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

Job Description Form

Cyber Security Testing Coordinator– Level 7 (DPC21002)

14 January 2021

Division/Directorate
Office of Digital Government

Branch/Section
Cyber Security

Reports to
Manager, Cyber Security (Capability)

Supervises
2

Operational Context:
The Office of Digital Government (DGov) leads, supports, and coordinates the digital transformation of the WA public sector. The office consists of three business units: Cyber Security; Digital Transformation and Strategy and Digital Transformation and Technology.

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:
The Cyber Security Testing Coordinator undertakes day to day management of the Office of Digital Government's penetration testing program, including the development of strategies, work plans, technology/tools, and associated program documentation. This is a leading role and performs high quality cyber security and technical vulnerability testing of agency systems, networks, and applications.

Role Responsibilities:

Leadership and Management

- Responsible for leading and motivating staff in the development and achievement of the Office of Digital Government (DGov) penetration testing program business goals.
- As a member of the Cyber Security Unit management team, has shared responsibility for the operations, directions and outcomes of the Unit.
- 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.
- In an environment of constraint, ensures that resources including financial, physical, technological and information requirements are efficiently applied to maintain a high level of products/service delivery.

Penetration Testing

- Coordinates the 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 and private sector service providers, builds and maintains positive working relationships with them.
- Oversees vulnerability testing activities across 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 to public sector agencies on the planning and execution of security testing. Defines and communicates the test strategy.

- Authors formal reports on testing activities, suitable for consumption by both technical and non-technical audiences.
- Responsible for team & vendor management, overall use of resources and initiation of corrective action where required for the penetration testing program.

Other

- Provides support in the preparation and development of presentation materials and reporting processes.
- Provides guidance and support to junior staff and work experience students.
- 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)

- Considerable 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.
- Highly 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
- 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.
- 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.
- Proven ability to work collaboratively and lead 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

Certification

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