

# Technology Security Engineer Information Group

## About MSD

### Our purpose

Manaaki tangata, Manaaki whānau

We help New Zealanders to be safe, strong, and independent.

### Our commitment to Māori

As a Te Tiriti o Waitangi partner we are committed to supporting and enabling Māori, whānau, hapū, Iwi and communities to realise their own potential and aspirations.

### Our strategic direction

|  |  |  |
| --- | --- | --- |
| Mana manaakiA positive experience every time | KotahitangaPartnering for greater impact | Kia takatū tatouSupporting long-term social and economic development |

### Our Values

|  |  |  |  |
| --- | --- | --- | --- |
| ManaakiWe care about the wellbeing of people | WhānauWe are inclusive and build belonging | Mahi tahiWe work together, making a difference for communities | Tika me te ponoWe do the right thing, with integrity |
|  |  |  |  |

### Working in public service

Ka mahitahi mātou o te ratonga tūmatanui kia hei painga mō ngā tāngata o Aotearoa i āianei, ā, hei ngā rā ki tua hoki. He kawenga tino whaitake tā mātou hei tautoko i te Karauna i runga i āna hononga ki a ngāi Māori i raro i te Tiriti o Waitangi. Ka tautoko mātou i te kāwanatanga manapori. Ka whakakotahingia mātou e te wairua whakarato ki ō mātou hapori, ā, e arahina ana mātou e ngā mātāpono me ngā tikanga matua o te ratonga tūmatanui i roto i ā mātou mahi.

In the public service we work collectively to make a meaningful difference for New Zealanders now and in the future. We have an important role in supporting the Crown in its relationships with Māori under the Treaty of Waitangi.  We support democratic government. We are unified by a spirit of service to our communities and guided by the core principles and values of the public service in our work potential and aspirations.

### The outcomes we want to achieve

* New Zealanders get the support they require
* New Zealanders are resilient and live in inclusive and supportive communities
* New Zealanders participate positively in society and reach their potential

### We carry out a range of responsibilities and functions including

* Employment, income support and superannuation
* Community partnerships, programmes, and campaigns
* Advocacy for seniors, disabled people, and youth
* Public housing assistance and emergency housing
* Resolving claims of abuse and neglect in state care
* Student allowances and loans

### He Whakataukī\*

|  |  |
| --- | --- |
| Unuhia te rito o te harakeke | If you remove the central shoot of the flaxbush |
| Kei hea te kōmako e kō? | Where will the bellbird find rest? |
| Whakatairangitia, rere ki uta, rere ki tai; | Will it fly inland, fly out to sea, or fly aimlessly; |
| Ui mai ki ahau, | If you were to ask me, |
| He aha te mea nui o te ao? | What is the most important thing in the world? |
| Māku e kī atu, | I will tell you, |
| He tangata, he tangata, he tangata\* | It is people, it is people, it is people |

\*We would like to acknowledge Te Rūnanga Nui o Te Aupōuri Trust for their permission to use this whakataukī.

## Position Detail

### Overview of position

The Technology Security Engineer is part of the Technology Security and Identity Practice and drives effective and efficient security engineering and operation of MSD’s information technologies. They provide security operational support and project work within a multi-platform integrated environment, liaising with IST technical and delivery teams, vendors and MSD business stakeholders.

The Technology Security Engineer performs a wide variety of tasks across MSD’s technology security services. They are responsible for security aspects of engineering design, build, configure, test, maintenance and support for security services and associated technology and tools. In order to be successful in doing this, a breadth of understanding around different engineering disciplines is required to be able to plan and integrate these security engineering principles.

The Technology Security Engineer plays a vital role in shaping the design and strategic direction of new and existing security infrastructure and services. They are instrumental in developing robust security engineering practices, ensuring they adapt to the evolving needs of our dynamic security landscape at the Ministry.

The Technology Security Engineer will work with Practice Managers, Security Architects and Technology Security Specialists to ensure that security solutions are planned and engineered with appropriate controls in accordance with the security and identity architecture and design standards. They will manage and maintain configuration of security services and ensure configuration documentation is kept up to date throughout the service lifecycle.

The Technology Security Engineer will plan and collaborate with other engineers and business stakeholders to understand business requirements and propose solutions. They also support Security Analysts by providing security engineering advice when it comes to the development and maintenance of security operations technology and tools.

The Technology Security Engineer will also assist with resolving any security incidents requiring security engineering expertise.

### Location

National Office, Wellington and Auckland.

### Reports to

Practice Manager Technology Security

## Key responsibilities

### Required skills (SFIA8)

### Systems Design (DESN) Level 5

### Designs large or complex systems and undertakes impact analysis on major design options and trade-offs.

### Ensures that the system design balances functional and non-functional requirements.

### Reviews systems designs and ensures that appropriate methods, tools and techniques are applied effectively. Makes recommendations and assesses and manages associated risks.

### Adopts and adapts system design methods, tools and techniques. Contributes to development of system design policies, standards and selection of architecture components.

### System Software (SYSP) Level 5

* Ensures that system software is provisioned and configured to facilitate the achievement of service objectives.

### Evaluates new system software and recommends adoption if appropriate. Plans the provisioning and testing of new versions of system software.

### Investigates and coordinates the resolution of potential and actual service problems.

### Ensures that operational procedures and diagnostics for system software are current, accessible and well understood.

### Systems and Software Life cycle Engineering (SLEN) Level 5

* Collaborates with those responsible for ongoing systems and software life cycle management to select, adopt and adapt working practices.
* Supports deployment of the working environment for systems and software life cycle working practices.
* Provides effective feedback to encourage development of the individuals and teams responsible for systems and software life cycle working practices. Provides guidance and makes suggestions to support continual improvement and learning approach.
* Contributes to identifying new domains within the organisation where systems and software life cycle working practices can be deployed.

### Configuration Management (CFMG) Level 5

### Plans the capture and management of CIs and related information.

### Agrees scope of configuration management processes and the configuration items (CIs) and related information to be controlled.

### Identifies, evaluates and manages the adoption of appropriate tools, techniques and processes (including automation) for configuration management.

### Contributes to the development of configuration management strategies, policies, standards, and guidelines.

### Information Security (SCTY) Level 4

### Provides guidance on the application and operation of elementary physical, procedural and technical security controls.

### Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems.

### Identifies risks that arise from potential technical solution architectures. Designs alternate solutions or countermeasures and ensures they mitigate identified risks.

### Investigates suspected attacks and supports security incident management.

### Levels of responsibility

Autonomy – Level 5

* Works under broad direction.
* Work is often self-initiated.
* Is fully responsible for meeting allocated technical and/or group objectives.
* Analyses, designs, plans, executes, and evaluates work to time, cost and quality targets.
* Establishes milestones and has a significant role in the assignment of tasks and/or responsibilities.

Influence – Level 4

* Influences customers, suppliers and partners at account level.
* Makes decisions which influence the success of projects and team objectives.
* May have some responsibility for the work of others and for the allocation of resources.
* Engages with and contributes to the work of cross-functional teams to ensure that customers and user needs are being met throughout the deliverable/scope of work.
* Facilitates collaboration between stakeholders who share common objectives.
* Participates in external activities related to own specialism.

Complexity – Level 5

* Implements and executes policies aligned to strategic plans.
* Performs an extensive range and variety of complex technical and/or professional work activities.
* Undertakes work which requires the application of fundamental principles in a wide and often unpredictable range of contexts.
* Engages and coordinates with subject matter experts to resolve complex issues as they relate to customer/organisational requirements.
* Understands the relationships between own specialism and customer/organisational requirements.

Business skills – Level 4

* Communicates fluently, orally and in writing, and can present complex information to both technical and non-technical audiences when engaging with colleagues, users/ customers, suppliers and partners.
* Selects appropriately from, and assesses the impact of change to applicable standards, methods, tools, applications and processes relevant to own specialism.
* Demonstrates an awareness of risk and takes an analytical approach to work.
* Maximises the capabilities of applications for their role and evaluates and supports the use of new technologies and digital tools.
* Contributes specialist expertise to requirements definition in support of proposals.
* Shares knowledge and experience in own specialism to help others.
* Learning and professional development — maintains an awareness of developing practices and their application and takes responsibility for driving own development.
* Takes the initiative in identifying and negotiating their own and supporting team members’ appropriate development opportunities.
* Contributes to the development of others.
* Security, privacy, and ethics — fully understands the importance and application to own work and the operation of the organisation.
* Engages or works with specialists as necessary.

**Knowledge - Level 4**

* Has a thorough understanding of recognised generic industry bodies of knowledge and specialist bodies of knowledge as necessary.
* Has gained a thorough knowledge of the domain of the organisation.
* Is able to apply the knowledge effectively in unfamiliar situations and actively maintains own knowledge and shares with others.
* Rapidly absorbs and critically assesses new information and applies it effectively.

### Embedding Te Ao Māori

* Embedding Te Ao Māori (te reo Māori, tikanga, kawa, Te Tiriti o Waitangi) into the way we do things at MSD.
* Building more experience, knowledge, skills and capabilities to confidently engage with whānau, hapū and iwi.

### Health, Safety and Security

* Understand and implement your Health, Safety and Security (HSS) accountabilities as outlined in the HSS Accountability Framework.
* Ensure you understand, follow and implement all Health, Safety and Security and wellbeing policies and procedures.

### Emergency Management and Business Continuity

* Remain familiar with the relevant provisions of the Emergency Management and Business Continuity Plans that impact your business group/team.
* Participate in periodic training, reviews and tests of the established Business Continuity Plans and operating procedures.

### Know-how

* Relevant qualification or equivalent experience in a systems engineer or senior security analyst role.
* Demonstratable experience across a broad range of security services, including cloud security, data and information security, network security, endpoint security, boundary security, email security, Identity and Access Management, PKI, MDM, MAM, SSO/Federation and SIEM.
* Extensive experience in developing and implementing security policies, standards, and guidelines aligned with industry best practices and compliance requirements (e.g., NZISM, PSR, PCI-DSS, ISO27001)
* Demonstratable experience in security administration of the following cloud technologies and platforms:
	+ Amazon Web Services
	+ Microsoft Azure
	+ Microsoft 365.
* Experience in server installation, configuration, and troubleshooting.
* Experience implementing and supporting system change based on technology or policy change.
* Experience in scripting and automation.
* Deep understanding of one or more of the following: NIST, ACSC Essential Eight, CertNZ Top Ten controls.
* Good understanding of latest cyber security principles, standards, frameworks, guidelines, techniques and threats.
* Excellent communication, documentation and problem-solving skills
* Ability to follow change management procedures utilizing ITIL standards.

### Attributes

* Excellent communication and problem-solving skills.
* Commitment to continuous learning and keeping up to date with best practices and technology advances.
* Ability to articulate ideas and facilitate discussions and meetings towards achievable outcomes.
* Strong written and verbal skills with the ability to communicate issues and concepts.
* Ability to build effective working relationships with a wide range of business and technical stakeholders.
* A team player and self-starter with a strong desire to learn.
* Rigorous intellectual analytical ability.
* Inquisitive and interested in emerging technologies and practices.
* Commitment to achievement and quality.
* Critical evaluation.
* Sound judgement.
* Honesty and integrity.

### Key relationships

Internal

* Technology Security and Identity Practice (including Practice Managers, Architects, Engineers, Administrators and Analysts)
* Security and Identity Programme delivery team
* IST technical and delivery teams
* Security risk and assurance functions

External

* Vendors and partners

### Other

Delegations

* Financial – No
* Human Resources – No

Direct reports

* No

Security clearance

* No

Children’s worker

* Not a children’s worker

Travel

* Limited ad hoc travel may be required.