



Job Description Form



Principal Cyber Security Specialist (Infrastructure) - Level 6 (DPC21072)

9 March 2022

Division/Directorate

Office of the Digital Government

Branch/Section

Cyber Security Unit/Capability

Reports to

Manager Cyber Security Uplift

Supervises

0

Operational Context:

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.

Role Overview:

The Principal Cyber Security Specialist (Infrastructure) is responsible for assisting in designing and implementing programs of work to assist WA Government agencies in increasing their cyber security maturity.

In the context of the Government's digital transformation priorities, the Principal Cyber Security Specialist (Infrastructure) will support the successful implementation of the WA Government Cyber Security Policy to support the Digital Strategy for the Western Australian Government.

Role Responsibilities:**Leadership and Management**

- Within the Branch, promotes a culture supportive of innovation and continuous business process improvement.
- Provides proactive and timely advice to the Director Cyber Security (Capability), Manager Cyber Security Uplift and stakeholders in relation to the cyber security uplift program and initiatives.
- Provides guidance and support to junior staff.

Cyber Security Capability Uplift

- Contributes to the design and implementation of technical services offerings/work packages to provide technical assistance to WA Government agencies, with a focus on Microsoft Cloud (Azure, Office 365, Defender) and hybrid cloud environments.
- Contributes to the creation of whole of government cyber security guidelines and standards to support the WA Cyber Security Policy to address other emerging issues.
- Maintains awareness of emerging cyber security trends/issues to provide contemporary and practical cyber security advice to Government and agencies.

Communication and Engagement

- Building and maintaining positive working relationships with WA Government agencies, as well as inter-jurisdictional and private sector partners.
- Assists in providing expert input into the preparation of reports, briefing notes and correspondence for internal and external stakeholders, including Ministers.

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 Occupational Safety and Health Act 1984.

Role Specific Requirements and Capabilities

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

1. Considerable experience in system administration services, particularly experience in Microsoft Azure, PowerShell, Office 365 services, and the Microsoft Defender suite with practical experience in defining, installation, configuration, tuning and maintenance of corporate systems and networks.
2. Sound knowledge of common enterprise security technologies, for example: End Point Detection and Response, SIEM systems, vulnerability scanners, patch management platforms, application allow-listing tools.
3. Demonstrated experience in implementing security controls aligned with industry standard security frameworks (for example: ASD Essential 8, ASD ISM, NIST Cyber Security Framework, the ISO/IEC 27000-series.)
4. Well-developed communication skills, including written and oral communication, negotiation, influencing and interpersonal skills.
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 relevant industry certificates for technology.
- Possession of relevant industry certifications for security.
- Possession of or progression towards a relevant tertiary qualification
- Experience with other Public Cloud services (Amazon Web Services, Google Cloud Platform)
- Knowledge of the processes of government.

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
- National Criminal Record Screening Clearance

Certification

DDG Signature:

People Services:

Date:

Date: