Job Description Form – Cyber Security Administrator

|  |  |  |  |
| --- | --- | --- | --- |
| **Position number:** | 16463 | **Classification:** | Level 5 |
| **Division:** | Corporate Services | **Branch/section:** | Digital and Technology Services |
| **Reports to:** | 16347 – Manager Cyber Security – L7 | **Direct reports:** | Nil |

About the Department

|  |  |  |
| --- | --- | --- |
| Mission | Vision | Values |
| To lead the public sector in community – focused delivery with a high performing organisation and thriving workforce. | Western Australia is celebrated as the best place to live in Australia. | Respectful  Accountable  Responsive  Open-minded  Integrity |

Context

The Corporate Services team includes human resources, payroll, business operations and digital and technology services. It helps the Department of Local Government, Sport and Cultural Industries to reach its mission to enable dynamic and inclusive communities and support the WA economy through effective regulation and the facilitation of outstanding sporting and cultural experiences and opportunities.

Position purpose

Responsible for configuring and managing security tools, technologies and controls to protect information systems and digital assets. Undertakes security reviews, audits and testing to identify vulnerabilities and harden cyber security posture. Responsible for the development of security procedures and providing advice on current, evolving or emerging issues as related to information security.

Responsibilities

1. Implements, configures, manages and optimises security tools and technologies, controls, monitoring and alerting including firewalls, intrusion detection/prevention systems and endpoint protection.
2. Conducts security reviews, audits, testing and information systems risk assessments.
3. Assists in the management of role-based access control and identifies access management solutions.
4. Assists in the detection, triaging, containment, and response to cyber security incidents by gathering information to support analysis, containment and recovery in alignment with procedures.
5. Engages stakeholders to raise awareness of cyber security protection requirements and foster a ‘security first’ culture.
6. Provides technical advice and expertise to stakeholders regarding security matters and provides advice regarding information technology options or solutions that will uplift cyber security posture.
7. Develops and implements procedures and standards for ICT systems to safeguard sensitive and confidential data and associated information.
8. Creates and generates of security reports, dashboards and metrics to evaluate the efficacy of security policies, tools and controls.
9. Contributes to the management of security penetration testing and other cyber security testing programs such as phishing simulations.
10. Adheres to Work Health and Safety, Equal Opportunity and other legislative requirements in accordance with the parameters of the position.
11. Perform any other duties as assigned or necessary to support the objectives of DLGSC.

Work related requirements

This section outlines the necessary minimum requirements, in relation to the knowledge, skills, experience and qualifications required to perform the duties of the position.

Essential

1. Demonstrated experience in implementing, configuring and optimising cyber security technologies, tools and solutions including firewalls, intrusion detection/prevention systems and endpoint protection.
2. Demonstrated experience and knowledge of modern cyber security threats, tools and techniques with ability to detect and analyse threats, respond to security incidents and identify root causes.
3. Sound written communication skills including the ability to prepare presentations, reports, technical documentation and other materials tailored to the target audience.
4. Sound verbal and interpersonal skills with the ability to build productive relationships and capability of communicating technical concepts to diverse stakeholders at all levels.
5. Demonstrated capability to achieve deadlines, self-manage workload and manage competing demands simultaneously with attention to detail and quality.

Desirable

1. Possession of or progression towards a relevant tertiary qualification.
2. Possession of relevant industry certifications for security (e.g. Security+, CC, SC-200, CSX-P, GSOC, CISSP).
3. Proficiency in scripting languages (eg. PowerShell, Python).

Special conditions

Nil

Pre-employment requirements

All department positions require a current Criminal History Check (National Police Certificate or equivalent) and 100-point Identification Check prior to commencement.

|  |  |
| --- | --- |
| Registration date | 7 October 2024 |