Position Details

Position title:	**ICT Security and Operations Manager**
Award Classification:	Senior Officer
Department:	Digital and Technology Services
Division:	People and Experience
Date Approved:	April 2026
Approved By:	Chief Executive Officer
Employees:	14 FTE
Operating Budget:	ICT Security & Operations ($6M)
Capital Budget:	As approved through endorsed capital program
Financial Delegation:	As per financial delegation framework

Organisational Relationships:

Reports To:	**Chief Information and Innovation Officer**
Supervises:	ICT Security Operations Lead; Team Lead Cloud Services; Team Leader ITSM and Cloud Projects, Solution Designer
Key Internal Stakeholders:	Leadership network; Procurement & Contract Management Steering Committee; Crisis Management Team; Council; Audit and Risk Committee.
Key External Stakeholders:	Major contractors; regulatory bodies/ statutory authorities; government agencies; and customers; emergency services

POSITION SUMMARY

Position Objectives

Provide organisation-wide leadership in protecting the City of Port Phillip's digital assets while ensuring the secure, resilient, and reliable operation of the City's technology environment.

The role leads cyber security and technology operations as the organisation's senior authority (CISO-equivalent), with accountability for platforms, services, and operational capabilities that underpin organisational resilience, service continuity, and digital trust.

This includes:

- Leadership of cyber security strategy and operations aligned to NIST CSF, Essential Eight, and ISO 27001
- Executive oversight of cloud, infrastructure, endpoint, and IT service management functions

- Leadership of the organisation's ICT Strategy, Enterprise Architecture Plan, ICT asset lifecycle management, IT Operations Management and IT Service Management, ensuring technology investment, platforms, services and controls are secure-by-design, strategically aligned, cost-effective, resilient and governed across their full lifecycle.
- Enterprise governance and policy leadership across ICT, cyber security, and emerging domains including AI
- Risk-based integration of security, operations, and governance aligned to legislative obligations and organisational strategy
- Driving a culture of performance, security, and continuous improvement

Contribute to broader organisational leadership as an active member of the leadership network, role modelling organisational values, and supporting organisational strategy and improvement.

Key Responsibilities and Duties

1. **People & Culture Leadership:** Cultivate a high performing, engaged, and resilient workforce. Ensure clarity in roles, responsibilities, and performance expectations; build team capability; and manage capacity to meet service demands efficiently. Foster a safety-first, inclusive, and accountable culture. As a member of the Leadership Network, contribute to broader organisational leadership and champion a positive, values-driven workplace culture.
2. **Technology Operations, ITOM and ITSM Service Assurance:** Provide strategic leadership for secure and resilient technology operations across cyber security, cloud, infrastructure, endpoints, service management and operational platforms. Oversee IT Operations Management and IT Service Management practices including incident, problem, change, request, asset, configuration, availability, continuity and service performance management. Ensure technology services are reliable, measurable, customer-focused, continuously improved and aligned with agreed service levels, organisational priorities and risk appetite.
3. **IT Strategy, Enterprise Architecture, Security by Design, Governance and Policy:** Lead the development, maintenance and implementation of Council's ICT Strategy, Enterprise Architecture Plan, architecture principles, technology standards and digital governance frameworks. Ensure technology investments, solution designs, cloud services, SaaS platforms, infrastructure, applications and emerging technologies are assessed and governed through enterprise architecture, cyber security, privacy, data, AI, procurement and risk lenses. Embed security-by-design and privacy-by-design into technology planning, procurement, design, delivery, transition and operational support.
4. **ICT Asset and Technology Lifecycle Management:** Own the governance of Council's ICT asset lifecycle, including technology asset standards, lifecycle planning, refresh planning, risk-based prioritisation, obsolescence management, licensing oversight, platform rationalisation and alignment with financial planning. Ensure ICT assets, platforms and services are recorded, assessed, maintained, secured and retired in accordance with enterprise architecture principles, cyber security requirements, vendor obligations and budget settings.
5. **Commercial, Vendor and Financial Stewardship:** Manage strategic vendor relationships, contracts, and service providers. Oversee operational and security budgets, ensuring alignment with strategic priorities, cost optimisation, and measurable business value.

6. **Stakeholder Partnership and Influence:** Provide authoritative advice to the CIIO, Executive Leadership Team, and Council on cyber security posture, technology risk, and operational priorities. Build strong partnerships with business leaders to ensure technology outcomes support organisational objectives.

Leadership and Management Expectations

1. **People Leadership:** Lead and inspire a large, multidisciplinary workforce, fostering a safety-first, high-performance culture. Empower staff at all levels through clear direction, professional development, and by promoting accountability and initiative. Champion diversity, inclusion, and teamwork, ensuring staff are motivated and engaged in delivering excellent public service.
2. **Strategic Vision:** Set and communicate a clear vision that aligns (secure and resilient technology operations) with Council's strategic goals. Anticipate future trends and challenges (e.g. technology, *growth, climate change, policy reforms*) and develop innovative, sustainable solutions to keep services resilient and effective.
3. **Collaboration & Influence:** Work collaboratively with other Council departments and the Executive Leadership Team to integrate services and achieve shared objectives. Build trust and effective relationships with the Mayor and Councillors by providing expert advice, timely information, and transparent reporting on (Cyber security, ICT operations) matters. Engage with external partners to share best practices, influence policy, and pursue joint initiatives.
4. **Results & Accountability:** Drive a strong performance culture focused on outcomes and continuous improvement. Set clear KPIs for service quality, financial performance, safety, and sustainability, and rigorously manage to these targets. Use data and evidence to guide decision-making and resource allocation. Hold yourself and your teams accountable for meeting commitments and uphold the highest standards of integrity and compliance.

Key Selection Criteria

1. **Strategic Digital, Cyber Security and Technology Operations Leadership:** Proven senior leadership across cyber security, ICT strategy, enterprise architecture, IT operations and service management, with the ability to set strategic direction, prioritise investment, mature operational capability and deliver enterprise-wide outcomes.
2. **People Leadership & Culture**: Demonstrated experience managing large,multidisciplinary teams with a focus on safety, performance, and staff development.
3. **Financial, Contract, Vendor and ICT Asset Management:** Strong capability managing substantial budgets, ICT asset lifecycle planning, complex procurements, vendor relationships, service contracts, licensing obligations and technology renewals to ensure value for money, security, resilience, compliance and long-term sustainability.
4. **Cyber Security & Resilience Uplift:** Demonstrated experience establishing, maturing, and operationalising security frameworks and controls aligned to NIST CSF, Essential Eight, and ISO 27001, including incident response, vulnerability management, security operations, business continuity and recovery planning.

5. **ICT Strategy, Enterprise Architecture, Security by Design and Governance:** Demonstrated capability leading ICT strategy development, Enterprise Architecture Plan implementation, architecture governance, secure-by-design practices, ICT governance forums, technology standards and organisational policies across ICT, cyber security, data, privacy and AI.
6. **ITOM, ITSM and ICT Asset Lifecycle Management:** Demonstrated record delivering secure, reliable and scalable technology services through mature IT Operations Management, IT Service Management, asset lifecycle planning, service performance management, automation uplift and continuous improvement.
7. **Stakeholder Engagement & Communication:** Proven communication skills and political acumen to engage effectively with Councillors, Executive Leadership Team, stakeholders, community, contractors and regulatory bodies, and to explain complex technology, security and architecture matters in practical business terms.
8. **Qualifications & Sector Experience:** Relevant tertiary qualifications and senior leadership experience in local government or a comparable operational environment. Relevant cyber security, enterprise architecture, IT service management or cloud certifications are desirable.

ADDITIONAL DETAILS

Accountability and Extent of Authority

1. **People and Culture Leadership:** Cultivate an aligned, engaged, and high-performing workforce and a safe and inclusive workplace.
2. **Accountable for the security posture**, operational resilience, and performance of the City's ICT environment
3. Authority to make **operational and strategic decisions within approved budgets**, delegations, and CIIO direction
4. **Compliance & Risk Management:** Ensure compliance with all relevant laws and regulations. Proactively manage risks, implementing controls and contingency plans.
5. **Financial Stewardship:** Manage departmental budgets and contracts responsibly, delivering within budget and identifying efficiency improvements. Demonstrate strong financial governance, value-for-money in procurement, and effective contract oversight.
6. **Service Continuity & Resilience:** Ensure continuity of critical services under all conditions. In the event of disruptions lead swift and effective responses to minimise service downtime and support community recovery, reinforcing the city's resilience.

Judgement, Decision Making and Financial Responsibility

Exercise independent judgement interpreting legislation. Makes strategic decisions anticipating operational and policy challenges. Uses data and insights for decisions. Resolves complex operational issues. Makes high-impact decisions on safety, service continuity, and budgets.

Specialist Skills and Knowledge

Advanced knowledge of cyber security frameworks, ICT operations, cloud platforms, enterprise architecture, IT service management, automation, governance, and regulatory compliance.

Interpersonal Skills

Excellent communication and influencing skills. Political acumen. Effective collaboration with ELT, departments, contractors, and community. Strong stakeholder engagement and customer focus. Ability to lead through change.

Qualifications and Experience

Tertiary qualifications in Information Technology, Information Systems, or a related discipline, with significant senior-level experience across cyber security and technology operations. Relevant cyber security and cloud certifications are desirable.

Child-Safe Standards

Maintain a child safe culture at City of Port Phillip by understanding and activating your role in preventing, detecting, responding and reporting suspicions of child abuse to the relevant authorities by adhering to relevant City of Port Phillip policies and relevant legislation.

Occupational Health and Safety Responsibilities

All employees of City of Port Phillip are responsible for maintaining and ensuring the OHS programs in their designated workplace as required by the Occupational Health and Safety Act 2004. Where applicable this includes taking every reasonably practicable step to ensure the health and safety of employees, contractors, visitors, and members of the public through identifying hazards, assessing risk, and developing effective controls within the area of responsibility and by adhering to relevant City of Port Phillip policies and legislation. Our leaders are responsible for championing and enhancing safety in our organisation.

Diversity and Equal Employment Opportunity

The City of Port Phillip welcomes people from diverse backgrounds and experiences, including Aboriginal and Torres Strait Islander peoples, people from culturally and linguistically diverse (CALD) backgrounds, LGBTIQ+, people with disability, as diversity and inclusion drives our

success. Our leaders are responsible for championing and enhancing diversity and inclusion in our Organisation and City.

Security Requirements and Professional Obligations

Pre-employment screening will apply to all appointments. Prior to a formal letter of offer, preferred applicants will be asked to provide:

- Evidence of mandatory qualifications/registrations/licences,
- Sufficient proof of their right to work in Australia
- Sufficient proof of their identity.
- Complete a National Police Check completed **via** City of Port Phillip's Provider.
- Evidence of a Working with Children Check *(employee type with City of Port Phillip registered as the organisation).*

The City of Port Phillip celebrates a vibrant and diverse work environment and community, which includes people of Aboriginal and/or Torres Strait Islander background, people of diverse sexual orientation and gender, people from culturally and linguistically diverse backgrounds and people of varied age, health, disability, socio-economic status, faith and spirituality. Employees can develop both professionally and personally whilst planning and delivering a range of important services and programs to the community.