Position Description

Information Security Analyst

Digital, Strategy & Customer | Cyber Security Governance

Objectives

- Support the protection of sensitive data and information assets through proactive governance and operational security measures.
- Establish and maintain the organisation's Information Security Standard, policies and supporting guidance.
- Monitor and improve compliance with the Information Security Standard through tools, controls and assurance activities.
- Build and embed a culture of information security awareness across the organisation.
- Contribute to the overall maturity uplift and continuous improvement of the information security and cyber security functions.

Role Specific Accountabilities

- Develop, implement and maintain the Information Security Standard, policies, and supporting guidance.
- Conduct periodic reviews, audits and gap assessments to track maturity and identify areas for improvement.
- Monitor information security compliance using Data Loss Prevention (DLP) tools.
- Support incident response activities, including the investigation of information security breaches and data loss events.
- Contribute to vendor and third-party risk assessments with an information security focus.
- Deliver or support training, awareness campaigns, and communication initiatives to improve staff knowledge of information security practices.
- Stay informed of emerging threats, trends and regulatory requirements to advise on appropriate controls and improvements relating to information security.
- Provide reporting and insights to leadership on compliance, incidents, and maturity progress.
- Any other duty or task as reasonably and lawfully directed by TasNetworks.

To be successful in this role

- At least 2 years demonstrated experience in information security, governance, risk or compliance role.
- Understanding of information security frameworks and standards (e.g., ISO 27001, NIST)
- Familiarity with data protection technologies such as DLP.
- Strong written and verbal communication skills, with the ability to influence and raise awareness across the business.
- Analytical and problem-solving abilities with attention to detail.
- Ability to balance technical, compliance and business perspectives in decision-making.
- Ability to foster teamwork and collaborative relationships.

Desirable

- Qualifications in Cyber Security, Information Security, or an IT-related discipline.
- Industry certification (e.g., ISO 27001 Lead Implementer, CISSP or equivalent).
- Experience working within critical infrastructure or regulated industries.
- Experience with the Australian Energy Sector Cyber Security Framework (AESCSF) would be highly advantageous.

Reports to:	Direct reports:	Approved:
Cyber Security Governance Lead	0	July 2024