

Job Description Form

Principal Cyber Security Analyst - Level 6 (DPC21061)

17 February 2023

Division/Directorate

Office of Digital Government

Branch/Section

Cyber Security/Technical

Reports to

Director Cyber Security - Technical

Supervises

2

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:

Leads the Incident Coordination team 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 cyber security situational awareness and coordination of incident response between Public Sector Agencies and other Australian jurisdictions.

Role Responsibilities:

Leadership and Management

- Leads and motivates staff within the Team in the provision of Incident Response Coordination services to Western Australian Public Sector Agencies.
- Promotes a culture supportive of innovation and continuous business process improvement.
- Provides information security policy, technical and operational advice to Public Sector Agencies on their Cyber Security Incident Response capabilities and processes.
- Works collaboratively with other members of the Cyber Security Unit to process cyber incident response workflows effectively and efficiently.
- Develops and maintains information security policies, standards, procedures, and frameworks.

Incident Response Coordination

- Prioritises and diagnoses information security breaches, undertakes root cause analysis, and assists in security incident investigation, resolution, and prevention.
- Provides principal support to the Director Cyber Security – Technical in the management and coordinated response to significant cyber security incidents affecting WA Public Sector Agencies.
- Provides principal support to the Director Cyber Security – Technical in the management and coordinated response to cyber security incidents that fall under the Cyber Incident Management Arrangements for Australian Governments (CIMA).
- Monitors, assesses, and assist in the continual improvement of the performance of information systems security services and controls.
- Responsible for the analysis and reporting of cyber security incidents affecting WA Public Sector Agencies.

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)

- Experience in a supervisory or management capacity.
- Demonstrated written communication and interpersonal skills, and the ability to consult with internal and external clients, stakeholders, and business partners.
- Demonstrated high level skills and experience in the resolution of information security breaches, against appropriate security frameworks, principals, policies, and standards.
- 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, SIEM and relevant cloud security solutions.
- Well-developed conceptual and analytical skills, and the ability to resolve complex problems.

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:

