Department of
the Premier and Cabinet

GOVERNMENT OF WESTERN AUSTRALIA

Job Description Form

Senior Cyber Security Analyst, Level 5 (DPC20002)

Directorate:	Office of Digital Government	Reports to:	Principal Cyber Security Analyst
Branch/Section:	Cyber Security Unit/Technical	Supervises:	0 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

Senior Cyber Security Analysts are responsible for analysing data collected from various cyber security defence tools and supporting continuous improvement of Security Operational capabilities to mitigate cyber security threats. Senior Security Specialists will draw on their expertise of cyber security threats, incident management and will support agencies in meeting the requirements of the WA Cyber Security Policy.

Cyber Security tasks

- Monitors, assesses and assist in the continual improvement of the performance of information systems security services and controls.
- Coordinates between internal and external partners with respect to the delivery of information security services.
- Identify and analyse cyber threats, investigate security breaches, assess operational impacts, assisting with incident management, and prioritise risk treatments to enhance organizational cybersecurity.
- Coordinates, performs and support scheduled security scans, reviews and compliance testing to ensure adherence to information security policies, standards and procedures and identify and execute against opportunities for improvement.
- Delivers information security awareness and education, based on standards, trends and alerts from appropriate industry and security monitoring services.
- Provides information security policy, technical and operational advice to relevant stakeholders.
- Assists in the development and maintenance of information security policies, standards, procedures and frameworks including but not limited to incident response plans, escalation playbooks and disaster recovery procedures.
- Provides guidance and support to junior staff.

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. Working experience in the identification and resolution of information security incidents, against appropriate security frameworks (for example MITRE ATT&CK), principals, policies, and standards.
3. Working knowledge of information security technologies, such as vulnerability management, authentication and access control, next-gen firewalls, data leakage protection, endpoint protection, 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: