Department of Justice

Tasmania

Office of the Chief Information Officer

Principal Cyber Security Officer – Statement of Duties

Objective

The Principal Cyber Security Officer contributes toward the achievement of the Department's information security objectives by providing specialist cyber security leadership and advice to a wide range of stakeholders across the Department, delivering cyber security programs to improve security practices and technology and ensuring the Department can meet its risk and compliance obligations.

Duties

- Providing high level and in-depth cyber security advice, training, and assistance to a range of stakeholders across the Department
- Assisting stakeholders to implement strategies and initiatives to ensure the Department meets its information security policy, regulatory and statutory security compliance obligations
- Developing information security procedures, policies, guidelines, and standards
- Coordinating Cyber Security Incident Response activities including the development and operation of plans, procedures, and playbooks.
- Leading information security improvement programs and activities
- Contribute to the operation of information security risk management frameworks, processes, and procedures
- Leading information security risk assessments and assisting business units to develop and implement risk treatment plans
- Identifying security training and awareness requirements and developing resources and delivering training programs
- Promoting and advocating cyber security training, culture, and awareness
- Perform other duties as envisaged by the assigned classification under the relevant industrial award or agreement and in accordance with the skills, competence, and training of the occupant.

Level of responsibility

As the Principal Cyber Security Officer, you will:

- Act autonomously in performing the assigned duties, and, as necessary, consult with the Chief Information Security Officer to agree on a suitable course of action
- Provide authoritative specialist cyber security advice and engage, network, and consult with key stakeholders across, and external to, the Department.

- Ensure efficient and effective management of work health, wellbeing, and safety for the areas of responsibility in accordance with the WHS requirements in the WHS Act.
- Our values are we act with Integrity, Respect and Accountability and our workplaces are Inclusive and Collaborative. You are responsible for contributing to our values-based workplace culture, leading your team in a values-based manner, ensuring your team uphold the values and role modelling the values.

Direction and supervision received

The position reports to the Chief Information Security Officer for general direction and supervision, but is expected to operate with a degree of autonomy in accordance with Departmental policies, practices, and procedures.

Selection criteria

1. Excellent communication skills with a proven capability to interpret and articulate complex issues to non-technical stakeholders including cyber security training, together with demonstrated strong written communication skills with an ability to develop policies, procedures, reports, training, and other documentation
2. High level strategic, conceptual analytical and creative skills with demonstrated ability to make sound judgements relating to information security to support complex business requirements and outcomes
3. Demonstrated experience interpreting applicable information security compliance requirements, and develop and execute agreed remediation plans
4. Demonstrated experience implementing and maintaining contemporary information security frameworks and standards, including but not limited to, ISO 27001, the Australian Government Essential 8, Protective Security Policy Framework and Information Security Manual
5. Demonstrated experience in applying risk management processes and procedures across a broad range of stakeholders in diverse and complex environments which are hosted in cloud, hybrid, and on-premises ICT systems.
6. High level technical knowledge of contemporary ICT systems with demonstrated ability to rapidly acquire knowledge and apply information security principles and practices in a continuously evolving environment.

Essential requirements

- Nil

Desirable requirements

- Tertiary qualifications in a relevant discipline
- Industry recognised accreditation in or training towards accreditation in Cyber Security
- Industry experience in a similar role

Pre-employment Checks

The Head of State Service has determined that the person nominated for this vacancy is to satisfy a pre-employment check before taking up the appointment, promotion or transfer.

The following checks are to be conducted:

1. Pre-employment checks
   - Arson and fire setting
   - Violent crimes and crimes against the person
   - Sex-related offences
   - Drug and alcohol related offences
   - Crimes involving dishonesty
   - Crimes involving deception
   - Making false declarations
   - Malicious damage and destruction to property
   - Serious traffic offences
   - Crimes against public order or relating to the Administration of Law and Justice
   - Crimes against Executive or the Legislative Power
   - Crimes involving Conspiracy
2. Disciplinary action in previous employment.
3. Identification check.

Position Summary

Title	Principal Cyber Security Officer
Number	357708
Award	Tasmanian State Service Award
Classification	General Stream Band 7
Output Group	Corporate Strategy and Policy
Full Time Equivalent	1.0
Division	Office of the Chief Information Officer
Branch	Office of the Chief Information Officer
Supervisor	Chief Information Security Officer
Direct Reports	Nil
Location	Hobart
Position category and funding	A752