POSITION DESCRIPTION

Role title:	**Head of Information Technology Operations** *Head of IT Operations*
Term:	Fixed term backfill position of 6-months. Available as a contract position or as a secondment.
Full-time equivalent:	1.0FTE
Job Classification:	VPS Grade 5.1 equivalent
Base salary:	$113,022 – $124,884 per annum *Classification dependent on experience*
Entitlements:	• Superannuation of 15.5%, paid on base salary • 12 Rostered Days Off (RDOs) per year • 4 weeks of annual leave
Enterprise Agreement:	*The CPSU SPSF Group Victorian Branch Staff Agreement 2017*
Reporting to:	The Branch Secretary
Primary workplace:	128 Exhibition Street, Melbourne VIC 3000

ROLE PURPOSE

The **Head of IT Operations** is responsible for the end-to-end operational management, reliability, security, risk, and continuous improvement of the Branch's information technology environment. The role ensures that all core systems — including equipment, infrastructure, cloud services, internal and external applications, websites, and the organisation's case tracking and membership systems — are operational, secure, resilient, compliant, and fit-for-purpose, and that technology effectively supports the union's industrial, organising, campaigning, governance, and accountability objectives.

The role also acts as the organisation's **Privacy Officer**, with accountability for data protection, privacy compliance, cyber security incident response, and related assurance obligations across all IT systems and platforms.

ORGANISATIONAL CONTEXT

The **Community and Public Sector Union, State Public Services Federation Group (CPSU SPSF Group Victoria)** is the union that represents Victorian public sector workers. This includes employees in the Victorian Public Service, associated public entities such as statutory authorities, public corporations, and arts and cultural institutions; as well as a handful of community and other third-sector organisations.

CPSU Victoria represents members across a wide range of occupations and departments—policy, administration, regulation, heritage and culture, IT, justice, child protection, corrections, and more. The union is based at **Level 4, 128 Exhibition Street, Melbourne**, and operates within the national industrial relations system, principally but not only under the *Fair Work Act 2009* and the *Registered Organisations Act 2009*.

The **CPSU Victoria** has a proud history dating back to 1885, when the first Victorian public service association was formed to secure fair treatment, job security, and independence from political interference. Today, CPSU Victoria continues that tradition—fighting for fair pay, safe workplaces, secure jobs, and respect for the vital work public sector employees do to serve the Victorian community.

ORGANISATIONAL CONTEXT
The union is a democratic, member-led organisation, governed by an elected Branch Council and Executive. It is affiliated with Victorian Trades Hall and the Australian Council of Trade Unions (ACTU) and works collaboratively with other unions and civil society partners to advance the rights of working people.

DUTY AREA	DESCRIPTION
Ensure IT Service Reliability	• Lead and manage the day-to-day operation of the Branch's information technology environment, ensuring systems are reliable, available, secure, and fit-for-purpose. • Act as the primary operational point of contact for IT service performance and system issues, ensuring timely investigation and resolution. • Establish, maintain, and continuously improve operational standards, procedures, and controls across all IT systems and platforms. • Oversee incident, problem, and change management processes to minimise disruption and improve system resilience.
Maintain IT Equipment, Infrastructure, Platforms and Core Systems	• Oversee the operation and lifecycle management of IT equipment, servers, networks, cloud services, end-user computing environments, internal and external applications, websites, case tracking systems, and membership systems. • Manage and protect these systems as mission-critical operational platforms, ensuring they are secure, stable, well-integrated, and fit-for-purpose. • Ensure appropriate backup, recovery, and disaster recovery arrangements are in place and regularly tested. • Maintain oversight of system capacity, performance, scalability, and operational sustainability. • Maintain the IT components of the Branch Register of Assets.
Systems Development, Continuous Improvement & Operational Alignment	• Lead the development, maintenance, and enhancement of internal tools and systems to improve operational efficiency and support industrial, organising, campaigning, and governance activities. • Work closely with industrial, organising, campaigning, communications, and administrative teams to ensure IT systems effectively support operational and strategic needs. • Translate organising, advocacy, and campaign requirements into practical, secure, and sustainable technical solutions. • Identify opportunities to streamline processes, improve user experience, and increase system effectiveness through technology. • Provide forward-looking advice on emerging technologies and operational improvements.
Vendor & Service Provider Management	• Manage day-to-day relationships with external IT vendors, service providers, and contractors, and support maintenance of the IT component of the Branch Register of Contracts. • Monitor performance against contracts and service levels, ensuring value for money and operational reliability. • Lead operational input into procurement processes, renewals, and vendor performance management.
Risk, Compliance, Governance & Assurance	• Identify, assess, and manage operational IT risks, ensuring compliance with relevant legislation, policies, and standards relating to data, privacy, information security, and record-keeping.

DUTY AREA	DESCRIPTION
	• Ensure systems and practices support the Branch's governance, accountability, and assurance obligations. • Maintain clear system documentation, records, and operational reporting. • Provide clear, timely advice to senior leadership on IT risks, system vulnerabilities, incidents, and mitigation strategies. • Report on IT performance, incidents, risks, and improvement initiatives to senior leadership and governance bodies.
Cyber Security, Privacy & Data Protection (Privacy Officer)	• Act as the organisation's **Privacy Officer**, with accountability for privacy compliance across all IT systems and platforms. • Oversee cyber security controls, data protection measures, access management, and monitoring. • Lead responses to data breaches, cyber incidents, and privacy complaints, including investigation, remediation, and reporting. • Develop, maintain, and deliver privacy and information security policies, procedures, and staff training.
Other duties	• Any other duties as assigned by the Branch Secretary.