JOB PROFILE FORM

1. JOB DETAILS

WAP (Admin ONLY):

Position Title: Cyber Incident Response Lead

Team: Cyber Security

Division: Technology Strategy & Portfolio

Group: Service Futures

Reports to (Name / Title): Nick MacCallum, Head of Cyber Security

Number of Direct Reports: N/A

Budget Mgt Accountability (Opex & Capex Amounts): N/A

2. WHAT DOES THIS JOB DO?

Job Purpose:

Reporting to the Head of Cyber Security, the Cyber Incident Response Lead is responsible for managing and coordinating the organisation's response to cybersecurity incidents. This role involves developing incident response strategies, and ensuring the organisation is prepared to effectively handle and recover from cybersecurity incidents. The Cyber Incident Response Lead will be a dual role covering cyber incident response and security awareness. This role requires a strong understanding of cyber threats, incident handling procedures, and security awareness techniques whilst working collaboratively with Major Incident Management, Emergency Management, and Learning teams to improve our maturity in these key areas.

Responsibilities (20 dot points or less):

Cyber incident response:

- Lead and coordinate the Cyber team response during incidents, ensuring timely identification, containment, eradication, and recovery.
- Conduct post-incident analysis to identify lessons learned and areas for improvement, updating response plans.
- Plan and coordinate regular cyber incident response simulation exercises and ensure learnings are incorporated into improvement plans.
- Maintain and improve the Cyber Incident Response Plan.
- Develop, implement and maintain incident response playbooks for various scenarios (e.g., ransomware).
- Collaborate with internal teams to ensure an integrated approach to response plans, procedures and risk management. Ensure incident response plans comply with relevant laws, regulations and industry standards.

JOB PROFILE FORM

Security awareness:

- Design, implement and maintain a comprehensive security awareness program that aligns with organisational goals and regulatory requirements.
- Stay current with emerging threats and vulnerabilities.
- Conduct regular vulnerability assessments to identify weaknesses.
- Regularly assess the effectiveness of awareness programs (through phishing simulations, training courses, tests, surveys, etc.).
- Refine training based on training results, best practices and threat awareness.
- Prepare and present reports on awareness program outcomes, engagement metrics, and areas for improvement to management and stakeholders.

JOB PROFILE FORM

3. WHAT ATTRIBUTES ARE REQUIRED TO UNDERTAKE THIS JOB?

3A. WHAT KEY SKILLS OR EXPERIENCES ARE REQUIRED TO COMPLETE THIS JOB?

Skill/ Experience	**Level of Skill/ Experience** i.e. Basic / intermediate/ Advanced	**Years of Experience** (optional)
Experience in a cyber incident response role (either dedicated or a significant part of your role)	Intermediate or greater	
Experience in handling cyber security incidents and simulation exercises	Intermediate or greater	
Experience managing (or working as part of) a security awareness program would be advantageous	Basic or greater	

3B. WHAT DEVELOPMENT BUILDS THE CAPABILITY FOR THIS ROLE?

PEEPS will capture training or certifications that a person requires to undertake their job activities. When completing this section, do not only consider performance effectiveness, but also consider auditing and safety compliance requirements. When a person is associated with a job, but does not have the required skills, the manager and person will be notified.

	Mandatory/ Highly Desirable/ Suggested?	**Method of Training** (e.g. certificate, ticket, observation, on-the-job etc....)	**Renewal Required** (Y/N/Unsure)	**Renewal Frequency** (e.g. Never, 1 year, 5 years etc....)
Qualifications / Certificates				
AIIMS	Desirable		N	N/A
GCIH (or equivalent)	Desirable		N	N/A
SSAP (or equivalent)	Desirable		N	N/A
Tertiary degree in Computer Science, Information Security, or related field	Mandatory			

JOB PROFILE FORM

3C. WHAT ARE THE CRITICAL PERSONAL ATTRIBUTES REQUIRED FOR THIS JOB?

Personal Attributes *i.e., such as resilience, emotional intelligence*	Diligence, resilience, positivity, outgoing, approachable

3D. WHAT ARE THE KEY PHYSICAL, OR ENVIRONMENTAL REQUIREMENTS OF THE ROLE?

Key requirements *i.e. required to lift heavy boxes* *Note: some field-based roles will need to complete additional requirements for the role (Complete this form here)*	Hybrid working - meeting stakeholders, leaders and impacted teams at the Mitcham office and at others sites as directed (e.g. treatment plants etc.) to build a strong understanding of the YVW "business" and to develop trusting and strong relationships with "client" groups

4. WHAT CAREER PATH IS POSSIBLE IN THIS ROLE

PEEPS will hold career path information for jobs within the organisation. This will feed into the PEEPS career and succession planning functionalities. For this job, consider what jobs within the organisation precede and proceed this from a career pathways perspective. Feel free to enter more than one job.

Role before (Name, Team, Division)	
Role after (Name, Team, Division)	

5. CHECKPOINT

Does this role require	☐ Police check ☐ Working with children
Comments	