POSITION DESCRIPTION

Position Title:	Cybersecurity Analyst - Security Operations Centre (SOC)
Business Unit/Department:	DTS Cyber Security
Division:	Digital Technology Services (DTS)
Award/Agreement:	Health & Allied Services, Managers & Administrative Workers (Victorian Public Sector) (Single Interest Employers) Enterprise Agreement
Classification:	HS3
Reports To:	Cyber Security Manager
Direct Reports:	NA
Date Prepared/Updated:	27 July 2025

Position Purpose

The role provides technical support and advice to Western Health on the Information Security risks and controls needed to ensure the design of the processes and technology meets the security requirements of the institution. The position will assist in the development and ongoing maintenance of a comprehensive library of Information Security Design Patterns, Security Principles and Security controls that form the basis of Western Health's design and build of technology solutions.

The DTS Cybersecurity Analyst provides expertise in the Security Information and Event Management and Security Operations Centre (SIEM/SOC), ensuring security events capture and analysis, as well as broader Security Orchestration, Automation, and Response (SOAR). The Analyst effectively identifies, documents, and communicates associated risks (based on ISO 27001, NIST, and the ASD Essential Eight), and recommends mitigating controls to guide Solution Designers in delivering secure and compliant solutions across both cloud and on-premises environments.

The role will achieve continuous DTS security improvements through technical expertise and demonstration of excellent written and verbal communication capabilities. The role will show an acute awareness of the emerging compliance requirements that may impact Western Health and develop plans to meet current and future compliance obligations. The role also has oversight of security across Business as Usual (*BAU*) functions and Projects to ensure security is maintained and operates in an effective manner.

As part of this role, there is a requirement to work through an on-call roster to provide after hour coverage as required.

Business Unit Overview

Western Health Digital Technology Services Division provides leading, innovative, vibrant, and excellent DTS solutions to everyday hospital issues that enable increased productivity and effectiveness to Western Health staff and customers which will ultimately lead to improved patient care.

Purpose statement for DTS Services at Western Health:

- Providing a responsive and high level of Service Delivery through proactive and consultative services that are focused on the business requirements
- Establishing DTS technology as a business enabler by providing an DTS environment that supports the business environment and is agile to business change
- Alignment of business needs and user requirements to DTS value and effectiveness (*particular attention to obtaining the maximum benefits from the DTS investment*)
- DTS services is responsible for DTS infrastructure, software applications, communications (*voice, data and wireless*) and computing services at Western Health

Key Responsibilities

The DTS Cybersecurity Analyst is responsible for:

- Monitoring networks and endpoints for security events, alerts, threats, intrusions, and compromises; assisting the Security team as needed.
- Analysing security events from various sources, including Security Information and Event Management (SIEM) systems, network intrusion detection tools, and identity protection systems
- Reviewing automated alerts and intelligence sources daily to detect and defend against threats targeting systems and data.
- Tracking and assessing emerging threats and vulnerabilities, and ensuring appropriate actions are taken.
- Promptly responding to security incidents, including evidence collection and escalation where necessary.
- Utilising cyber security platforms and applying best practices for security events capture and analysis. Building dashboards based on security events capture.
- Supporting the Cyber Security Manager in the development of Security Orchestration, Automation, and Response (SOAR), enhancing incident response and improving overall security posture.
- Supporting the Cyber Security Manager in delivering ongoing cybersecurity guidance for identity, devices, and data, aligned with the NIST Zero Trust Architecture framework.
- Reviewing, documenting, and enhancing security-related processes to improve the overall security posture.
- Managing security incidents, providing advice and education, and maintaining the health and effectiveness of deployed security tools.
- Collaborating with operations and delivery teams to help them understand and address security requirements and threats.
- Assisting the Cyber Security Manager in assessing Western Health's core systems and third-party vendors for compliance with the organisation's information security policies and controls and producing related reports and recommendations.
- Assisting the Cyber Security Manager in promoting cybersecurity awareness across the organisation, including the delivery of training and education programs.
- Assisting the Cyber Security Manager in the development, standardisation, education, and maintenance of Information Security principles, standards, guidelines, patterns, and controls to protect Western Health's digital environment.
- Report to Cyber Security Manager on matters of security compliance aligned with Western Health's DTS cybersecurity strategy and industry standards, including supporting regular security control testing and continuous improvement.

In addition to the key responsibilities specific to your role, you are required to deliver on the Key Organisational Accountabilities which are aligned with the Western Health strategic aims.

Key Working Relationships

Internal:

- Western Health's DTS Leadership Team and DTS Team Members
- Other Western Health employees and/or guests who may seek advice with regards to Western Health DTS environment

External:

- Vendors of hardware, software or DTS related services, including outsourced services
- Melbourne Health Shared Services teams and Health Shared Services teams

Skills Framework for the Information Age (SFIA)

Information Security – SCTY (SFIA skill level 4)

- Develops and communicates information security policy, standards and guidelines. Contributes to the development of strategies that address information control requirements. Ensures architectural principles are applied during design to reduce risk and drives adoption and adherence to policy, standards and guidelines.

Security Operations– SCAD (SFIA skill level 4)

- Maintains and optimises operational security processes. Checks that all requests for support are dealt with according to established protocols, including for cloud-based and automated systems. Provides advice on implementing and managing physical, procedural and technical security encompassing both physical and digital assets. Investigate security breaches in accordance with established procedures using advanced tools and techniques and recommend necessary corrective actions. Enables effective implementation of recommended security measures and monitors their performance.

Vulnerability Assessment – VUAS (SFIA skill level 4)

- Collates and analyses catalogues of information and technology assets for vulnerability assessment. Performs vulnerability assessments and business impact analysis for medium complexity information systems. Contributes to selection and deployment of vulnerability assessment tools and techniques.

IT governance – GOVN (SFIA skill level 3)

- Reviews information systems for compliance with legislation and specifies any required changes. Responsible for ensuring compliance with organisational policies and procedures and overall information management strategy.

Consultancy – CNSL (SFIA skill level 4)

- Manages provision of consultancy services in own areas of expertise, provides advice and guidance to the client through involvement in the delivery of services. Engages with clients and maintains client relationships.

Technical Specialism – TECH (SFIA skill level 4)

- Provides organisational guidelines to promote the development of specialist knowledge in the organisation. Plans and manages implementation of processes and procedures, tools and techniques for monitoring and managing the performance of automated systems and services.

Testing – TEST (SFIA skill level 4)

- Determines testing policy and owns the supporting processes including software security testing. Takes responsibility for the management of all testing activities within a development or integration project or programme. Manages all risks associated with the testing and takes preventative action when any risks become unacceptable. Assesses and advises on the practicality of testing process alternatives, including automated testing. Initiates improvements to test processes and directs their implementation. Assesses suppliers' development and testing capabilities. Determines project testing standards for all phases, influencing all parties to conform to those standards. Manages client relationships with respect to all testing matters.

Methods and Tools – METL (SFIA skill level 4)

- Promotes and ensures use of appropriate techniques, methodologies and tools.

Service Level Management – SLMO (SFIA skill level 2)

- Monitors and logs the actual service provided, compared to that required by service level agreements.

Selection Criteria

Essential

- The appointee will have:
  - A degree in a relevant field with subsequent relevant experience, and
  - an appropriate industry Certification, and/or
  - an equivalent combination of relevant experience and/or education/training
- Extensive experience with large scale Information Security systems and processes
- Highly developed interpersonal, communication and negotiation skills, with the ability to liaise effectively with internal and external stakeholders. Demonstrated excellent written and verbal communication skills.
- Proven ability to communicate security-related concepts to a broad range of technical and non-technical staff
- Demonstrated awareness of the current trends and threats in Cyber security, for example: Information Security Industry Standards and technologies (*for example: Identity Management; Threat Intelligence; Threat Management; Cloud Security; End-Point Device Protection; Malware control Management, Network Dynamic Micro-segmentation*)
- Exceptional teamwork abilities and a demonstrated capacity to work collegiately and collaboratively with others
- Demonstrated ability to prioritise tasks and delivery a quality service
- Strong understanding of security concepts, including Data Loss Prevention, Encryption, Single Sign On, Multi-Factor Authentication, Certificate-based authentication.
- Awareness of MITRE ATT&CK framework

Desirable

- CISSP: Certified Information Systems Security Professional certification
- DTS/ICT technology experience in a large Health Sector and/or Public Sector environment
- Current licensed car driver valid in the State of Victoria
- Experience and/or certification in IT service management *(i.e. ITIL)*
- Experience with security technologies, including Firewalls, web filtering, NAC, IDS/ IPS, SSO, Certificate Management, SIEM, Endpoint Protection, Vulnerability management.
- Experience with Crowdstrike, MS/Azure Security/Purview, Cisco FTD/ISE/Umbrella/CES, Tenable.io, Forescout, and Cloudflare as well as, common products NDR platforms is highly regarded.

Additional Requirements

All employees are required to:

- Obtain a police / criminal history check prior to employment
- Obtain a working with children check prior to employment (if requested)
- Obtain an Immunisation Health Clearance prior to employment
- Report to management any criminal charges or convictions you receive during the course of your employment
- Comply with relevant Western Health clinical and administrative policies and guidelines.
- Comply with and accept responsibility for ensuring the implementation of health and safety policies and procedures
- Fully co-operate with Western Health in any action it considers necessary to maintain a working environment, which is safe, and without risk to health
- Protect confidential information from unauthorised disclosure and not use, disclose or copy confidential information except for the purpose of and to the extent necessary to perform your employment duties at Western Health
- Be aware of and comply with relevant legislation: Public Administration Act 2004, Victorian Charter of Human Rights and Responsibilities Act 2006, Work Health and Safety Act 2011, the Work Health and Safety Regulations 2011 (and 2012), the Victorian Occupational Health and Safety Act 2004, Public Records Act 1973, Fair Work Act 2009 (as amended), the Privacy and Data Protection Act 2014 and responsibilities under s141 Health Services Act with regard to the sharing of health information
- Be aware of and comply with the Code of Conduct for Victorian Public Sector Employees and other Western Health employment guidelines

General Information

- Redeployment to other services or sites within Western Health may be required
- Employment terms and conditions are provided according to relevant award/agreement
- Western Health is an equal opportunity employer and is committed to providing for its employees a work environment which is free of harassment or discrimination. The organisation promotes diversity and awareness in the workplace
- This position description is intended to describe the general nature and level of work that is to be performed by the person appointed to the role. It is not intended to be an exhaustive list of all responsibilities, duties and skills required. Western Health reserves the right to modify position descriptions as required. Employees will be consulted when this occurs
- Western Health is a smoke free environment

I confirm I have read the Position Description, understand its content and agree to work in accordance with the requirements of the position.

Employee's Name: Click here to enter the Employee's name.

Employee's Signature: _____ Date: Click here to enter a date.