Senior Developer - Identity Management Program

Duties:

Responsible for the ongoing development, deployment, and support of identity management programs. Ensures that end-user needs for access to systems are met in a secure, comprehensive, and cost-effective manner. Primary duties include writing code, analyzing data, integrating identity/access management (IAM) applications, administers IAM components and overall system, and resolves complex system problems.

The Senior Developer identifies business needs, provides project management and hands-on implementation support for new IAM applications. Must be team oriented, able to identify high-level functional and technical requirements, interact with project managers to plan project schedules, provide quality assurance review, and be willing to learn new technologies. Additional duties include architecting/designing software solutions, leading teams of developers (both onshore and offshore), conducting code reviews, and developing and enforcing coding standards.

This role performs enterprise level technical analysis, design, installation, maintenance, and modification of client's computer systems focused on managing user identities and user access to system resources.

Requirements:

- Responsible for the technical aspects of implementing IAM best practices
- Design and develop custom applications using Java framework and its integration with IAM (Identity & Access Management)
- Create identity management processes, strategies, and architecture documentation
- Develop security standards and best practices related to identity access management
- Support administration and maintenance of systems as directed by the Information Security Officer
- Support Security Operations as needed and directed by the Information Security Officer
- Other duties as assigned.

Education/Experience/Certifications:

- Bachelor's degree (B.A.) in an IT related discipline required with 5-7 years of relevant software development experience.
- Identity and Access Management (IAM) domain experience with a distinguished track record on technically demanding projects.
- Solid experience delivering federated authentication and account registration solutions.
- Deep understanding of industry standard authentication and authorization protocols, such as Oauth, OpenID, SAML, and secure-by-design principles.
- Experience with security and compliance standards relating to customer data management
- Strong ability to enhance and support IAM systems in complex environments including operationalization, monitoring, and process refinement.
- Equivalent combination of education, experience, and/or training will be considered.

This position requires proof of vaccination. The Company requires that all employees be vaccinated or be approved for a medical or religious accommodation.

Pacxa is an Equal Opportunity Employer.