Job Description

Position Title	Cyber Security Engineer	**Level**	B
Reports to (role)	Manager, Cyber Security	**Career Stream**	Professional
Team	Information, Communication & Technology		
Location	The Kids Research Institute Australia, Perth Children's Hospital, 15 Hospital Ave, Nedlands		

PURPOSE OF POSITION

The Cyber Security Engineer plays a pivotal role in designing, implementing and maintaining the robust security posture of our systems across on premise and cloud environments.

This role actively contributes to improving the robustness and resilience of our on premise and cloud infrastructure and applications through practical implementation of security controls, monitoring, testing and incident response activities.

This position will also be required to contribute to a positive team culture where excellence, value and customer outcomes are key measures of performance.

KEY RESPONSIBILITIES

Key Responsibilities	Tasks required to achieve Key Responsibilities	Measures
Team Collaboration and Engagement	• Help foster a "secure by design" culture by collaborating with technical teams to integrate security best practice into their workflows and solutions. • Conducting security risk assessments and developing risk mitigation strategies for projects. • Developing, maintaining and communicating security policies and procedures. • Promote and champion integrating security into the software development lifecycle, automating security testing and vulnerability management in the CI/CD pipeline.	• Teams are empowered and enabled to better safeguard the delivery of their solutions. • Risk findings are proactively communicated and addressed. • Policies and procedures are documented and communicated effectively. • Security testing and vulnerability management is integrated into the software development lifecycle.

Customer Service	• Promote and lead a cyber safe culture empowering our teams to improve their cyber security practices across the Institute • Providing guidance and training on best practices for staying safe online. • Educating customers on potential threats, such as phishing scams or malware, and how to avoid them. • Collaborating with customer service teams to ensure that security concerns are properly identified and addressed. • Communicating security updates and alerts to customers in a timely and effective manner. • Work collaboratively with People & Culture to develop and maintain security related training and awareness materials for employees.	• Number of security incidents reported by customers and their resolution time. • Customer satisfaction ratings related to cybersecurity interactions and support. • Improvement in overall customer security awareness and behaviour, as measured by surveys or other methods. • Security updates and alerts are communicated effectively. • Security awareness and training programs are implemented.
Governance	• Reporting on security-related metrics and measures, providing updates to project and executive stakeholders. • Developing and maintaining security policies, procedures, and guidelines including for security controls, such as firewalls, intrusion detection systems, and encryption technologies. • Conducting reviews of security documentation to ensure compliance with industry standards and regulatory requirements.	• Security-related metrics and measures are available and accessible. • Accuracy and completeness of documentation related to security policies, procedures, and controls. • Documentation updates are proactively made in response to changes in security policies, procedures, and controls.
Cyber Security	• Administer and support security applications, including anti-malware and vulnerability scanning tools, to ensure optimal performance and effectiveness. • Investigating and resolving security related issues reported by customers or detected by monitoring systems. • Analyse security incidents to identify root causes, ensuring continuous improvement opportunities are identified and actioned. • Conducting regular security audits and risk assessments to identify potential vulnerabilities and improve overall security posture. • Responding to security incidents and breaches and initiating appropriate remediation activities. • Communicating security updates and alerts to technical support staff and	• Effectiveness of security controls to prevent or mitigate security incidents, measured by reduction in incidents or severity of incidents. • Number and severity of security vulnerabilities identified and remediated in the environment. • Number and effectiveness of security audits or assessments conducted to identify potential risks and vulnerabilities. • Number and

	customers in a timely and effective manner.	effectiveness of incident response and disaster recovery plans and their implementation during actual incidents.
Workplace Safety	• Take reasonable care for your own safety and health and avoid harming the safety and health of others through any act or omission at work. • Identify and assess workplace hazards and apply hazard controls. • Report every workplace injury, illness or near miss, no matter how insignificant they seem. • Abide by The Kids Research Institute Australia policies and procedures.	• Responsibilities are embedded in work practices. • Hazards are effectively managed or reported. • Accidents and incidents are reported in a timely manner. • All applicable safety policies and procedures are sought, understood and implemented.

ESSENTIAL CRITERIA

Qualifications:	Bachelor's Degree in Cyber Security, Computer Science or a related field or equivalent experience.
Essential Skills, Knowledge & Experience:	• Strong analytical and problem-solving skills to identify and mitigate security threats and vulnerabilities. • Proficiency with Vulnerability scanning tools, which includes Microsoft and AWS technologies (M365 suite, Defender, AWS Security Hub). • Demonstrated ability to be self-motivated and work autonomously and as part of a team, with a flexible, positive and collaborative approach. • Excellent verbal and written communication skills, including demonstrated interpersonal skills to effectively communicate security-related information to both technical and non-technical audiences. • Strong understanding of security best practices, standards, and regulations, such as ISO 27001, NIST, Australia Privacy Act, and GDPR. • Knowledge of networking and infrastructure technologies, such as TCP/IP, DNS, and routing protocols. • Understanding of common attack vectors and vulnerabilities, such as social engineering, phishing, and SQL injection. • Technical proficiency and a good understanding of cyber security and contemporary technology (e.g. Cloud, DevSecOps) • Understanding of cryptographic concepts and technologies, such as encryption and digital signatures. • Knowledge of security incident response and disaster recovery planning.

	• Experience in security risk assessments, vulnerability assessments, and penetration testing. • Experience in managing security incidents and breaches.
Desirable Skills, Knowledge & Experience:	• Experience in Essential 8 uplifts/implementations and governance alignments for ISO, NIST standards are beneficial. Previous experience working within a cross functional team. • Experience with CICD and software development practices • Understanding of end point and network security technologies. • Experience with scripting and automation such as PowerShell, python, terraform.

DIRECT REPORTS	None

Approved by:	*Chief Technology Officer*
Date approved:	*28.01.2025*
Reviewed by P&C:	*04.11.2025*