Position Description

Position title:	IDAM Security Analyst
Reports to:	IT Assurance & IDAM Manager
Business unit:	IT
Employment category:	Employment Agreement

About CitiPower and Powercor

As electricity distribution companies we provide safe, reliable and affordable power to 1.9 million Victorian customers. We use our network of poles, wires and infrastructure to bring power to homes and businesses across almost 65% of Victoria — that's more than 120,000 kilometres of wires and 850,000 poles.

But we do so much more than manage poles and wires. We're also the gateway to a clean energy future, dedicated to finding solutions and harnessing new technology to benefit our customers, communities and the environment. This includes industry leading projects in community batteries, demand management, smart charging for electric vehicles (EVs) and microgrids.

And as more customers choose solar, batteries, EVs and smart appliances — the electricity system is becoming increasingly complex, and so too is the level of innovation required to manage it.

About the IT team you'll be part of

Information Technology provide the business with technology, tools and solutions that help us achieve our strategic objectives. The team are responsible for managing and enabling our core business systems, OT & network control systems, digital transformation, IT security, IT architecture, along with overseeing all desktop and network management applications.

Our core values

Purpose of the position

The IDAM Security Analyst is responsible for managing the end-to-end user access lifecycle, ensuring that only authorised users have appropriate levels of access to company systems. The role enforces auditable and compliant processes, while partnering with business owners to validate access requirements on an ongoing basis. It includes oversight of processes run by external service providers and collaboration with IT clients such as South Australian Power Networks and Wellington Electricity.

Your key responsibilities

IT User Access Processes

- Manage user access provisioning, modification, and deprovisioning in line with business and compliance requirements.
- Validate and fulfil access requests promptly, ensuring access is approved, appropriate, and assigned to the right individuals.
- Support seamless access processes across internal teams and external providers.
- Troubleshoot access issues, resolve incidents, and keep stakeholders updated throughout the resolution process.
- Process access requests within defined OLAs and SLAs, maintaining a strong customer focus.
- Liaise with IT support teams and business clients to ensure effective user access management.

Access Administration

- Ensure compliance with IT security standards, frameworks, and governance requirements.
- Maintain and improve user access documentation and procedures, securing stakeholder review and approval as needed.
- Support user access reviews with the Security team and business stakeholders to confirm access appropriateness.

Security Administration

- Ensure access and security records are accurate, complete, and auditable.
- Contribute to the development and maintenance of user access policies, standards, and procedures.
- Support audit and compliance activities by providing evidence, reporting and analysis on user access.

Employee Development

- Maintain current knowledge of Active Directory, Identity Management systems, and access lifecycle practices.
- Build expertise in role-based and birthright provisioning models, PAM/IGA concepts, and related IAM technologies.
- Develop technical and soft skills through collaboration with senior team members, security architects, and external providers.
- Proactively identify opportunities for process improvement and participate in initiatives to uplift the organisation’s access management capability

What you'll bring to the business

Education / Qualifications:

- Tertiary qualification in IT/Computer Science, or related discipline
- Sailpoint & Microsoft AD and Entra Administration desirable

Knowledge:

- Strong working knowledge of Microsoft Active Directory (AD) administration, SailPoint IIQ, CyberARK Entra AD.
- Understanding of Identity Management systems and access lifecycle concepts (e.g., role-based, birthright provisioning).
- Experience in IT systems administration with data analysis/manipulation skills (Excel or equivalent).
- Knowledge of IT security frameworks and compliance requirements.
- Strong customer service orientation with excellent communication and stakeholder engagement skills.
- Analytical problem-solving skills with openness to innovation and continuous improvement

Experience:

- Strong knowledge user access management principles and best practices
- Administration of identity management access systems and tools
- Strong Analytical and MS Excel skills
- Previous experience (two years minimum) in an IT Service Desk or IT Desktop support environment

The skills and competencies you'll have

'Thought' competencies

1. Customer focus: Building strong customer relationships and delivering customer-centric solutions
2. Manages complexity: Making sense of complex, high quantity, and sometimes contradictory information to effectively solve problems
3. Balances stakeholders: Anticipating and balancing the needs of multiple stakeholders

'Result' competencies

1. Action oriented: Taking on new opportunities and tough challenges with a sense of urgency, high energy, and enthusiasm
2. Resourcefulness: Securing and deploying resources effectively and efficiently
3. Optimises work processes: Knowing the most effective and efficient processes to get things done, with a focus on continuous improvement

'People' competencies

1. Collaborates: Building partnerships and working collaboratively with others to meet shared objectives
2. Communicates effectively: Developing and delivering multi-mode communications that convey a clear understanding of the unique needs of different audiences
3. Manages conflict: Handling conflict situations effectively, with a minimum of noise

'Self' competencies

1. Being resilient: Rebounding from setbacks and adversity when facing difficult situations
2. Self-development: Actively seeking new ways to grow and be challenged using both formal and informal development channels
3. Situational adaptability: Adapting approach and demeanour in real time to match the shifting demands of different situations

Other relevant information

- Availability duty may be required