

Identity and Access Developer

ASX Position Description

ASX “All Roles Flexible”

ASX offers mutually beneficial flexible working arrangements.
We recognise that employees need to balance work and personal lives.

ASX Opportunity Snapshot		What’s On Offer
Role:	Identity and Access Developer	Identity and access management is a critical component of IT security and an enabler for ASX staff and customers. This role will be responsible for leading development of ASX’s Identity & Access, and Privilege Management systems. The role entails using new technology to improve efficiency, customer satisfaction, compliance and control effectiveness in this area. The role will require an understanding of the technologies involved, a compliance and development mindset, as well as the ability to innovate and drive change in the area.
Reports to:	Identity and Access Manager	
People Management:	N/A	
Budget:	N/A	
Team:	Technology Security	
Date:	August, 2021	
Location:	Sydney, NSW	
Flexible Role:	Yes	

What you’ll do:

- Identity and Access Management development and integration for common Identity Management Platforms
- Provide 2nd and 3rd level support for the ASX Identity Platforms identified above as well as Privilege and Secrets Management solutions
- Manage the Dev Ops deployment approach for the ASX Identity function
- Take ownership and drive key Identity Access Management compliance and business requirements with a perspective on continued development and automation of industry leading Identity & Privileged Access Management solutions
- Assist with the solutions design of IAM projects by applying your experience to expand your skillset with a multitude of industry leading technologies, applications and platforms
- Work with business stakeholders to:
 - Identify and implement business specific access using the company role-based access models to help promote security and efficiency
 - Code development to meet required project and day to day needs surrounding access and management of external / internal accounts and permissions
 - On-boarding of external customer access to various in-house systems and applications utilising your development skillset to code and adapt code where required
 - Analyse, develop and implement appropriate segregation of duties

- Develop and implement Privileged Access roles and rules to facilitate controlled access to Production systems
- Implementation of action plans to resolve security related issues
- Deal with internal teams to achieve resolution of issues or requests as required
- Ensure IAM policies and procedure documentation remain current and meet with compliance
- Assist in the investigation, identification and documentation of IAM risks and associated controls
- Build and extend upon the strong environmental controls and processes by continually questioning and enhancing the process

What you've done:

- Foundation in modern development practices and languages such as: Java, and JavaScript/Groovy
- Experience with Dev Ops practices for deploying & managing deployments including CI/CD tools such as Git/GitHub, Bamboo/Jenkins, GOCD, Ansible
- Experience in the delivery & support of identity management solutions for both internal and external customer facing scenarios
- Experience in implementing OAUTH2 / OpenID Connect (OIDC) / SAML 2.0 flows
- Understanding of Privileged Access and Secrets Management concepts
- Experience with large-scale enterprise infrastructure
- Knowledge or experience with database security concepts
- Working knowledge of networking principles
- Understanding or experience with Multi-factor authentication technologies
- Experience with patching and upgrading of operating systems
- Familiarity with:
 - ✓ Windows and Linux Operating systems
 - ✓ Application solutions such as Active Directory, SQL Databases and Cloud Services
 - ✓ Data scripting, extraction, transformation and loading
- Technical documentation

And if you've got some of this, even better:

- Knowledge or experience with the SailPoint and ForgeRock Identity Platforms
- Must be able to think out of the box to troubleshoot non-standard / undocumented issues, and to look at the big picture and determine solutions that fit within the existing framework
- Be confident to provide input to assist with continual improvements
- Been accountable for execution according to established standards, procedures, and processes
- Been accountable for day-to-day system support requirements
- Knowledge or experience with Cloud platforms and applications technologies (Google, Azure and AWS)
- Financial services experience

What you need to enjoy and be good at for this role:

- Keen developer mindset who likes delivering good experiences for customers
- Strong control awareness in an environment where there is no compromise on process controls
- Analytical approach to identify current user profiles, map them to access matrices / models / roles and ensure these are maintained and reviewed appropriately
- Enjoy working in a collaborative environment to implement and maintain best practise security protocols
- Inquisitive nature to question the process to drive innovation
- Be a self-starter and take initiative to communicate, interact and cooperate with others
- Ability to adapt to high pressure situations and priorities