Asset Manager

Position Details

Reports to: Head of Technology Operations	**Location:** Royal New Zealand Police College, Porirua
District/Service Centre: ICT	**Shift work/non shift work:** No
Group: Service Delivery	**Remuneration range:** Grade 20
PHPF Level Purpose: Individual Contributor	**Employee Type:** Employee
Direct reports: None	**Delegated financial authority:** N/A

Position Description

New Zealand Police is the lead agency responsible for reducing crime and enhancing community safety. We work in partnership with individuals, communities, businesses and other public sector agencies to achieve our vision of Safer Communities Together.

Context

Information and Communications Technology Service Centre Group

When it comes to protecting the community, service is everything. At the New Zealand Police, we're leading the world in using technology to ensure that our service to the New Zealand public is all it can and should be. By doing this we provide the right technology in the right way to support Police operations and strategies.

The ICT function within Police is delivered by the Information and Communications Technology Service Centre Group (ICT) and consists of the following teams, working together collegially to deliver on the performance expected by a modern policing operation:

- Business Enablement whose mission is to align ICT to Police strategy, resources and market capability.
- Service Operations whose mission is to ensure that ICT services work for Police operations.
- Information Management and Assurance whose mission is to balance opportunities and risks.
- Technology Development whose mission is to deliver solutions that meet Police's operational needs.

The Service Operations Group

The Service Operations Group is the centre for service delivery for Police Users and is responsible for the end to end provisioning, performance and availability of the services.

The Group's main functions are to optimise the end to end service experience for our users (internal and external) by providing management of the ICT Service Hub and District Operational Services, to centrally task and deploy the appropriately skilled service personnel to the correct prioritised job at the correct time.

In addition the Service Operations Group provides incident, release and problem management to optimise the performance and availability of services by driving a continuous improvement culture.

Purpose

The IT Asset Manager is responsible for the management of all ICT assets within New Zealand Police. He or she will have overall responsibility for establishing and maintaining the IT asset database. This database will also contain all information required by the Software Asset Management (SAM) processes.

In addition, the IT Asset Manager will have overall responsibility for the service asset and configuration management process. Their primary responsibility is to define and control the components of services and infrastructure and maintain accurate asset and configuration records.

Accountabilities

Service Delivery

- Promotes a professional customer-focused service delivery culture that is service-based and aligned with current IT industry best practices.
- Implements the service asset management policy and standards.
- Evaluates existing asset management systems and the design, implementation and management of new / improved systems for efficiency and effectiveness.
- Agrees scope of asset management processes, function, the items that are to be controlled, and the information that is to be recorded.
- Develops asset management standards, asset management plans and procedures.
- Ensures that the asset management methods and processes are properly approved and communicated to staff before being implemented.
- Agrees assets to be uniquely identified with naming conventions; ensures that staff comply with identification standards for object types, environments, processes, lifecycles, documentation, versions, formats, baselines, releases and templates.
- Proposes / agrees interfaces with change management, problem management, network management, release management and computer operations.
- Plans population of the asset DB; manages the asset DB, central libraries and tools; ensures regular housekeeping of the asset DB.
- Provides reports, including management reports to an agreed schedule.
- Act as a focal point for all asset management issues.
- Responsible for ensuring that that Senior IT management are correctly advised on asset management issues and the provision of accurate business forecasts.
- Responsible for high level NZP IT configuration management: Implements the configuration management policy and standards.
- Agrees scope of the configuration management processes, function, the items that are to be controlled, and the information that is to be recorded.
- Develops configuration management standards, configuration management plans and procedures.
- Ensures that changes to the configuration management methods and processes are properly approved and communicated.
- Manages the configuration management plan, principles and processes and their implementation.
- Agrees CIs to be uniquely identified with naming conventions.
- Ensures that staff comply with identification standards.
- Plans population of the CMS; manages CMS, central libraries, tools, common codes and data; ensures regular housekeeping of the CMS.
- Perform periodic asset discovery and audit tasks, with a particular emphasis on Licensing.
- Track all software licenses, their usage and owners.
- Assist with software license audit activities when requested.

- Ensure licenses are compliant with vendor usage specifications.

Relationships

- Works collaboratively with the Capacity, Change and Release Managers to ensure that all releases which impact upon assets and CIs are appropriately assessed for their impacts on the CMDB & Asset DBs.
- Works collaboratively with the Programme/Project Managers to ensure that all assets procured by the project are identified and inserted into the AMDB and CMDB.
- Monitors the AM CIs collaboratively with vendors to ensure they comply with agreed processes and ensures their delivery of services and quality is in line with business expectations.
- Work proactively with all the operational teams to ensure appropriate levels of IT assets from suppliers and Police ICT met business expectations.

Person Specification

Knowledge: Excellent understanding of asset, configuration, lifecycles and supplier management.

Skills: The following SFIA technical skills are required for this role:

Skill	Skill description	Level description
Asset Management (ASMG)	The management of the lifecycle for all managed assets (hardware, software, intellectual property, licences, warranties etc) including security, inventory, compliance, usage and disposal, aiming to protect and secure the corporate assets portfolio, optimise the total cost of ownership and sustainability by minimising operating costs, improving investment decisions and capitalising on potential opportunities. Knowledge and use of international standards for asset management and close integration with security, change, and configuration management are examples of enhanced asset management development.	Level 4: Controls IT assets in one or more significant areas, ensuring that administration of the acquisition, storage, distribution, movement and disposal of assets is carried out. Produces and analyses registers and histories of authorised assets (including secure master copies of software, documentation, data, licences and agreements for supply, warranty and maintenance), and verifies that all these assets are in a known state and location. Acts to highlight and resolve potential instances of unauthorised assets such as unlicensed copies of software.
Configuration management (CFMG)	The lifecycle planning, control and management of the assets of an organisation (such as documentation, software and service assets, including information relating to those assets and their relationships. This involves identification, classification and specification of all configuration items (CIs) and the interfaces to other processes and data. Required information relates to storage, access, service relationships, versions, problem reporting and change control of CIs. The application of status accounting and auditing, often in line with acknowledged external criteria such as ISO 9000 and ISO/IEC 20000, throughout all stages of the CI lifecycle, including the early stages of system development.	Level 5: Manages configuration items (CIs) and related information. Investigates and implements tools, techniques and processes for managing CIs and verifies that related information is complete, current and accurate.
Availability management (AVMT)	The definition, analysis, planning, measurement and improvement of all aspects of the availability of IT services, including the availability of power. The overall control and management of service availability to ensure	Level 4: Contributes to the availability management process and its operation and performs defined availability management tasks. Analyses service and component availability, reliability, maintainability and

	that the level of service delivered in all services is matched to or exceeds the current and future agreed needs of the business, in a cost effective manner.	serviceability. Ensures that services and components meet and continue to meet all of their agreed performance targets and service levels. Implements arrangements for disaster recovery and documents recovery procedures. Conducts testing of recovery procedures.
Relationship Management (RLMT)	The identification, analysis, management and monitoring of relationships with and between stakeholders. (Stakeholders are individuals, groups, or organisations who may affect, be affected by, or perceive themselves to be affected by decisions, activities and outcomes related to products, services or changes to products and services). The clarification of mutual needs and commitments through consultation and consideration of impacts. For example, the coordination of all promotional activities to one or more clients to achieve satisfaction for the client and an acceptable return for the supplier; assistance to the client to ensure that maximum benefit is gained from products and services supplied.	Level 4 - Implements stakeholder engagement/ communications plans, including, for example; handling of complaints; problems and issues; managing resolutions; corrective actions and lessons learned; collection and dissemination of relevant information. Uses feedback from customers and stakeholders to help measure effectiveness of stakeholder management. Helps develop and enhance customer and stakeholder relationships.

Experience:	• Previous experience in asset and configuration management within a large complex IT service environment essential. • Previous experience in a 24/7 IT service environment essential. • Previous experience in a multi supplier environment preferred. • Previous experience in relationship management both internal and third party preferred. • Previous Project Management experience preferred.
Qualification/s:	• ITIL certification preferable

Competencies *The following competencies are most critical for being successful in this role:*

Competency	Definition	Level
» Communicate	Two-way communication is an essential part of what we do as an organisation. We listen carefully and convey information in a clear, constructive, and professional manner at all times.	Supervisor
» Solve	We consider situations from different perspectives, and explore alternatives and consequences before taking action. We take responsibility for our decisions and are prepared to review and change our approach when required.	Individual Contributor
» Deliver	We are committed to delivering a high standard of service. We take personal responsibility for our performance – setting clear expectations, planning and prioritising our work, and seeking feedback from others in order to achieve our objectives.	Individual Contributor

Additional Requirements

- Pre-Employment Checks