
- Degree in Computer Science, Information Security, or a related field.
- Knowledge of Power BI or other business intelligence tools.

**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 position 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](mailto:Aboriginal.Workforce@easternhealth.org.au)