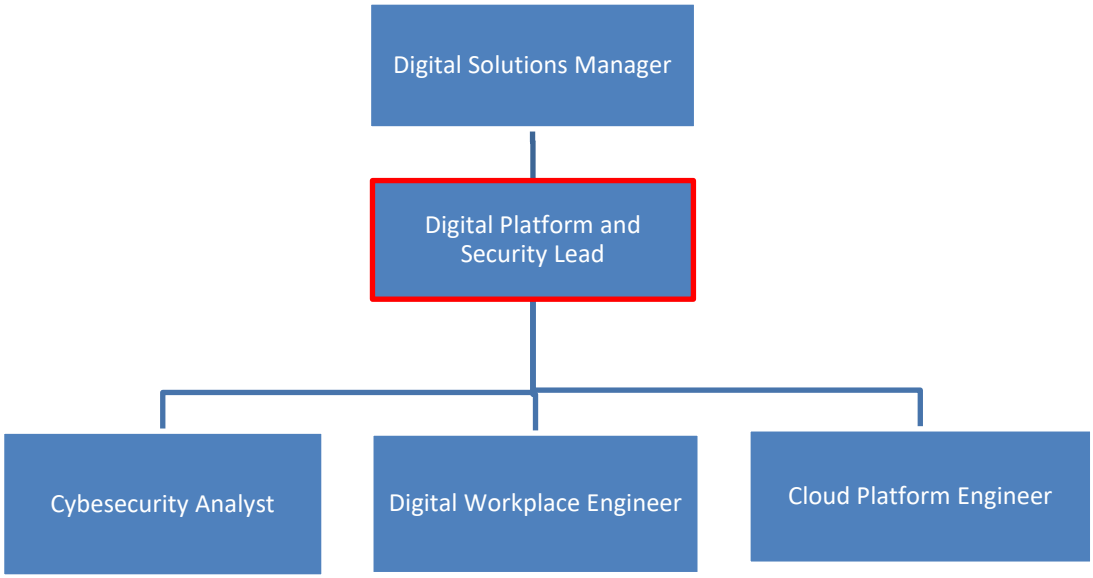
DIGITAL PLATFORM AND SECURITY LEAD
KAIĀRAHI HAUMARU & PŪNAHA MATIHIKO
POSITION DESCRIPTION

POSITION INFORMATION

Group	Organisation Performance
Team	Digital Solutions
Reports to	Digital Solutions Manager
Direct Reports	3
Primary Location	67 Horomatangi Street, Taupo and working mobile between various Council offices and around the district

TEAM STRUCTURE



POSITION PURPOSE

This is a hands-on leadership role responsible for ensuring the secure, reliable, and efficient operation of TDC's digital platforms, maintaining a safe digital environment for both staff and customers. This position is responsible for leading the organization's strategic transition towards modern cloud, SaaS, and Zero Trust technologies, while systematically reducing dependence on legacy on-premises infrastructure. You will manage day-to-day cybersecurity risk, compliance requirements, and incident response activities, ensuring consistent application of security controls that enable safe access to systems, data, and services. In this capacity, you play a critical role in safeguarding information, upholding trust, and minimising disruption from security incidents.

As a leader, you and your team will collaborate closely with internal support teams, managing operational relationships and defining well-structured escalation protocols to facilitate the prompt resolution of complex

platform and security challenges. The role also ensures digital platforms and security measures align with business continuity and disaster recovery objectives, supporting TDCs in sustaining essential services during outages or adverse events.

Key Responsibilities:

- **Primary SME:** Technical roadmap execution, operational risk management, and vendor ecosystem
- **Cross-Domain Backup:** Acts as Level 4 escalation point across all domains.

Responsibility	Key Functions/outcome
IT Operations and improvements	**Technology Road-mapping & Execution:** Translate the overarching Digital strategy into an actionable, multi-year technical roadmap, driving the phased transition toward a modern cloud environment. **Disaster Recovery & Resilience:** Design and maintain technical disaster recovery plans and system resilience, ensuring they fully support the council's broader business continuity objectives. • Provides technical leadership to optimise the performance of the technology infrastructure. • Drives the adoption of tools, AI and process automation for effective operational management and delivery. • Oversees the planning, installation, maintenance and acceptance of new and updated infrastructure components, network and infrastructure-based services. • Aligns to service expectations, security requirements and other quality standards. • Ensures operational procedures and documentation are current and effective, tracks and addresses operational issues and reports to stakeholders. Engages and influences stakeholders to ensure services are developed and managed to meet agreed service levels, security requirements and quality standards.
Technical Security & Risk Operations	Implement and manage cybersecurity controls, operational compliance, and incident response strategies, actively surfacing key technical risks to leadership. • Develops comprehensive policies, standards, processes and guidelines for organisational security across the entire digital landscape. • Ensures the ongoing relevance and effective implementation of security policies and standards, adapting to emerging technologies and threats. • Reviews and advises on security aspects of new business initiatives considering implications in the evolving digital landscape. • Leads strategic planning for security operations, integrating advanced threat intelligence and automation to enhance organisational resilience.
Information Security	• Develops and communicates corporate information security policy, standards and guidelines. • Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy, standards and guidelines. • Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors

Responsibility	Key Functions/outcome
	environmental and market trends and proactively assesses impact on business strategies, benefits and risks. • Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts.
Supplier Management	Vendor & Support Management: Oversee the operational performance of Tier 1/2 support escalations and external technical vendors, defining clear L3 escalation pathways and ensuring consistent service delivery. • Manages suppliers to meet key performance indicators and agreed targets. • Manages the operational relationships between suppliers and ensures potential disputes or conflicts are raised and resolved. • Performs bench-marking and makes use of supplier performance data to ensure performance is adequately monitored and regularly reviewed. Use suppliers' expertise to support and inform development roadmaps. • Manages implementation of supplier service improvement actions. Identifies constraints and opportunities when negotiating or renegotiating contracts. • Ongoing Financial management (FinOps) to maximise business value from cloud computing outcomes.
Leadership	• Provides leadership at an operational level. • Implements and executes policies aligned to strategic plans. • Assesses and evaluates risk. • Provides operational direction, support and guidance to assigned colleagues. • Allocates routine tasks or project work, in line with team objectives and individual capabilities. • Monitors quality and performance against agreed criteria to make learning recommendations or to escalate concerns. • Coaches colleagues in developing target skills and capabilities in line with team and personal goals. • Facilitates effective working relationships between team members.
Collaboration, Communication and Leadership	• Ensures collaborative ways of working throughout all stages of work to meet user/customer needs. • Builds effective relationships across the organisation and with customers, suppliers and partners. • Brings a continuous improvement mindset, consistently seeking ways to improve systems, processes, and outcomes through automation/Ai, thoughtful, incremental change. • Foster a high-performance team culture through strategic leadership, mentoring and continuous improvement growth mindset, empowering the team to reach their full potential and deliver exceptional value.
Health & Safety and Wellbeing	• Model a culture of safety and wellbeing for your staff (if in a Supervisor/Manager position) • Take responsibility for your own health and safety. • Ensure your own actions keep self and others safe. • Identify, report and assist to eliminate hazards/risks in workplace. • Participate in local workplace safety management practices. • Participate in workplace wellbeing initiatives.

Responsibility	Key Functions/outcome
	• Ensure compliance under Health and Safety at Work Act 2015.
Emergency Management	• Participate in civil defence emergency management (CDEM) events and training.
Change Management	• Develops and implements effective solutions within their area of responsibility, while contributing to organisational change and transition including collaboration with external partners to enable wider local government reform.

Note: This is a broad outline of the responsibilities for this position and not an exhaustive list of your responsibilities. Key responsibilities may vary from time to time as directed by your supervisor/manager to accommodate the operational needs of the team and organisation.

FUNCTIONAL RELATIONSHIPS

Internal	External
• Digital Solutions team • Business Excellence Team • Digital Programme Governance Group • Enterprise Architecture and Change Control Review Boards • Project owners/teams/stakeholders • Exec /Enterprise Leadership Team • All Staff	• Third party suppliers and consultants • District ratepayers and residents • Consultants/Professional Advisors • Other Local Authorities and Government Agencies

ORGANISATIONAL BEHAVIOURS

Six key behaviours summarise how we will operate and support our values:

- Share and seek information with open, effective and intentional communication
- Support one another with honesty, respect and integrity in all interactions
- Exceed expectations of the community and beyond
- Seek improvement in all that we do
- Harmonise life and work
- Build a stronger relationship with the whenua and the people

PERSON SPECIFICATION

Education and Qualifications

Essential	Desirable
• Tertiary qualification in information technology or related discipline.	• CISSP (Certified Information Systems Security Professional) or CISM (Certified Information Security Manager), • ITIL4 Managing Professional,

Essential	Desirable
• 7+ years' experience in cybersecurity or IT operations, with demonstrated team leadership or supervisory experience	• Checkpoint Certified Security Expert (CCSE) • Azure/AWS Solutions Architect Associate/ Expert • FinOps • DevOps

Personal Attributes

Essential	Desirable
• Commitment to delivering high-quality solutions to organisational needs • Demonstrating integrity and honesty • Taking ownership and responsibility for your decisions, work, and actions • Accepts full responsibility for self and contribution as a team member; displays a strong commitment to organisational success. • Demonstrates an open-minded approach to understanding people regardless of their background; treats all people fairly and consistently; effectively works with people from diverse backgrounds by treating them with dignity and respect. • Able to clearly & confidently present and communicate information • Establishes good relationships with customers and staff; builds wide and effective networks of contacts inside and outside the organisation. • Able to make prompt, clear decisions which may involve tough choices or considered risks • Works productively in a pressurised environment • Effectively balances the demands of a work life and a personal life • Strategic thinker with ability to influence at executive and governance levels." • Proven leadership in managing change and capability uplift.	• Working within and role modelling the organisation values • Driving for team success over personal success • Highly professional in conduct and acting as a positive role model for others. • Continuous improvement mindset and implementing/maintaining best practice frameworks. • Able to gain agreement and commitment from others by persuading, convincing and negotiating. • Works strategically to realise organisational goals • Receptive to feedback • Understands the workings, structure, and culture of Council as well as the political, social, economic, and service delivery issues affecting a local government organisation. • Commitment to making a difference to community life and services in the Taupō region

Knowledge and Experience

Essential	Desirable
• Strong understanding of security frameworks, compliance standards (particularly ISO 27001), and IT operations best practices • Experience with cloud infrastructure, security tools, and IT service management processes	• Previous experience in a public sector - Council, government or regulated environments. SFIA 9 skills equivalent of: • Technology Service Management – Level 6 • Information Security – level 6

Essential	Desirable
• Proven experience in managing operational teams, coordinating projects, and delivering services in a fast-paced environment • Familiarity with incident management, change control, and vulnerability management processes • Experience working with agile and DevOps practices • Strong leadership and team management capabilities with the ability to guide, motivate, and support team members • Excellent communication skills with the ability to facilitate clear information flow between team members and stakeholders • Proven problem-solving abilities and conflict resolution skills to address team challenges effectively • Organisational and planning skills to manage multiple priorities and coordinate complex workflows • Outcomes-focused mindset with agility to cope with changing priorities in a scale-up technology environment	• Security Operations (SCAD) Level 6 • Supplier Management – Level 5 • Change control – level 5 • Collaboration – level 5 Communication – Level 5

JOB DESCRIPTION SIGN-OFF

Please note that this Job Description will be discussed annually to ensure currency of the position responsibilities.

	Manager	Employee
Name		
Signature		
Date		