DEPARTMENT OF HEALTH

Statement of Duties

Position Title:	Senior Cybersecurity Operations Officer
Position Number:	527317
Classification:	Information and Communication Technology Level 3
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:	Manager - Cybersecurity Operations
Effective Date:	July 2022
Check Type:	Annulled
Check Frequency:	Pre-employment
Desirable Requirements:	Appropriate tertiary qualifications in 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:	From time to time, the role may require: • Some duties to be undertaken outside normal working hours • Travel between sites to be undertaken • Intra- and/or Interstate travel

Note: 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 Senior Cybersecurity Operations Officer will deliver high level cybersecurity operations capability, focusing on threat detection, threat intelligence, vulnerability management, and incident response and support the Department in ongoing development of cybersecurity operations strategy and capability.

Duties:

1. Undertake the day-to-day operation of the DoH Cybersecurity Operations function, delivering services to enable the detection, analysis, response, reporting, and the preparation for, and prevention of, cybersecurity incidents.
2. Analyse and disseminate cyber threat intelligence, create and maintain threat profiles and ensure Indicators of Compromise (IOCs) are identified and acted upon.
3. Provide high-level specialist cybersecurity advice to internal and external stakeholders, aiding in the identification, assessment, prioritisation and management of cybersecurity risks.
4. Undertake identification, analysis and tracking of cybersecurity vulnerabilities affecting the organisation, as well as providing assistance and guidance to stakeholders regarding vulnerability remediation.
5. Actively monitor and triage alerts from a suite of security tools and enact appropriate procedures and playbooks in response to cybersecurity threats, including incident investigation, evidence collection and threat hunting activities.
6. Assist in the preparation and ongoing improvement of cybersecurity incident response processes, including participation in table-top exercises with internal and external stakeholders.
7. Assist the Manager – Cybersecurity Operations in the ongoing measurement and reporting of cybersecurity operational matters, including threats, vulnerabilities and incidents.
8. Proactively provide technical leadership, including coordinating and mentoring other team members.
9. Actively identify and implement improvements to the Cybersecurity Operation function's tools and processes.
10. 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 Manager – Cybersecurity Operations, the Senior Cybersecurity Operations Officer is expected to:

- Apply significant expertise and initiative in undertaking operational goals and objectives to efficiently detect and respond to cybersecurity events and incidents.
- Exercise sound judgment, work with minimal supervision and demonstrate autonomy in day-to-day activities.
- Provide authoritative specialised advice and recommendations to guide the business in the identification and management of cyber risk.

- 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. Proven record of achievement in delivering innovative cybersecurity solutions, services and/or expert technical support within a complex work environment.
2. Demonstrated experience working harmoniously and collaborating with technical specialists and non-specialists to foster a productive work ethic and positive workplace culture.
3. Conceptual and problem-solving skills demonstrated through a successful record in analysing and responding to cybersecurity events and incidents, including complex technical investigations within a diverse and fast-paced environment subject to change.
4. Well-developed communication, negotiation and expectation management skills, including proven ability to articulate complex issues to non-technical stakeholders such as senior executives and customers.
5. Self-awareness with a proven capacity to effectively model agile, flexible, and innovative work practices to achieve results.

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.