Department of
the Premier and Cabinet

GOVERNMENT OF
WESTERN AUSTRALIA

Job Description Form

Principal Cyber Security Specialist, Level 6 (DPC21071)

Directorate:	Office of Digital Government	Reports to:	Manager Cyber Security Uplift
Branch/Section:	Cyber Security Unit/Capability	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

Principal Cyber Security Specialists are responsible for contributing to the design, implementation and assurance of cyber security programs that protect information systems from cyber security threats. Principal Cyber security specialists will draw on broad experience in cyber security threats, governance or infrastructure/architecture security, and cyber security frameworks to support agencies in meeting the requirements of the WA Cyber Security Policy.

Cyber Security Tasks

- Designs, configures, or contributes to the implementation of cyber security controls for information systems and system components with a focus on Microsoft Cloud (Azure, Entra, Office 365, Defender) and hybrid cloud environments. Examples include implementing security solutions, performing remediation activities, Essential 8 controls and system hardening.
- Performs security assessments, reviews and compliance testing to ensure adherence to information security policies, standards and procedures and identify opportunities for improvement.
- Contributes to the development and maintenance of information security policies, 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.
- Building and maintaining positive working relationships with WA Government agencies, as well as inter-jurisdictional and private sector partners.
- Contributes to the preparation of reports, briefing notes and correspondence for internal and external stakeholders.
- 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. Considerable experience in contributing to cyber security programs in enterprise IT environments, including cloud computing environments, using industry standard security frameworks (for example: ASD Essential 8, ASD ISM, NIST Cyber Security Framework, the ISO/IEC 27000-series.)
2. Practical experience in the implementation or administration of common enterprise security technologies, for example: End Point Detection and Response, SIEM systems, Endpoint Management, vulnerability scanners, patch management platforms and application allow-listing tools.
3. Experience performing research, analysis, and review of complex cyber/technology problems, and developing evidence-based options, and recommended solutions to resolve problems and mitigate risks.

4. Well-developed communication skills, including written and oral communication, negotiation, influencing and interpersonal skills to engage and build effective relationships 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 project management or IT Service Delivery (e.g. PRINCE2, PMP, Project+, ITIL Foundations)
- Possession of relevant industry certifications for security (e.g. Security+, SC-200, SC-300, CC, CISM, CRISC, CISSP).

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:

Date:

People Services:

Date: