DEPARTMENT OF HEALTH

Statement of Duties

Position Title:	Manager - Cybersecurity Operations
Position Number:	526722
Classification:	General Stream Band 7
Award/Agreement:	Health and Human Services (Tasmanian State Service) Award
Group/Section:	Health ICT - Cybersecurity Services
Position Type:	Fixed-Term, Full Time
Location:	South, North, North West
Reports to:	Senior Manager - Cybersecurity Services
Effective Date:	December 2021
Check Type:	Annulled
Check Frequency:	Pre-employment
Desirable Requirements:	Appropriate tertiary qualifications in business management, ICT, information management or a cybersecurity related discipline A security clearance of Negative Vetting 1 (Secret) or the ability to obtain one Current Driver's Licence
Position Features:	Some regular out of hours work or oncall may be required to meet specific needs and/or deadlines

NB. The above details in relation to Location, Position Type and Work Pattern may differ when this position is advertised – please refer to these details within the actual advert. The remainder of the content of this Statement of Duties applies to all advertised positions.

Primary Purpose:

The Manager - Cybersecurity Operations will:

- Oversee the development and execution of the Department of Health's (DoH) Cybersecurity Operations capability, focusing on delivering cybersecurity services spanning threat detection, threat intelligence, vulnerability management, and incident readiness planning and response.

- Manage the cybersecurity operations team, including, but not limited to, day-to-day cyber operations activities and personnel management, ongoing development and improvement of the function and relevant measurement and reporting.

Duties:

1. Manage the day-to-day operation of the DoH Cybersecurity Operations function, including developing, integrating, implementing, and evaluating complex cybersecurity requirements with a focus on operational cybersecurity detection and response activities.
2. Assist management in overseeing the human and financial resources for the Cybersecurity Operations team. This may also include the performance and development of staff.
3. Provide expert and authoritative advice and regular and ad-hoc reporting to senior management on cybersecurity operational matters, including threats, vulnerabilities, incidents, and adoption of new technologies and practices; and provide input into cybersecurity and ICT strategy.
4. Provide high-level specialist advice to clients, staff, management and other internal and external stakeholders and service providers/vendors, contributing to the overall strategic direction and management of DoH Cybersecurity Services and work in collaboration with senior management to identify risks and develop and/or implement improvements to established plans and systems.
5. Analyse and identify system maintenance, technical solutions, and improvement opportunities to enhance the overall effectiveness of DoH Cybersecurity Operations, including evaluating current, and future, Cybersecurity Services performance through the development and implementation of operational strategies, policies, and procedures.
6. Develop and maintain productive relationships and strong communication links with clients, other staff and managers within Health ICT, and key internal and external stakeholders and service providers/vendors.
7. Represent the Agency on working parties, interdepartmental committees, planning bodies and other groups, providing options and solutions for service improvement, as required.
8. The incumbent can expect to be allocated duties, not specifically mentioned in this document, that are within the capacity, qualifications and experience normally expected from persons occupying positions at this classification level.

Key Accountabilities and Responsibilities:

Under the broad direction of the Senior Manager - Cybersecurity Services, and within delegated authority and the areas of responsibility, the Manager - Cybersecurity Operations will:

- Be responsible for managing the day-to-day operation of the DoH Cybersecurity Operations function, providing high-level specialist cybersecurity advice services to a variety of personnel.
- Assist management in overseeing human and financial resources.
- Utilise initiative and professional judgement in undertaking day to day tasks, including working with considerable autonomy, and identifying risks and developing and/or implementing operational strategies, policies and procedures.

- Where applicable, exercise delegations in accordance with a range of Acts, Regulations, Awards, administrative authorities and functional arrangements as mandated by Statutory office holders including the Secretary and Head of State Service. The relevant Unit Manager can provide details to the occupant of delegations applicable to this position.
- Comply at all times with policy and protocol requirements, including those relating to mandatory education, training and assessment.
- Actively participate in and contribute to the organisation's Quality & Safety and Work Health & Safety processes, including in the development and implementation of safety systems, improvement initiatives, safeguarding practices for vulnerable people, and related training.

Pre-employment Conditions:

It is the Employee's responsibility to notify an Employer of any new criminal convictions during the course of their employment with the Department.

The Head of the State Service has determined that the person nominated for this job is to satisfy a pre-employment check before taking up the appointment, on promotion or transfer. The following checks are to be conducted:

1. Conviction checks in the following areas:
    a. crimes of violence
    b. sex related offences
    c. serious drug offences
    d. crimes involving dishonesty
2. Identification check
3. Disciplinary action in previous employment check.

Selection Criteria:

1. Demonstrated high-level specialised expertise, knowledge, and experience in providing cybersecurity services within a large organisation and an understanding of future trends within cybersecurity and ICT technologies, including a proven understanding of ICT systems, networks, and concepts.
2. Highly developed strategic, conceptual, analytical, and creative reasoning skills to develop and make sound judgments about the application of ICT, including having extensive experience and skills in cybersecurity research, planning, analysis, and problem-solving.
3. Proven-high level interpersonal and communication skills, including oral and written, together with negotiation, conflict resolution and consultancy skills, and the ability to liaise effectively with staff, management, and a wide range of internal and external stakeholders.
4. Demonstrated highly developed management skills and expertise to lead a team to provide cybersecurity services efficiently and effectively, including managing individual and team professional development opportunities.
5. Ability to work effectively as a member of the team, assist management in overseeing human and financial resources, and support individual and team professional development opportunities.

Working Environment:

The Department of Health is committed to improving the health and wellbeing of patients, clients and the Tasmanian community through a sustainable, high quality and safe health system. We value leading with purpose, being creative and innovative, acting with integrity, being accountable and being collegial.

The Department seeks to provide an environment that supports safe work practices, diversity and respect, including with employment opportunities and ongoing learning and development. We value the diverse backgrounds, skills and contributions of all employees and treat each other and members of the community with respect. We do not tolerate discrimination, harassment or bullying in the workplace. All employees must uphold the *State Service Principles* and *Code of Conduct* which are found in the *State Service Act 2000.* The Department supports the Consumer and Community Engagement Principles.