Department of the Premier and Cabinet

GOVERNMENT OF WESTERN AUSTRALIA

Job Description Form

Principal Cyber Security Analyst, Level 6 (DPC21061)

Directorate:	Office of Digital Government	Reports to:	Director Cyber Security - Technical
Branch/Section:	Cyber Security Unit/Technical	Supervises:	2 FTE
Location:	Perth Metro		

Our vision is to lead a connected government that delivers a brighter future for Western Australians.

The Department of the Premier and Cabinet (DPC) leads the public sector in providing whole-of-Government advice and support to the Premier and Cabinet in their service of the WA community.

Our areas of responsibility include Office of Digital Government, Intergovernmental Relations and Strategic Priorities, Aboriginal Engagement and Community Policy, Infrastructure, Economy and Environment and State Services.

Join us and work in a role where you can make a real difference to the lives of children, families, individuals and communities throughout Western Australia.

Our values, *Leadership, Connection and Impact*, underpin the way we work.

The Office of Digital Government (DGov) is leading the digital transformation of the WA public sector to support agencies in improving service delivery to the community. This includes providing more convenient access to government services online, and not disadvantaging those who cannot or do not want to use digital services. Ensuring that personal information and data collected, stored and shared by the WA Government is protected is a crucial element of what we do.

About the Role and Responsibilities

Principal Cyber Security Analysts are responsible for the coordination of the cyber security incident response, threat Intelligence and supporting the continuous improvement security operations capabilities to mitigate cyber security threats. Principal Cyber Security Analysts will draw upon their expertise of cyber security threats, cyber situational awareness, incident management and will support agencies in meeting the requirements of the WA Cyber Security Policy.

Cyber Security Tasks

Leadership and Management

- Leads and motivates staff within the Team to coordinate Cyber Security Threat Intelligence and Incident Response activities.
- Promotes a culture supportive of innovation and continuous business process improvement.
- Provides information security policy, technical and operational advice on Cyber Security Threat Intelligence and Incident Response capabilities and processes.
- Works collaboratively with team members and peers to process threat intelligence and incident response workflows effectively and efficiently.
- Management of objective based initiatives to expand cyber security capabilities to the team and peers.
- Develops and maintains information security standards, policies and procedures.

Threat Intelligence & Incident Response Coordination

- Priorities and diagnoses information security breaches, undertakes root cause analysis, and assists in security incident investigation, resolution, and prevention.
- Lead strategic cyber threat intelligence efforts, direct high-impact security investigations, evaluate critical operational risks, and design risk mitigation strategies to strengthen organizational cybersecurity resilience.
- Gather real-time threat intelligence to maintain an accurate operational picture and coordinate with sharing of threat intel to relevant parties.
- Monitors, assesses, and assist in the continual improvement of the performance of information systems security services and controls.

Corporate Responsibilities

- Exhibits accountability, professional integrity and respect consistent with DPC Values, the Code of Conduct, and the public sector Code of Ethics.
- Takes reasonable care to protect your own safety and health at work, and that of others by co-operating with the safety and health policies and procedures of the Department and complying with all provisions of the Work Health and Safety Act 2020
- Undertakes other duties as required.

Work Related Capabilities (Selection Criteria)

1. Well-developed conceptual and analytical skills with the ability to apply these to the treatment of modern cyber security threats and resolve complex problems.
2. Considerable experience in the identification and resolution of information security incidents, against appropriate security frameworks (for example MITRE ATT&CK), principals, policies, and standards.
3. Considerable experience in the use of information security technologies, such as vulnerability management, authentication and access control, next-gen firewalls, data

leakage protection, endpoint protection, endpoint forensics, threat enrichment, SIEM and relevant cloud security solutions.

4. Well-developed written communication skills and interpersonal, and the ability to consult with internal and external stakeholders.
5. Experience working as part of multidisciplinary and cross functional teams and can understand the organisations objectives and align operational activities accordingly.

Desirable

- Possession of or progression towards a relevant tertiary qualification.
- Possession of relevant industry certifications for security (e.g. Security+, CC, SC-200, CSX-P, GSOC, CISSP).
- Knowledge and experience in providing information security services within a government or large corporate environment.

To be eligible for permanent appointment to the role, employees must also be eligible to live and work in Australia indefinitely. Employees engaged on fixed term appointments need a valid work visa for the duration of their contract.

Appointment is also dependent on a 100-point identification check and Criminal Records Screening Clearance.

Certification

Authorising Signature: **People Services:**

Date: **Date:**