Position Description

Employment Agreement:	Individual Employment Agreement
Position Title:	**Cyber Security Engineer**
Service & Directorate:	Information Services
Location:	Dunedin
Reports to:	Technology and Services Manager
DHB Delegation Level:	Level 5
Number of direct reports:	0
Date:	

Our Vision

Better Health, Better Lives, Whanau Ora

We work in partnership with people and communities to achieve their optimum health and wellbeing

We seek excellence through a culture of learning, enquiry, service and caring

Our Shared Values and Behaviours

Kind *Manaakitanga*	Open *Pono*	Positive *Whaiwhakaaro*	Community *Whanaungatanga*
***Looking after our people*:** We respect and support each other. Our hospitality and kindness foster better care.	***Being sincere*:** We listen, hear and communicate openly and honestly. We treat people how they would like to be treated.	***Best action:*** We are thoughtful, bring a positive attitude and are always looking to do things better.	***As family:*** We are genuine, nurture and maintain relationships to promote and build on all the strengths in our community.

Our statutory purpose

To improve, promote and protect the health of our population

Promote the integration of health services across primary and secondary care services

Seek the optimum arrangement for the most effective and efficient delivery of health services

Promote effective care or support for those in need of personal health or disability support services

Promote the inclusion and participation in society and the independence of people with disabilities

Reduce health disparities by improving health outcomes for Maori and other population groups

Foster community participation in health improvement and in planning for the provision of and changes to the provision of services

Uphold the ethical and quality standards expected of use and to exhibit a sense of social and environmental responsibility

PURPOSE OF ROLE

The Cyber Security Engineer is responsible for the design, oversight, and ongoing management of the information security program, including policies, procedures, technical systems, and workforce training in order to maintain the confidentiality, integrity, and availability of data within all SDHB information systems. The security officer role addresses electronic systems architecture and functionality as it affects safeguards of protected health information (PHI) and business information assets with a high focus on performing the day to day operations, management and administration to protect the integrity, confidentiality, and availability of the IT systems and data.

Competencies

The following competencies apply to this position. The employee will be assessed against these as part of their annual performance and development review.

Organisational Competencies	
Managing Vision & Purpose	Communicates a compelling and inspired vision or sense of core purpose; talks beyond today; talks about possibilities; is optimistic; creates mileposts and symbols to rally support behind the vision; makes the vision sharable by everyone; can inspire and motivate entire units or organizations.
Integrity and Trust	Is widely trusted; is seen as a direct, truthful individual; can present the unvarnished truth in an appropriate and helpful manner; keeps confidences; admits mistakes; doesn't misrepresent him/herself for personal gain.
Managerial Courage	Doesn't hold back anything that needs to be said; provides current, direct, complete, and "actionable" positive and corrective feedback to others; lets people know where they stand; faces up to people problems on any person or situation (not including direct reports) quickly and directly; is not afraid to take negative action when necessary.
Informing	Provides the information people need to know to do their jobs and to feel good about being a member of the team, unit, and/or the organization; provides individuals information so that they can make accurate decisions; is timely with information.
Planning	Accurately scopes out length and difficulty of tasks and projects; sets objectives and goals; breaks down work into the process steps; develops schedules and task/people assignments; anticipates and adjusts for problems and roadblocks; measures performance against goals; evaluates results.
Decision Quality	Makes good decisions (without considering how much time it takes) based upon a mixture of analysis, wisdom, experience, and judgment; most of his/her solutions and suggestions turn out to be correct and accurate when judged over time; sought out by others for advice and solutions.

KEY RELATIONSHIPS

Within Southern DHB	External to Southern DHB
• Director of Information Systems	• Ministry of Health
• Technology and Services Manager	• SDHB Stakeholders
• Change Delivery Manager	
• Business Solutions Manager	
• Enterprise Information Architect	
• Digital Relationships Manager	
• Technical Architect	

PERSON SPECIFICATION

The expertise required for a person to be fully competent in the role. Position specific competencies:

	ESSENTIAL	DESIRABLE
Education and Qualifications (or equivalent level of learning)	• Bachelor’s degree required with a major - or field of interest - in information technology or equivalent experience.	• Tertiary qualification required with a major - or field of interest - in information technology.’
Experience	• A minimum of three years of information technology experience with a focus on Cyber Security.	• A minimum of five years’ experience in the Health Industry
Knowledge and Skills	• Experienced in the management of both physical and logical information security systems. • Strong technical skills (applications and operating system hardening, vulnerability assessments, security audits, TCP/IP, intrusion detection systems, firewalls, etc.). • Outstanding interpersonal and communication skills. Pragmatic in approach to addressing risk. • Must possess a high degree of integrity and trust with the ability to work independently. • Excellent documentation skills. • Ability to weigh business risks and enforce appropriate information security measures. • Ability to work collaboratively even in intense situations. • Planning, testing, documenting and analysis of disaster recovery processes and procedures.	
Personal Qualities	• Commitment and personal accountability. • Excellent interpersonal skills, including ability to work effectively with people at all levels of the organisation. • Acts with discretion, sensitivity and integrity at all times. • Is adaptable and flexible – open to change (positive or negative). • Maintains an exceptionally high level of confidentiality.	

KEY RESULT AREAS:

Key Accountabilities:	Example of successful delivery of duties and responsibilities
Overall Information Security of SDHB systems	
• The Cyber Security Engineer will be responsible for maintaining the confidentiality, integrity and availability of the organisations cyber systems and networks. • Responsibility for IT asset management lifecycle with reference to Cyber Security risk. • Continuous development of assurance tools, systems and business processes including but not limited to SIEM, IDS, IPS, AV, ConfigManagement, SOAR which are automated and autonomous with minimal maintenance and upkeep. • Afterhours On-Call	• Annual Penetration testing of perimeter and internal networks. • Detailed Reporting on threats to Information Security and mitigation strategies • High level monitoring of security logs • High level of protection from malware or virus activity. • Assure reliable and secure operational systems 24x7 with 99.99% availability by preventing security incidents • Performing or assisting with investigations • Assist technical teams, key personnel and system owners of achievable solutions to known risks which result in an outcome of remediation or mitigation.
Information Security Policy	
• Establish and maintain Information Security Policies and Standards	• Development and continual review of SDHB Information Security Policy • Responsible for the creation and updating of Information security standards • Supporting the implementation of Ministry of Heath mandates into organisation workflows, processes and policy.
Information Security Policy	
• Planning, testing, documenting and analysis of disaster recovery processes and procedures.	• Annual DR restore testing • Annual review and update of IT DR Plan
User Education	
• Demonstrate an increase in awareness of Information Security issues and what staff can actively do to prevent security incidents within the SDHB.	• Creation of user training material • Raising awareness of security issues through presentations to key stakeholders. • Implementation of a user training programme • Successful Information Security surveys measured by favourable levels of staff participation. • Assist team leaders and management of how to improve cyber hygiene into IT administrators' actions and activities.
Information Security Roadmap	
• Establish and document a planned approach to continually improve information security.	• Development of the SDHB Information Security Roadmap • Planning a clear way forward to improve information security within the SDHB
Audit and Compliance	

• Ensure compliance with all Information Security Audits • Be involved in the Change Control process to pre-emptively triage and assess cyber security risk of activity.	• Achieve successful external audit compliance. • Practice after-action review on approved Change Control requests to re-assess changed systems integrity.
Security Monitoring	
• Provide detailed monitoring of information security	• Present monthly information security reporting outlining risks, issues and mitigations to the Technology and Services Manager. • Ensure all firewall and security appliance logs are captured and monitored appropriately. • Produce cyber security risk assessment reports in a timely manner with which can be used in both contexts of technical, or business risk discussions.
Other Duties	
Undertaking duties from time to time that may be in addition to those outlined above but which fall within your capabilities and experience.	• You respond positively to requests for assistance in own and other areas, demonstrating adaptability and willingness. • You produce work that complies with SDHB processes and reflects best practice. • Research undertaken is robust and well considered.
Professional Development – self	
Identifying areas for personal and professional development.	• Training and development goals are identified/agreed with your manager. • Performance objectives reviewed annual with your manager. • You actively seek feedback and accept constructive criticism.
Health, Safety and Wellbeing	
Taking all practicable steps to ensure personal safety and the safety of others while at work, in accordance with the Southern DHB's Health, Safety and Wellbeing policies, procedures and systems.	• You understand and consistently meet your obligations under Southern DHB's Health and Safety policy/procedures. • You actively encourage and challenge your peers to work in a safe manner. • Effort is made to strive for best practice in Health and Safety at all times.
Treaty of Waitangi	
Giving effect to the principles of the Treaty of Waitangi – Partnership, Participation and Protection through your interaction with others on a day to day basis.	• *Partnership* – You interact in good faith and in the nature of a partnership. There is a sense of shared enterprise and mutual benefit where each partner takes account of the needs and interests of the other. • *Participation* – You work in partnership with our treaty partners to enable our organisation to prosper. You are mindful of the varying socio-economic conditions that face our people and work hard to remove barriers of access to health and education. • *Protection* – You work proactively to protect the rights and interests of Māori, including the need to proactively build the capacity and capability of Māori.

For Job Evaluation Purposes: (As per the current Southern DHB Delegation of Authority Policy)

Number of direct reports: 0 :
Southern DHB Delegation of authority (level 1 – 5) : Level 5

Staff Authority

Authority to engage, promote, discipline and dismiss staff

No authority:

Contractual Authority

No authority to enter into agreements or contracts on behalf of the Southern DHB

Work Complexity

- Leads on the formulation and implementation of IS strategy. Applies a high level of leadership skills. Has a deep understanding of the industry and the implications of emerging technologies for the wider business environment.

Freedom To Act

- Has defined authority and accountability for actions and decisions within a significant area of work, including technical and quality aspects. Work is often self-initiated. Is fully responsible for meeting allocated technical and/or project/supervisory objectives.

Financial Responsibilities

- Controls a budget N
- Maximum that may be spent without reference to manager N/A
- Jobholder can spend unbudgeted capital N/A
- Jobholder is responsible for committing the organisation to long-term contracts N/A
- Jobholder signs correspondence for Company N/A

CHANGES TO POSITION DESCRIPTION

From time to time it may be necessary to consider changes to the position description in response to the changing nature of our work environment – including technological requirements or statutory changes. This Position Description may be reviewed as part of the preparation for your annual performance and development review.

Acknowledged / Accepted:

....
Employee Date

....
Manager Date