

# Position Description



Powering a  
Bright Future

## Cyber Security & Data Integrity Leader

Digital Solutions

Transformation, Strategy & Digital

### Objectives

- Lead the governance, monitoring, reporting and delivery of the Network asset management database
- Define policies, procedures, models and technologies to be used in collecting, organising, storing and accessing company data
- Implement, maintain and administer digital cyber security solutions and improve security measures to meet changing business needs

### Role Specific Accountabilities

- Ensure asset essential data and information is known, stored and readily available to the business for consumption in order to enable evidence based decision making
- Design and implement the Asset Management Information System (AMIS) Improvement Program to ensure that the AMIS is on a continual path of improvement to support business requirements
- Manage cyber security resources that will identify and analyse technical security risks, threats or vulnerabilities and their potential impact
- Oversee the design and implementation of security controls against potential cyber threats and other security risk
- Act as escalation point for security trouble shooting and fault rectification
- Evaluate, design and implement security technologies to ensure effective and secure implementation and enhancements to the information systems, applications and networks
- Integrate cyber security requirements into application development and infrastructure projects
- Any other duty or task as reasonably and lawfully directed by TasNetworks

TasNetworks and **you.**

## To be successful in this role

- Superior experience in leading and managing teams and projects in a highly complex, diverse and challenging business environment
- Superior experience in Aptitude for strategic thinking and ability to make recommendations for solutions
- Experience working directly with customers, including executives, senior leaders, vendors and subject matter experts, as well as internal teams
- Experience in working with AESCSF, CIS Controls or NIST security frameworks
- Solid understanding of security protocols, cryptography, authentication, authorisation and anti-malware platforms.
- Experience with email security, web filtering, mobile device and other application level security mechanisms.
- Experience with identity management, federation technologies and concepts.
- Ability to work under pressure, self-manage, and prioritise tasks to ensure efficiencies

### Reports to:

Head of Digital Solutions

### Direct reports:

10-12

### Approved:

November 2022

Our behaviours **be curious** **be brave** own it

