# Position Description

| | |
|---|---|
| POSITION TITLE: | Cyber Security Engineer |
| LOCATION: | SAHMRI, North Terrace |
| REPORTS TO: | Head of ICT |
| DEPARTMENT: | ICT |

## PURPOSE AND SCOPE OF THE POSITION

The Cyber Security Engineer will assist in the protection of the organisation's systems, infrastructure and data across on-premises and cloud environments. Reporting to the Head of ICT, the position will be responsible for the design, implementation and maintenance of security controls, leading key security initiatives, and working closely with Infrastructure, Applications, Service Desk and research teams to embed security best practice across IT operations.

As part of the ICT Operations function, the Cyber Security Engineer will provide practical cyber security engineering capability across infrastructure, applications, identity, cloud services, endpoints, monitoring and incident response. The position will support in protecting sensitive research, clinical, corporate and operational data, and secure collaboration with researchers, partners and external service providers. The role also works closely with system owners, project teams and ICT service owners to advise and manage security risks within their areas of responsibility.

## KEY RESPONSIBILITIES

The specific duties include: Standard Responsibilities below, insert role specific responsibilities/duties.

- Design, implement, and support security controls and solutions across on-premises and cloud environments that protect sensitive research, clinical, participant and corporate data.
- Manage and improve core security infrastructure, including firewalls, endpoint protection, Active Directory, and Microsoft Entra ID.
- Monitor systems and networks for threats, investigate incidents, and coordinate effective response and recovery activities.
- Review and support the secure exposure of internal and cloud-hosted applications, including SSO, reverse proxies, secure tunnels, TLS configuration, access controls and monitoring.
- Conduct vulnerability assessments, support remediation activities, and help maintain a strong security posture.
- Strengthen identity and access management practices, including user access, permissions, and secure configuration.
- Provide security input into technology selection, procurement, architecture, implementation and change management processes.
- Support the development and maintenance of security policies, playbooks, standards, and procedures aligned with relevant frameworks and compliance requirements.
- Partner with ICT and business teams to embed security best practice into projects and operational processes.
- Provide guidance, mentoring, and awareness support to help build cybersecurity capability across the organisation.
- Prepare clear reports and updates on risks, incidents, projects, and overall security posture for stakeholders and leadership.
- Participate in special projects to continuously improve processes, tools, systems and organisation.

- Take reasonable care to protect own health, safety and welfare at work and avoid affecting the health and safety of any other person at work.
- Participate in the implementation of the Institute's Work, Health and Safety Management System and related laws, regulations and guidelines.
- Ensure that duties are performed in keeping with the principles outlined in SAHMRI's Vision, Mission and Values and the **Code of Conduct Policy.**

## SPECIAL REQUIREMENTS

- Some out of hours work may be required.
- DCSI Employment Screening and Police Checks may be required.

# Person Specification

## QUALIFICATIONS

- A degree in Cyber Security, Information Technology, Computer Science, or a related field, or equivalent industry experience.
- Relevant cybersecurity certifications will be highly regarded.

## EXPERIENCE, KNOWLEDGE AND SKILLS

- Demonstrated ICT experience, including at least 2 years in a dedicated cybersecurity role.
- Experience supporting security in a small-to-medium ICT team where the role requires both strategic judgement and hands-on delivery
- Proven experience securing Microsoft Active Directory and Entra ID, including identity, access, and authentication management.
- Proven experience securing Windows and Linux environments; exposure to macOS is advantageous.
- Strong network and infrastructure security knowledge, including firewalls, VPNs, intrusion detection/prevention, and monitoring tools.
- Experience with security monitoring, incident response, vulnerability management, SIEM, EDR, and log analysis.
- Practical knowledge of cloud security, particularly Microsoft Azure and hybrid environments.
- Familiarity with security frameworks and compliance requirements such as Essential Eight, NIST, and privacy obligations.
- Identity and access management, including Active Directory, Entra ID, MFA, conditional access, and privileged access tools.
- Windows Server and Linux security hardening, with macOS experience desirable.
- Network and cloud security across firewalls, routers, switches, segmentation, and traffic analysis.
- Threat detection and response using SIEM/SOAR platforms, incident response processes, and security automation tools.
- Vulnerability management, endpoint protection, patching, and secure configuration standards.
- Strong understanding of cybersecurity frameworks, best practice controls, and compliance obligations.

- Demonstrated experience leading or contributing to security projects and initiatives.
- Strong planning, prioritisation, and project delivery skills.
- Excellent communication skills, with the ability to explain technical issues clearly to different audiences.
- A collaborative approach and the ability to build strong relationships across teams.
- A proactive, analytical, and detail-oriented approach to problem-solving.
- The ability to mentor others and promote strong security awareness practices.
- High levels of professionalism, integrity, adaptability, and accountability.

- Support SAHMRI's commitment to reconciliation and acknowledge the importance of working in partnership with Aboriginal and Torres Strait Islander People
- Able to demonstrate the following SAHMRI Values and Culture:
  - **Innovation** – Bold, Driven, Dynamic
  - **Excellence** – Persistent and Focused
  - **Courage** – Collaborative and Enabling
  - **Integrity** – Embrace Diversity, Demand Equity
  - **Teamwork** – Friendly, Fast, Flexible, Fun