

ENVIRONMENT SOUTHLAND

Senior ICT Systems and Security Engineer

Role description

About us

Our mission

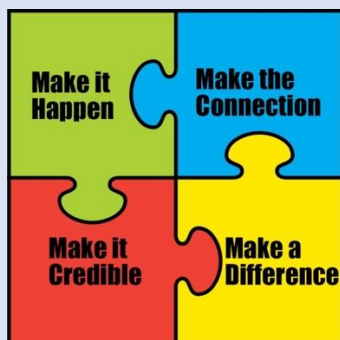
Working with the community to enhance Southland's environment.

Our vision:

A thriving Southland (Te taurikura o Murihiku)

Our values:

Here at ES, we -



Role purpose

The purpose of the **Senior ICT Systems and Security Engineer** role is to help ensure the security and integrity of Council's Information and Communication Technology (ICT) systems by protecting sensitive information and promoting a secure computing environment for all users.

The role includes providing input and assisting with planning for future server, computer and network upgrades and security, and leading Council's cybersecurity activities.

This position may require some work to be completed outside of Environment Southland's normal hours of work of 8:00 am to 5:00 pm Monday to Friday.

About your role

Grade: 18

Pathway: T5

Group/Division: Corporate Services / ICT Operations Team

Reports to: Team Leader ICT Operations

Who you will be working with

Direct reports:

- Nil

Indirect reports:

- Nil

Key relationships

External:

- Server / Computer hardware vendors
- Telecommunication providers
- IT Service companies
- Training providers
- IT contractors
- Emergency Management Southland

Internal:

- Information & Technology Services team
- Business system owners
- Project support
- Other staff at Environment Southland

Delegations

In line with the Environment Southland Delegations Manual

Your leadership profile – Individual Contributor

Your crucial challenge as an Individual Contributor is to find a way to add value while working effectively with others.

*To be an effective **Individual contributor**, aim to:*

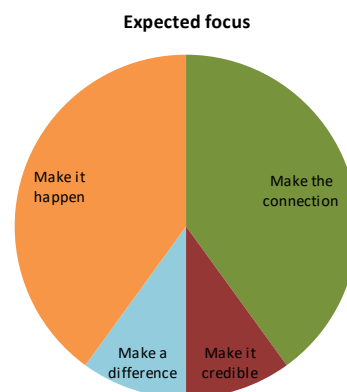
Make it Happen – Show initiative, take accountability and deliver high-quality work on time.

Make the Connection – Focus on meeting your customers' needs and work collaboratively as part of your team.

Make it Credible – Communicate clearly, show integrity, and focus on building your professional skills.

Make a Difference – Show curiosity, make thoughtful and evidence-based decisions, and aim to understand the wider context for your work.

While all elements of the Environment Southland Leadership Competency Framework are important, as an **Individual Contributor**, you will have a stronger focus on Make it Happen and Make the Connection.



Your accountabilities

Infrastructure and System Support	<ul style="list-style-type: none"> • Assist with the overall communications and infrastructure, including network switches and firewalls, and maintain it appropriately to support business continuity, including a strong focus on cybersecurity. • Work with the team leader and manager to develop the ICT strategic direction and roadmap and support the implementation of those strategies and roadmaps. • Work with the team leader in leading the design and maintain of IT infrastructure and continuously ensure it meets the needs of the wider organisation in conjunction with the IT team. • Work with the team leader to establish and enforce standardised configurations for hardware and software. • Assist with the development of the roadmap for hardware and software upgrades based on anticipated demand. • Assist with the planning of larger organisational and team projects, identifying appropriate technology/software/methodologies to address the issue and, ensuring the product meets the needs requested or root cause problem has been resolved. • Assist with evaluating emerging technologies to determine their potential impact on the Council's computing requirements. • Assist with the development, implementation, and enforcement of security policies and procedures to safeguard Council's assets. • Work with the team leader and engineers to implement monitoring tools to track application performance and identify bottlenecks.
IT Security	<ul style="list-style-type: none"> • Responsible for ensuring compliance with industry regulations and standards (e.g., GDPR, ISO 27001). etc • Work with the team leader to develop security standards to protect against potential threats. • Ensure compatibility and interoperability among different components of the computing environment. • Responsible for regularly reviewing and updating standards to align with industry best practices. • Lead employee education on security best practices and policy compliance. • Ensure process documentation is available, followed and improved.
Security Architecture and Access controls	<ul style="list-style-type: none"> • Implement and manage access controls to ensure that only authorised people have appropriate access to systems and data. • Responsible for regularly reviewing and updating user access privileges based on job roles and responsibilities. • Utilise and implement multi-factor authentication or appropriate tools to enhance access security. • Implement security measures, including firewalls, intrusion detection/prevention systems, and regular security audits. • Stay informed about the latest security threats and vulnerabilities. • Ensure that all systems and applications adhere to security best practices. • Design and implement a robust security architecture that includes firewalls, intrusion detection/prevention systems, and secure network configurations. • Collaborate with team leader and leading system architects to integrate security measures into the overall IT infrastructure. • Keep any sensitive information confidential.

Security Patching and Updates	<ul style="list-style-type: none"> • Responsible for maintaining, and improving the current patch management process to keep systems and software up to date to address vulnerabilities • Test patches in a controlled environment before deploying to production systems. • Assist with the establishing and security requirements in vendor contracts. • Conduct quarterly periodic security assessments of vendor systems.
Security Awareness Training	<ul style="list-style-type: none"> • Provide ongoing security awareness training for employees to ensure a security-conscious culture. • Conduct phishing simulations to test and improve employee resilience to social engineering attacks. • Promote a culture of reporting security incidents and concerns.
Incident Response and Backups	<ul style="list-style-type: none"> • Assist with the development and maintenance of an incident response plan to address security incidents promptly. • Assist with conducting regular drills and simulations to test the effectiveness of the disaster recovery plan and backups. • Investigate security incidents, analyse root causes, and implement corrective actions.
Project Management	<ul style="list-style-type: none"> • Participate in projects which may be financial, transformational, strategic and/or leadership focused from time to time • Application in line with Council's corporate project management systems and processes. • Ensure that project timelines and deliverables are met. • Assist with providing monthly and quarterly updates for the Manager
Finance (budgets)	<ul style="list-style-type: none"> • Consider the financial implications of actions.
Continuous improvement	<ul style="list-style-type: none"> • Continually seek opportunities to improve services for your customers (internal or external). • Show flexibility, adaptability and a willingness to change and are open to feedback as an opportunity to improve.
Stakeholder Relationships/Customer Service	<ul style="list-style-type: none"> • Develop strong and effective relationships with internal and external stakeholders. • Respond appropriately. • Understand situations from the customer's perspective. • Keep customers up to date about the progress of queries/requests/projects. • Maintain clear communication.
Other duties	<ul style="list-style-type: none"> • Any other duties that may be required from time to time.

Your health, safety and well-being

- Work safely and take responsibility for keeping self, colleagues, contractors and customers free from harm;
- Report all incidents, near-misses, hazards and accidents promptly
- Communicate whereabouts when out of the office (e.g. use Where Am I, Get Home Safe)
- Activity risk assessments are completed as part of planning for all field-based activities prior to work being undertaken, with relevant parties
- Know what to do in the event of an emergency
- Participate in safety and wellbeing initiative and programmes as required
- Attend required health and safety training and induction sessions.

Working with Māori

Working at Environment Southland requires all of our staff to uphold the council's Te Tiriti o Waitangi responsibilities as part of their day-to-day role. This might be through the appropriate delivery of functions through various legislation where Te Tiriti o Waitangi or partnering with mana whenua is required or upholding the commitments that our elected councillors have made to Ngāi Tahu ki Murihiku through the Charter of Understanding. Many of our established workstreams and programmes are delivered in partnership with the four papatipu rūnanga of Ngāi Tahu which hold mana whenua in Murihiku Southland.

This will regularly require:

- Understanding and delivery on Te Tiriti o Waitangi obligations for Environment Southland that are identified for your role
- Ensuring partnership and engagement practices are planned for, and suitable to the relationship with Ngāi Tahu ki Murihiku
- Undertaking regular learning and development for the role to support competency in delivering on Te Tiriti o Waitangi responsibilities, as directed

Your civil defence and emergency response responsibilities

All staff of Environment Southland may be required to undertake Civil Defence or Biosecurity duties in the event of an emergency. Training will be given as appropriate.

- Fulfil allocated Civil Defence and emergency response roles, as assigned.
- Manage or assist with other emergency responses that are required.
- Participate in Civil Defence and emergency response initiatives and programmes as required

Confidentiality, privacy and recordkeeping

All staff of Environment Southland are required to collect, retain, and maintain sensitive, confidential and personal information. Training will be given as appropriate to:

- Manage all information with care and respect in accordance with the Public Records Act 2005, Privacy Act 2020, Local Government Official Information and Meetings Act 1987 and all other relevant Local Government legislation.
- Retain information, regardless of format, e.g. records and data in official organisational systems.
- Ensure no sensitive, confidential, or personal information is inappropriately shared internally or externally without the appropriate approval.
- Report a privacy breach to the organisational Privacy Officer if a situation should occur.

Your experience, knowledge and qualifications

Knowledge/Experience

- Demonstrated knowledge to fulfil requirements of the key accountabilities specified for this position.
- Bachelor's degree in computer science or other relevant topic
- At least 5 years of senior IT engineer experience and/or 3 years in an IT senior security role.
- Proven experience in:
 - Microsoft products eg Azure, 365 etc

- Cyber security
- Firewall applications
- VMware
- Backup products, primarily Datto and Veeam
- Network documentation and diagrams
- Some experience with Manage Engine products will help but not required
- SQL skills would be advantageous
- Ability to see the big picture and quickly understand where and how to contribute
- Excellent relationship-building skills at all levels of the organisation that enable you to collaborate, gain buy-in and influence thinking

Attributes

- A can-do attitude, with excellent customer service skills, always striving for the right solution.
- Work effectively as part of a team, including the ability to show leadership in areas of expertise (including passing on these skills as appropriate).
- Committed to understanding and delivering on Te Tiriti o Waitangi matters on behalf of Environment Southland, specific to Murihiku context.
- Interest to develop further capability, in te reo me ona tikanga Māori
- Self-motivated, prepared to use initiative
- Honesty, integrity and commitment to preserving confidentiality.
- Able to prioritise work and manage time.
- Work for the benefit of the organisation and promotes organisational ideals and purpose.
- Ability to coach and mentor, combined with the ability to build strong networks with key stakeholders
- Root cause analysis skills to aid problem solving

Performance Review

We have a Professional Development Programme (PDP) that is the basis for performance assessment at all levels of the organisation. There is at least one formal meeting, annually, between the team member and their people leader, along with a six-month review and regular monthly catch-ups.

Acknowledgement

I _____ have received a copy of the job description and have read and understand the duties and responsibilities and key relationships described therein.

Signature _____

Date _____