GOVERNMENT OF WESTERN AUSTRALIA

Department of
the Premier and Cabinet

Job Description Form

Senior Cyber Security Analyst - Level 5 (DPC21065)

17 February 2023

Division/Directorate Office of Digital Government	**Branch/Section** Cyber Security/Technical
Reports to Security Operations Centre Manager	**Supervises** NIL

Operational Context:
The Office of Digital Government (DGov) is an Office within the Department of the Premier and Cabinet. DGov leads, supports, and coordinates the digital transformation of the WA public sector.

The Cyber Security Unit leads, coordinates and supports whole-of-government cyber security efforts to protect the WA Government's information, assets, and service delivery from cyber threats.

Role Overview:
Undertakes security event monitoring and advanced analysis of potential incidents across multi-agency networks across the WA Public Sector. Assists in the ongoing development, implementation and maintenance of information systems risk and security controls to protect the information assets of Western Australian Public Sector Agencies. Provides support for incident coordination and response to WA Public Sector Agencies and other Australian jurisdictions.

Role Responsibilities:

- Monitors, assesses, and assists in the continual improvement of the performance of information systems security services and controls.
- Prioritises and diagnoses information security breaches, undertakes root cause analysis and assists in security incident investigation, resolution and prevention.
- 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.
- Coordinates between internal and external services providers with respect to the delivery of information security services.
- 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 Public Sector Agencies.
- Assists in the development and maintenance of information security policies, standards, procedures and frameworks.
- Other duties as required

Corporate Responsibilities:

- Contributes to the achievement of corporate objectives by ensuring that stakeholders are dealt with in a professional and timely manner.
- Works within corporate policies and procedures, acts with integrity and demonstrates ethical behaviours aligned with the Department Code of Conduct.
- Performs other duties as directed.

- 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.*

Role Specific Requirements and Capabilities

(The experience, qualifications and behaviours required to fulfil the role)

- Well-developed conceptual and analytical skills, and the ability to resolve complex problems.
- Can effectively apply the concepts, demonstrated ability to utilise relevant technology to detect and respond to identified threats.
- Knowledge and experience in the identification and management of information technology risks and security vulnerabilities, relevant to on-premise and cloud-computing environments.
- Demonstrated skills in the use 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.
- Demonstrated skills and experience in the resolution of information security breaches, against appropriate security frameworks, principals, policies and standards.
- Well-developed written communication skills and interpersonal, and the ability to consult with internal and external clients, stakeholders and business partners.

Desirable

- Relevant tertiary qualifications and or certificates.
- Possess Industry Certification for example CISSP, CCSP, CRISC, CISM, CSXP and Security+ and/or equivalent qualifications.
- Knowledge and experience in providing information security services within a government or large corporate environment.

Pre-Employment Requirements

To be eligible for permanent appointment to the Department, employees must be eligible to live and work in Australia indefinitely. Employees engaged on fixed term appointments require a valid work visa for the duration of the entire employment contract.

Appointment is subject to:

- 100-point identification check; and
- Criminal Records Screening Clearance
- Baseline/NV1/NV2 Clearance

Certification

Director Signature:

People Services:

Date:

Date: