External Publication CO56891380-01

EMPLOYMENT OPPORTUNITY

Closing Date: 02.07.2024

IDENTITY AND ACCESS MANAGEMENT SPECIALIST

WINNIPEG, MB

Manitoba Hydro is consistently recognized as one of Manitoba's Top Employers!

Great Benefits

- Competitive salary and benefits package.
- Defined-benefit pension plan.
- Nine-day work cycle which normally results in every other Monday off, providing for a balanced approach to work, family life and community.
- Flex-time and partially remote work schedule (providing the option to work remotely 3 days per 2 week period), depending on nature of work, operational requirements and work location.

Manitoba Hydro is a leader among energy companies in North America, recognized for providing highly reliable service and exceptional customer satisfaction. Join our team of Manitoba's best as we continue to build a company that supports innovation, commitment, and customer service, while actively supporting a diverse, equitable and inclusive workplace.

As a key member of the Technology Platforms team, in the Information Technology division, you will be responsible for setting the strategic direction for Identity and Access Management (IAM) platforms across the enterprise in partnership with the Cyber Security & Enterprise Architecture division, executing projects against the IAM roadmap, and optimizing the ongoing operations of IAM services. As the Identity and Access Management Specialist you will oversee the implementation and maintenance of user directories, user authentication and authorization, identity management and access governance, and privileged identity across Digital & Technology (D&T) and the business. You will also be responsible for defining the processes, access policies/rules and monitoring the effectiveness of access controls that are enforced by access operations functions.

You will work closely with the Technology Platforms Manager and Cyber Security Office to develop and implement an IAM roadmap. The focus of the IAM roadmap will be on risk reduction, business enablement, operational efficiencies, cost reduction, and security and compliance in alignment with the strategic and operational objectives of D&T and the broader enterprise.

Responsibilities:

- Works with cybersecurity, IAM, and access management teams to identify a long-term vision and high-level IAM strategy.
- Develop the IAM roadmap and oversees the implementation of IAM technologies through the lens of security and an automation first approach.
- Lead access governance by overseeing identity workflows, request/approval workflows, access provisioning workflows, and required policy management.
- Identifies ways to improve efficiency via documentation, templates, and standardized processes.
- Provides subject matter expertise across all IAM topics as it relates to cloud, hybrid, and on-premises technology and privileged access management.
- Delivers successful information security projects by working directly with key business stakeholders, executives, and project teams, and applying industry security practices and principles.
- Conduct security reviews of identity access, assess the risk to these changes, and reduce the overall information risk profile of Manitoba Hydro.
- Implement or coordinate remediation required by policies, standards, reviews, and audits, documenting exceptions as necessary.
- Ensures IAM solutions are implemented to support on-premises, hybrid, and cloud applications.
- Leads Active Directory Services Management and is responsible for identity and role management of corporate resources.
- Provide support to application teams for application integration.
- May have direct reports in the future; would be responsible for staff recruitment, performance assessment, training, career development, and setting clear goal expectations.
- Collaborate with Enterprise Architecture and Cyber Security Office to develop, maintain, and promote technology standards, technical capability guidelines and/or guardrails.
- Work with Enterprise Architecture and Cyber Security Office to identify and document business and technical capabilities

required to support Strategy 2040.
- Contribute to developing and maintaining enterprise reference architectures with Enterprise Architecture and Cyber Security Office.

Qualifications:

- A four-year degree in Computer Science or Computer Engineering from a university of recognized standing with a minimum of six years of directly related experience in software development.
  OR
- A two-year diploma in Computer or Information Programming Technology from an institute of recognized standing with a minimum of eight years of directly applicable software development.
- Five or more years of directly related experience in IAM governance, security administration, or SecOps.
- Any of the following Cloud certifications; Azure Identity and Access Administrator Associate, Azure Security Engineer Associate, or similar GCP/AWS certification would be an asset.
- Experience working with cloud security and governance tools, cloud access security brokers (CASBs), and server virtualization technologies.
- Understanding of IAM related protocols and standards such as SAML, OAuth/OIDC, WS-Fed, SCIM, FIDO, TLS/SSL, RDP, RADIUS, and Kerberos.
- Knowledge and experience with user authentication (MFA, password-less), single sign-on (SSO), and identity access & governance (IAG).
- Knowledge of directory services (Active Directory, LDAP, cloud-based directories) would be preferred.
- In-depth experience designing and building complex Authorization Models by making informed decisions using deep understanding of industry standards such as RBAC/ABAC/PBAC etc.
- Demonstrated experience in architecting IAM solutions within Microsoft Azure and preferably, other cloud providers.
- Experience with user account provisioning and de-provision on a variety of platforms.
- Strong understanding of cloud computing architecture, technical design, and implementations, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) delivery models.
- Any professional security designation or certification would be considered an asset (incl. CISSP, CompTIA Security+, CompTIA Network+, CEH, CCIE, CISA, CRISC or CCNP).
- Proven ability to scope security technology requirements and objectives as well as effort and difficulty of project tasks.
- Demonstrated ability to coordinate and lead multiple projects or activities with competing priorities.

Salary Range
Starting salary will be commensurate with qualifications and experience. The range for the classification is $61.96-$68.46 Hourly, $95,747.86-$131,177.28 Annually.

Apply Now!

Visit www.hydro.mb.ca/careers to learn more about this position and to apply online.
The deadline for applications is **JULY 2, 2024.**

We thank you for your interest and will contact you if you are selected for an interview.

This document is available in accessible formats upon request. Please let us know if you require any accommodations during the recruitment process.
#IND1