

JOB DESCRIPTION

Position Title: Principal IT Officer

Division: Office of the General Manager	Location: Main Office, Matautu-tai
Report to: General Manager	Contract: 3 Years
Hours of Work: Monday to Friday, 9am – 5pm	Salary: \$55,431 - \$64,501 [L16]
Responsible for: Senior IT Officer	

Primary Objectives

The Principal IT Officer is responsible for leading and managing the Corporation's information technology infrastructure, cybersecurity, business systems, networks and digital services. The role ensures the reliability, security, availability and continuous improvement of all ICT resources and provides strategic advice to management on technology investments, risk management and digital transformation initiatives. The position oversees the planning, implementation, maintenance and support of ICT systems, ensuring that technology services effectively support the Corporation's operational and strategic objectives.

Part A: Key Responsibilities, Activities, Tasks & Key Performance Indicators (KPIs)

Key Areas of Responsibility	Key Activities and Tasks	Key Performance Indicators (KPIs)
ICT Strategy, Governance, Planning, Network & Systems Administration	- Develop and implement ICT policies, procedures, standards and best practices - Prepare ICT Strategic Plan, Digital Transformation Roadmap and annual ICT work plan aligned with organizational objectives - Provide strategic advice to Management on ICT investments, enterprise infrastructure and digital initiatives - Support ICT governance through compliance with organizational policies, standards and legislative requirements - Maintain and monitor the ICT Risk Register and report ICT risks and mitigation measures to Management - Prepare ICT reports, recommendations and performance updates for AGM/Management - Assist with ICT operational and capital budget planning, expenditure monitoring and procurement prioritization	- ICT Strategic Plan and annual work plan reviewed and updated annually 100% compliance with approved ICT policies and procedures - ICT Risk Register reviewed and updated quarterly with mitigation actions reported to Management - Annual ICT operational and capital budget prepared and submitted within approved timeframe - ICT expenditure monitored and reported quarterly within approved budget allocations - Network uptime maintained at ≥ 99% - Critical system outages resolved within 4 hours

	• Manage enterprise servers, network infrastructure, internet connectivity and communication systems • Administer • Administer firewalls, routers, switches, wireless networks and cloud services • Monitor system performance, network availability and enterprise systems interoperability • Manage user accounts, permissions and access controls • Ensure optimal performance, scalability and continuity of all ICT infrastructure across the Corporation	• User account request processed within 2 working days • Quarterly infrastructure performance assessment completed
Cybersecurity, Information Security, Backup, Disaster Recovery & Data Management	• Manage cybersecurity systems including firewalls, antivirus, endpoint protection and intrusion prevention systems • Monitor cybersecurity threats, vulnerabilities and security events • Conduct cybersecurity audits, risk assessment and vulnerability reviews • Ensure data protection, business continuity and disaster recovery measures are implemented and maintained • Coordinate ICT incident response, recovery and restoration activities during system failures or cybersecurity events • Manage enterprise system backups and disaster recovery processes • Maintain data integrity, availability and confidentiality • Monitor storage capacity and data retention requirements • Conduct regular backup and recovery testing and document outcomes	• No major cybersecurity breaches attributable to internal control failures or system weaknesses • Quarterly cybersecurity audit completed and corrective actions implemented • Backup recovery testing successfully completed at least twice annually • System backup success rate maintained at $\geq 99\%$, with documented exceptions and corrective actions • No preventable loss of critical business data due to system or process failure • Data recovery requests completed within agreed service levels
ICT Operations & Technical Support, Software & Website Administration, Asset Management & Procurement	• Provide technical support and troubleshooting services • Manage ICT service requests and incident management processes in accordance with agreed service levels • Install, configure, upgrade and maintain ICT hardware, software and operating systems • Maintain ICT operational support documentation • Ensure workstations and thin clients are operating effectively • Maintain and support software applications and systems • Manage software licensing and compliance	• 95% of ICT service requests resolved within agreed service levels • Average response time to ICT incidents less than 4 business hours • User satisfaction rating of at least 85% • ICT asset downtime maintained below 2% annually • 100% compliance with software licensing requirements

	• Coordinate software upgrades and system implementations • Maintain and update the Corporation's website • Ensure ICT systems remain secure, available and current • Maintain ICT asset registers and inventories • Recommend ICT equipment acquisitions, lifecycle replacements and technology upgrades • Monitor hardware and software lifecycle requirements • Monitor vendor performance against Service Level Agreements (SLAs) • Provide technical input into ICT procurement evaluations, contract renewals and vendor selection processes	• Website uptime maintained at $\geq 99\%$ • All critical software upgrades completed within approved timeframes • Annual software inventory completed and verified • ICT asset register maintained with 100% accuracy • Annual ICT asset verification completed • No expired software licenses • Vendor performance reviewed annually against agreed SLAs
Leadership & Staff Development	• Supervise ICT personnel • Allocate work, monitor performance and ensure service delivery standards are achieved • Coach and mentor ICT staff • Promote continuous improvement, innovation and knowledge sharing • Coordinate ICT operational continuity during critical incidents or executive delegated periods of responsibility, where applicable	• Staff performance reviews completed annually • Team objectives achieved at a minimum rate of 90% • Individual development plans implemented for ICT staff • ICT operational continuity maintained during critical incidents and delegated responsibilities

Part B: Merits and Selection Criteria

Skills and Abilities	✓ Strong knowledge of network administration, server management and systems infrastructure ✓ Experience with Sophos Firewall, cybersecurity monitoring and threat management ✓ Knowledge of Microsoft Windows Server environments, active directory, cloud technologies and virtualization ✓ Experience managing backups, disaster recovery and business continuity systems ✓ Proficiency in website administration and software support ✓ Knowledge of governance, risk management and information security frameworks ✓ Ability to analyze technical issues and implement effective solutions ✓ Strong project planning and organizational skills ✓ Ability to establish priorities and manage competing demands ✓ Ability to prepare technical reports and recommendations for management ✓ Strong vendor and contract management capabilities ✓ Experience developing ICT policies and procedures ✓ Excellent written and verbal communication skills in both English and Samoa ✓ Ability to explain complex technical information and non-technical audiences ✓ Strong stakeholder engagement and customer service skills
Personal Attributes	✓ High level of integrity and professionalism ✓ Strong leadership and decision-making capability ✓ Excellent analytical and problem-solving skills ✓ Results oriented with strong attention to detail ✓ Ability to work under pressure and meet deadlines ✓ Proactive and innovative approach to service improvement

	✓ Strong commitment to teamwork and organizational objectives ✓ Commitment to continuous learning and professional development
Work Performance and Experience	✓ Minimum of 5 years progressively responsible experience in Information Technology ✓ At least 3 years' experience in a supervisory, management or team leadership role ✓ Demonstrated experience managing enterprise networks, cybersecurity systems and ICT infrastructure ✓ Proven experience providing strategic ICT advice and preparing management reports ✓ Experience within a public sector, maritime or corporate environment (<i>desirable</i>) ✓ Experience managing ICT projects and digital transformation initiatives (<i>desirable</i>)
Qualifications	✓ Bachelor Degree in Computer Science, Information Technology, Information Systems, Cybersecurity, Software Engineering, or a related discipline from a recognized tertiary institution ✓ Industry certifications such as CISCO, Sophos, Cybersecurity, or equivalent (<i>desirable</i>)

Continued Professional Development

The Samoa Shipping Corporation is committed to provide CPD for the successful candidate. SSC expect the successful candidate to undertake available training courses and research to enhance personal knowledge, skills and experience.

