**Cyber Security Tester - Level 5 (DPC21075)**

|  |  |  |  |
| --- | --- | --- | --- |
| Directorate:  | Office of Digital Government | Reports to:  | Cyber Security Testing Coordinator |
| Branch/Section:  | Cyber Security | Supervises:  | 0  |
| 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**

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. 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.

### Penetration Testing

* + - * 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.
* Creates test cases using advanced technical analysis of risks and typical vulnerabilities. Provides reports on progress, anomalies, risk, and issues associated with test cases.
* Provides authoritative advice and guidance on the planning and execution of security testing.
* Takes a comprehensive approach to seeking vulnerabilities across departmental policies, processes, and defences in order to improve organisational readiness, training for defensive practitioners and inspects current performance levels.

### Communication Skills

* Interprets, executes, and documents complex test scripts using agreed methods and standards.
* Defines and communicates the test strategy.
* Authors formal reports on testing activities, suitable for consumption by both technical and non-technical audiences.
* Provides specialist advice to support others.
* Provides support in the preparation and development of presentation materials and reporting processes.

### Knowledge update

* Maintains current knowledge of contemporary cyber security threats including exploitation techniques.

### Leadership

* Provides guidance and support to junior staff and work experience students.

### Stakeholder Engagement

* 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

* 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. Demonstrated experience in the identification and management of information technology risks and security vulnerabilities, in networks, systems, and software.
2. Demonstrated experience with information security technologies, such as security/penetration testing tools, vulnerability management, authentication and access control, endpoint protection, and relevant cloud security solutions.
3. Well-developed written communication skills and interpersonal, and the ability to consult with internal and external clients, stakeholders from technical and non-technical backgrounds, and business partners.
4. 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.
5. 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.

**Desirable**

* Relevant tertiary qualifications.
* Relevant industry certification OSCP / OSCE / CREST CCT or CRT.

You 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: |  | People Services: |  |
| Date: |  | Date: |  |