Identity and Access Management (IAM) Engineer

Mission Aviation Fellowship (MAF), a Christian nonprofit organization founded in 1945, is seeking people who share our passion for seeing the Great Commission carried out near and far. MAF operates globally, but its headquarters are located in Nampa, Idaho. As a part of this organization, this position is a vital part in bringing the Gospel, healthcare, education, disaster relief, food and clean water to isolated people in developing countries.

A Brief Overview
To support the organization's identity and access management systems, as an essential part of the work of MAF so that the Gospel is proclaimed and God's Kingdom is extended.

Essential Duties
- Develop and maintain IAM landscape (50%)
    - Work with business analysts, internal customers, HR, and application owners to understand access requirements
    - Develop an IAM strategy in collaboration with the Information Security team
    - Implement, and maintain identity and access management systems, processes and procedures for self-hosted and Saas/Enterprise applications
    - Maintain documentation for the IAM systems, processes and procedures
    - Adapt the IAM system according to changes in the ever-evolving global organization's context
    - Troubleshoot, identify, and resolve technical identity and access management related issues
    - Improve identity and access management solutions and systems for protection against evolving threats and efficiency
    - Remain up-to-date on current IAM threats and industry solutions
- Network administration and support (30%)
    - Enable Tier 1 TechSupport, Tier 2 System Owners and Business Analysts to administer user accounts and access privileges in the organization's identity management system
    - Provide training to IT team members and end-users on the IAM system
    - Coach other members of the organization on best practices that should be followed in identity and access management
    - Enforcing company policies and procedures related to identity and access management
- Auditing and monitoring (20%)
    - Monitor user activity in the identity and access management system
    - Reporting on identity and access management system activity
    - Participate in IAM audits and review access control reports to identify potential risk

Qualifications
- Bachelor's degree in information technology, information security, computer science, or related field required
- 5 years or equivalent combination of relevant professional experience and education required
- Professional IAM Certification upon hire preferred

Competencies
- Oral/Written Communication
- Thoroughness
- Analytical Thinking
- Decisiveness
- Customer Orientation
- Fostering Teamwork
- Forward Thinking
- Building Collaborative Relationships
- Initiative

Skills
- Advanced understanding of identity and access management best practices, procedures, and software solutions such as EntraID, Okta, Ping Identity, SailPoint, etc.
- Advanced understanding of identity and access management technology such as single signon (SSO), two-factor authentication, privileged access management etc.
- Advanced understanding of network security technologies such as DNS and PKI
- Advanced understanding of authentication standards and technologies such as SAML, OAuth, OIDC, Kerberos, Zero Trust Architecture, FMA, etc.
- Intermediate understanding of Windows, Linux, scripting (VBA, Powershell), LDAP, and SQL
- Intermediate understanding of one or more programming languages (Java, Python, C#)

Physical Requirements
- Frequent walking and sitting.
- Occasional kneeling, crouching, crawling, standing, walking, and stooping.
- Lifting, carrying, pushing, and pulling of up to 75 lbs.
- Requires accurate vision, hearing, manual dexterity, and fine motor skills.
- Serves on stand-by rotation every 3-4 weeks; must be available to physically respond within 30 minutes to data center emergencies.
- Moderate international of up to two trips per year for a duration of one week to one month each for on-site support of computer and network systems

MAF offers a competitive benefits package which includes affordable and rich medical (basic or HDHP), dental and vision insurance; vacation and sick leave accrual begin at date of hire; ten paid holidays per year, plus two personal days; 403(b) plan with up to 5% employer match; paid parental leave; life insurance;, both short and long-term disability. Total Rewards package increases the base salary by an average of ~$35,000 per staff member.

MAF is committed to creating and maintaining a work environment free from any form of unlawful discrimination or harassment. As a faith-based religious organization pursuant to the Civil Rights Act of 1964, Section 702 (42 USC @2000e), MAF has the right to and does solely hire candidates who agree with our Statement of Faith and agree to abide by our Standards of Conduct.

MAF seeks to create a workplace that is intentional about Kingdom Inspired Diversity. Our commitment to our employees extends to their opportunities for personal and professional growth and development. We will make reasonable accommodation for qualified individuals with known disabilities, unless doing so would result in undue hardship to the organization.