JOB PROFILE FORM

1. JOB DETAILS

WAP (Admin ONLY):

Position Title: Cyber Analyst

Team: Cyber Security

Division: Technology, Strategy, & Portfolio

Group: Service Futures

Reports to (Role Title): 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:

The purpose of the Cyber Analyst role is to ensure our security operations are managed effectively and efficiently to protect YVW systems and data from cyber threats.

Responsibilities (20 dot points or less):

The key responsibilities for this role include, but are not limited to:

- Ensure security solutions and controls are effective and appropriately managed, updated, and improved (e.g., health checks, tuning, capacity, licensing) to reduce risk of cyber incidents and downtime.
- Work closely with external managed services to ensure they are operating effectively (e.g., assist with SIEM log ingestion, review/adjust agreed response actions, etc.).
- Monitor security alerts, triage, and take any protective actions as required to reduce risk and protect critical systems. Escalate to the Cyber Incident Response Lead where necessary.
- Regularly monitor outputs of vulnerability/ASM/posture management tools and ensure tickets are raised to manage critical vulnerabilities.
- Assist with penetration testing activities – scoping, raising risks for findings, tracking remediation to identify and remediate security vulnerabilities to strengthen YVW's security posture.
- Keep abreast of critical threats/vulnerabilities that may impact YVW and work with teams to promptly mitigate them.
- Review the output from Data Loss Prevention (DLP) tools for data loss events and investigate/report them ensuring the protection of sensitive information and reducing the risk of data breaches.
- Conduct threat hunting based on intelligence from trusted third parties improving threat detection capabilities (e.g., DGS, ACSC).
- Identify security risks and work with the GRC Lead to ensure they are managed via the risk management process.

JOB PROFILE FORM

- Proactively identify process gaps – identify procedures that need to be created, and existing ones that need to be updated/improved to ensure cyber activities are performed to a high/consistent standard.
- Contribute to cyber uplift initiatives as required to improve overall cyber security maturity and resilience across YVW.
- Comply with YVW Information Security Policy and Standards, regulatory requirements (SOCI Act, VPDSS), and best practice framework (NIST CSF).
- Assist with security audits to demonstrate compliance with relevant policies, standards and regulatory requirements (e.g., evidence collection).
- Assist with cyber incidents and simulation exercises as required to enhance incident response readiness and improve ability to detect, contain and recover from cyber security incidents.
- Other duties as required.

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**
Prior experience working in a Cyber Operations role – managing security solutions, vulnerability management, penetration testing, change management, working with external managed services, etc.	Basic	1+
Soft skills: communication, teamwork, problem solving, attention to detail, curiosity and continuous learning.	Intermediate	2+

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

JOB PROFILE FORM

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				
Tertiary qualification in IT or Cyber Security (e.g., Diploma, Degree)	Desirable	TAFE or University	N	Never
Cyber security certifications (e.g., CompTIA Security+, GSEC, CCSK, etc.)	Desirable	Certificate	N	Never

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

Personal Attributes *i.e., such as resilience, emotional intelligence*	• Resilience • Determination • Diligence

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

Key requirements *i.e. required to lift heavy boxes, repetitive work, dealing with irate customers* *Note: some field-based roles will need to complete additional requirements for the role*	Cyber security is a challenging space as we are under attack 24x7, and a target for very sophisticated and highly resourced adversaries. Psychological resilience is a critical attribute to anyone working in this space.

5. 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)	N/A
Role after (Name, Team, Division)	Cyber Operations Lead, Cyber Security, TS&P

JOB PROFILE FORM

6. CHECKPOINT

Is this a *Critical Worker* role requiring an AusCheck	☐ No ☒ Yes
Does this role require	☐ Police check ☐ Working with children
Comments	All Cyber Security team members are required to complete an AusCheck.