

# Technology Security Specialist 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 manaaki  A positive experience every time | Kotahitanga  Partnering for greater impact | Kia takatū tatou  Supporting long-term social and economic development |

### Our Values

|  |  |  |  |
| --- | --- | --- | --- |
| Manaaki  We care about the wellbeing of people | Whānau  We are inclusive and build belonging | Mahi tahi  We work together, making a difference for communities | Tika me te pono  We 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 Specialist is part of the Technology Security and Identity Practice and provides specialist and highly technical advice on matters relating to technology security to MSD’s technical and delivery teams, business stakeholders and vendors.

The role performs a wide variety of tasks across a range of specialist security areas. Specifically, the position:

* Has expert technology security knowledge and provides accurate and timely technical advice as it pertains to the security of technologies managed and used by MSD functions and staff.
* Responsible for ensuring that solutions are designed with appropriate controls in accordance with the MSD’s technology security and identity strategy, architecture, policies and standards.
* Develops, maintains and implements technology security standards, frameworks, guidance, and other guardrails to support secure by design practices and the technology security and identity strategic direction.
* Supports security risk and assurance functions by providing input into MSD’s certification and accreditation process. The role has a working understanding of risk management disciplines and is able to conduct robust assessment of technology security risks, both through the secure design of technology solutions, and in taking a risk-based approach to managing technology assets.
* Works collaboratively and constructively alongside Practice Managers, security architects, other security and technology specialists, and the wider business, that models a commitment to multi-disciplinary, cross-functional ways of working.

### Location

National Office, Wellington and Auckland.

### Reports to

Practice Manager, Technology Security

## Key responsibilities

### Required skills (SFIA8)

### Security operations (SCAD) Level 6

Delivering management, technical and administrative services to implement security controls and security management strategies.

* Develops policies, standards, processes, guidelines for ensuring the physical and electronic security of automated systems.
* Ensures that the policy and standards for security operations are fit for purpose, current and are correctly implemented.
* Reviews new business proposals and provides specialist advice on security issues and implications.

### Specialist advice (TECH) Level 5

Providing authoritative advice and direction in a specialist area.

* Provides definitive and expert advice in their specialist area.
* Actively maintains recognised expert level knowledge in one or more identifiable specialisms.
* Oversees the provision of specialist advice by others. Consolidates expertise from multiple sources, including third-party experts, to provide coherent advice to further organisational objectives.

Supports and promotes the development and sharing of specialist knowledge within the organisation.

* implemented.

### Information Security (SCTY) Level 5

Defining and operating a framework of security controls and security

management strategies.

* Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards.
* Contributes to development of information security policy, standards and guidelines.
* Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security, and recommends appropriate control improvements.
* Develops new architectures that mitigate the risks posed by new technologies and business practices.

### Information Assurance (INAS) Level 4

Protecting against and managing risks related to the use, storage and transmission of data and information systems.

* Performs technical assessments and/or accreditation of complex or higher-risk information systems.
* Identifies risk mitigation measures required in addition to the standard organisation or domain measures.
* Establishes the requirement for accreditation evidence from delivery partners and communicates accreditation requirements to stakeholders.
* Contributes to planning and organisation of information assurance and accreditation activities.
* Contributes to development of and implementation of information assurance processes.

Stakeholder relationship management (RLMT) Level 4

Influencing stakeholder attitudes, decisions, and actions for mutual benefit.

* Deals with problems and issues, managing resolutions, corrective actions, lessons learned, and the collection and dissemination of relevant information.
* Implements stakeholder engagement/communications plan. Collects and uses feedback from customers and stakeholders to help measure the effectiveness of stakeholder management.
* Helps develop and enhance customer and stakeholder relationships.

### 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 5**

* Demonstrates leadership in operational management.
* Analyses requirements and advises on scope and options for continual operational improvement.
* Assesses and evaluates risk.
* Takes all requirements into account when making proposals.
* Shares own knowledge and experience and encourages learning and growth.
* Advises on available standards, methods, tools, applications and processes relevant to group specialism(s) and can make appropriate choices from alternatives.
* Understands and evaluates the organisational impact of new technologies and digital services.
* Creatively applies innovative thinking and design practices in identifying solutions that will deliver value for the benefit of the customer/stakeholder.
* Clearly demonstrates impactful communication skills (oral, written and presentation) in both formal and informal settings, articulating complex ideas to broad audiences.
* Learning and professional development —  takes initiative to advance own skills and identify and manage development opportunities in area of responsibility.
* Security, privacy and ethics — proactively contributes to the implementation of appropriate working practices and culture.

Knowledge – Level 4

* Is fully familiar with recognised industry bodies of knowledge both generic and specific, and knowledge of the business, suppliers, partners, competitors and clients.
* Develops a wider breadth of knowledge across the industry or business.
* Applies knowledge to help to define the standards which others will apply

### 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

* Tertiary qualification in a relevant discipline and/or considerable professional experience
* Specialist knowledge in security controls 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
* Specialist knowledge in security controls for the following cloud technologies and platforms:
  + Amazon Web Services
  + Microsoft Azure
  + Microsoft 365.
* Demonstratable consulting and advisory experience in a large and complex environment.
* Experience in providing expert advice and guidance within complex environments with competing priorities.
* Experience in contributing to the development of security controls and security management strategies.
* Established experience working with current and emerging technologies.
* Knowledge of security standards such as NZISM, PSR, PCI-DSS or ISO27001.
* Good 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.

### 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.
* Rigorous intellectual analytical ability and able to think strategically.
* Strategic leadership and conceptual thinking.
* Inspires and motivates others.
* 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 teams

External

* Security professionals from other government agencies
* 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.