Government of **Western Australia**
Department of the **Premier and Cabinet**

Job Description Form

Senior Cyber Security Tester - Level 6 (DPC21003)

14 January 2021

Division/Directorate Office of Digital Government	**Branch/Section** Cyber Security
Reports to Coordinator Cyber Security Testing	**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 cyber security and technical vulnerability testing of agency systems, networks, and applications. Coordinates the Office of Digital Government's cyber security testing program, including the development of strategies, work plans, technology/tools, and associated program documentation.

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 Manager Cyber Security (Capability) and stakeholders in relation to the penetration testing program.
- Provides guidance and support to junior staff and work experience students.

Penetration Testing

- Supports the planning and management of a whole of government offensive security testing program.
- Works with internal and external stakeholders to execute the security testing program. Contributes to policy support and advice, and contributes to projects to deliver expected outcomes within agreed timeframes.
- Liaises with internal and external stakeholders, including Public Sector Agencies, interstate partners, builds and maintains positive working relationships with them.
- Supports vulnerability testing activities across the DGov, and contributes to internal security testing standards. Assess and advises on the practicality of testing process alternatives.
- Assesses departmental vulnerabilities through design and execution of technical offensive security testing and techniques. Analyses the existence of vulnerabilities, and the effectiveness of defences and mitigating controls.
- Seeks and assesses vulnerabilities across departmental policies, processes and defences in order to improve organisational readiness, training for defensive practitioners and inspects current performance levels.
- Creates test cases using advanced technical analysis of risks and typical vulnerabilities. Provides reports on progress, anomalies, risk and issues associated with test cases.
- Maintains detailed current knowledge of contemporary cyber security threats including exploitation techniques.
- Provides advice and guidance on the planning and execution of security testing. Defines and communicates the test strategy.
- Drafts formal reports for review on testing activities, suitable for consumption by both technical and non-technical audiences.

Other

- Provides support in the preparation and development of presentation materials and reporting processes.
- Participates on, and represents the Office of Digital Government at relevant committees and working parties involved in the development of ICT reform issues and projects.

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. Demonstrated experience in the identification and management of information technology risks and security vulnerabilities, in networks, systems, and software and technologies such as security/penetration testing tools, vulnerability management, authentication and access control, endpoint protection, and relevant cloud security solutions.
2. Well-developed interpersonal and communication skills with the capacity to communicate complex information in a clear, articulate and compelling manner to engage and build effective relationships with internal and external stakeholders
3. Thinks strategically by understanding strategic objectives that influence work goals. Supports a shared purpose and direction and understands and communicates reasons for decision to others. Harnesses information and opportunities by drawing on information from a variety of sources, using own judgement to analyse the information. Shows judgement, intelligence and common sense.
4. Commits to action by taking personal responsibility for meeting objectives and progressing work. Promotes and adopts a positive and balanced approach to work Demonstrates self-awareness and a commitment to personal development by self-evaluating performance and seeking feedback from others.
5. Proven ability to work collaboratively in a team environment and contribute to the achievement of team goals.

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
- Baseline Clearance

Certification

DDG Signature:	**People Services:**
Date:	**Date:**