

# Identity and Access Management (IAM) 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 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 Identity and Access Management (IAM) Engineer is part of the Technology Security and Identity Practice and drives competent and efficient IAM engineering and operation of MSD’s information systems. They provide IAM operational support and project work within a multi-platform integrated environment, liaising with IST technical and delivery teams, vendors and MSD business stakeholders.

The IAM Engineer performs a wide variety of tasks across MSD’s security services, including core identity, digital credentials, PAM and IGA. They are responsible for IAM aspects of engineering design, build, configure, test, maintenance and support for security services and associated technology and tools.

The IAM Engineer implement and continuously optimize Identity and Access Management services in line with evolving technologies and security regulations. They are responsible for designing, implementing, and maintaining IDAM technologies to ensure audit and privacy compliance, driving automation wherever possible.

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

The IAM Engineer will collaborate with project teams to integrate the ministry’s identity stores and implement authentication mechanisms as well as other identity technologies. They also support IAM Analysts and Administrators by providing IAM engineering advice when it comes to the development and maintenance of IAM operations technology and tools.

The IAM Engineer will also assist with resolving any security incidents related to identity and access or requiring IAM engineering expertise.

### Location

National Office, Wellington and Auckland.

### Reports to

Practice Manager Technology Security

## Key responsibilities

### Required skills (SFIA8)

### Systems Design (DESN) Level 4

Designing systems to meet specified requirements and agreed systems architectures.

* Designs system components using appropriate modelling techniques following agreed architectures, design standards, patterns, and methodology.
* Identifies and evaluates alternative design options and trade-offs.
* Creates multiple design views to address the concerns of the different stakeholders and to handle functional and non-functional requirements.
* Models, simulates, or prototypes the behaviour of proposed system components to enable approval by stakeholders.
* Produces detailed design specifications to form the basis for the construction of systems.
* Reviews, verifies, and improves own designs against specifications.

### System Software (SYSP) Level 4

Installing, managing, controlling, deploying and maintaining infrastructure systems software, to meet operational needs and service levels.

* Monitors system software metrics and adjusts configurations for optimum availability and performance.
* Reviews system software updates and identifies those that merit action.
* Configures system software for required functionality and performance.
* Investigates and resolves system software problems, requesting action from supplier if required.

### Systems and Software Life cycle Engineering (SLEN) Level 4

Establishing and deploying an environment for developing, continually improving, and securely operating software and systems products and services.

* Elicits requirements for systems and software life cycle working practices and automation.
* Prepares design options for the working environment of methods, procedures, techniques, tools, and people.
* Selects systems and software life cycle working practices for software components and micro-services.
* Deploys automation to achieve well-engineered and secure outcomes.

### Configuration Management (CFMG) Level 4

* Proposes and agrees the configuration items (CIs) to be uniquely identified with naming conventions.
* Puts in place operational processes for secure configuration, classification and management of CIs, and for verifying and auditing configuration records.
* Develops, configures and maintains tools (including automation) to identify, track, log and maintain accurate, complete and current information.
* Reports on the status of configuration management. Identifies problems and issues and recommend corrective actions.

### Information Security (SCTY) Level 3

Defining and operating a framework of security controls and security

management strategies.

* Applies and maintains specific security controls as required by organisational policy and local riskassessments.
* Communicates security risks and issues to business managers and others. Performs basic riskassessments for small information systems.
* Contributes to the identification of risks that arise from potential technical solution architectures.
* Suggests alternate solutions or countermeasures to mitigate risks. Defines secure systemsconfigurations in compliance with intended architectures.
* Supports investigation of suspected attacks and security breaches.

### Digital Forensics (DGFS) Level 3

Recovering and investigating material found in digital devices.

* Supports digital forensic investigations by applying standard tools and techniques to investigate devices.
* Recovers damaged, deleted or hidden data from devices.
* Maintains integrity of records and collects information and evidence in a legally admissible way.

### Levels of responsibility

Autonomy – Level 4

* Works under general direction within a clear framework of accountability.
* Exercises substantial personal responsibility and autonomy.
* Uses substantial discretion in identifying and responding to complex issues and assignments as they relate to the deliverable/scope of work.
* Escalates when issues fall outside their framework of accountability.
* Plans, schedules, and monitors work to meet given objectives and processes to time and quality targets.

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 4

* Work includes a broad range of complex technical or professional activities, in a variety of contexts.
* Investigates, defines, and resolves complex issues.
* Applies, facilitates, and develops creative thinking concepts or finds innovative ways to approach a deliverable.

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 IAM Analyst or Administrator role.
* Demonstratable knowledge and experience with identity and access management technology, such as, Privileged Access Management (PAM), Identity Governance and Administration (IGA), etc.
* Demonstratable knowledge and experience with authentication standards and technologies.
* Demonstratable knowledge of identity and access management best practices such as Role-Based Access Control (RBAC), Principle of Least Privilege (PoLP), etc.
* A good understanding 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
* 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
* IG stakeholders

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.