# Position Description

TasNetworks | Powering a Bright Future

## Leader Cyber Operations

Digital, Strategy & Customer | Cyber Security

| | |
|---|---|
| Objectives | • Implement, maintain and administer digital cyber security solutions and improve security measures to meet changing business needs .<br>• Lead a team of highly capable security engineers and technical resources who manage and monitor system security.<br>• Work across functional areas of the organisation to promote the importance of Asset and Information Security and support the growth of a positive cyber secure culture.<br>• Provide direction and guidance to evolve the security programs in accordance with strategic objectives, identify and engineer technology initiatives, and develop and enhance defensive measures. |
| Role Specific Accountabilities | • Manage cyber security resources that will identify and analyse technical security risks, threats or vulnerabilities and their potential impact<br>• Oversee the design and implementation of security controls against potential cyber threats and other security risk<br>• The escalation point for security trouble shooting and fault rectification<br>• Build and maintain effective relationships within system owners across the business to build trust and respect for the Cyber Security function<br>• Evaluate, design and implement security technologies to ensure effective and secure implementation and enhancements to the information systems, applications and networks<br>• Integrate cyber security requirements into application development and infrastructure projects<br>• Develop high performing team members to ensure that reliability of services is obtained, and accountability for outcomes is maintained<br>• Proactively monitoring known triggers for critical risks, maintaining effective continuity arrangements, participating in Incident/Executive Management Teams and/or releasing staff for incident management.<br>• Any other duty or task as reasonably and lawfully directed by TasNetworks. |

| | |
|---|---|
| To be successful in this role | • Bachelor's Degree or equivalent work experience required<br>• CISSP, CCSP, or other relevant industry security-focused certifications preferred<br>• Superior experience in leading and managing teams and projects in a highly complex, diverse and challenging business environment<br>• Superior experience in Aptitude for strategic thinking and ability to make recommendations for solutions<br>• Experience working directly with customers, including executives, senior leaders, vendors and subject matter experts, as well as internal teams<br>• Experience in working with AESCSF, CIS Controls or NIST security frameworks<br>• Solid understanding of security protocols, authentication, authorisation and anti-malware platforms<br>• Experience with email security, web filtering, mobile device and other application level security mechanisms<br>• Experience with identity management, federation technologies and concepts<br>• Ability to work under pressure, self-manage, and prioritise tasks to ensure efficiencies<br>• Demonstrated ability to innovate and identify opportunities<br>• Familiar with compliance and privacy regulations such as PCI, SOCI, and other regulations/standards<br>• A high level of confidence to lead and positively influence others<br>• Possess strong interpersonal skills and leadership capabilities |

| | |
|---|---|
| Compliance Requirements | • A satisfactory National Police Record check to confirm eligibility for the role<br><br>• A 'critical worker' suitability assessment for the purposes of the Security of Critical Infrastructure Act 2018 (Cth) (or any successor to that Act) and the Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules 2023 (Cth) (or any successor to those Rules), comprised of:<br>• a National Security Assessment by ASIO;<br>• a Criminal History Check by ACIC; and<br>• a Right to Work in Australia check; |

| Reports to: | Direct reports: | Approved: |
|---|---|---|
| Head of Digital Solutions | 7 | November 2023 |