### **IAM Principal Engineer - Cloud IAM Team**

**Role:** The Principal IAM Cloud Engineer is a senior-level technical and strategic leader responsible for architecting, designing, and overseeing the implementation of our greenfield multi-cloud IAM program. This role requires a deep understanding of identity and access management principles, as well as extensive experience with cloud-native IAM services. The ideal candidate will provide technical leadership, mentor a team of engineers, and ensure that our IAM solutions align with business objectives, security policies, and regulatory compliance frameworks.

**Responsibilities:**

* **Strategy and Architecture:**
  + Lead the design and continuous evolution of scalable, secure, and resilient IAM solutions across our multi-cloud, hybrid environment.
  + Define the IAM security architecture roadmap and vision, ensuring alignment with business goals and Zero Trust principles.
  + Develop and maintain technical standards, guidelines, and reference architectures based on industry trends and best practices.
  + Act as an advisor to leadership to influence the strategy for applications, infrastructure, and security.
* **Engineering and Implementation:**
  + Provide technical expertise in designing, configuring, and troubleshooting IAM solutions.
  + Lead the development and implementation of automated IAM processes using tools like Terraform, Powershell, or Python to improve efficiency and reduce errors.
  + Champion the use of technologies such as Okta, AWS Identity Center, Azure EntraID, and HashiCorp Vault to manage identities, authentication, and secrets.
  + Oversee the implementation of Identity Governance and Administration (IGA) solutions, including role-based access controls (RBAC), access reviews, and automated provisioning/de-provisioning.
* **Leadership and Mentorship:**
  + Mentor and guide other IAM engineers, fostering collaboration, accountability, and continuous learning.
  + Provide architectural guidance and support during security incidents related to identity and access.
  + Collaborate with cross-functional teams, including development, security, and infrastructure, to embed security best practices throughout the SDLC.

**Qualifications:**

* Bachelor's degree in Computer Science, Information Security, or a related field.
* 5-8 years of experience in IAM or related information security roles, with a focus on designing and implementing IAM solutions within a multi-cloud environment.
* Deep expertise with IAM platforms such as Okta, Azure EntraID, and AWS Identity Center.
* Extensive experience with IGA platforms (e.g., SailPoint, Veza) and Privileged Access Management (PAM).
* Strong understanding of SSO, MFA, and federation protocols (SAML, OAuth, OIDC).
* Proficiency in scripting or automation with tools like Terraform, Python, or PowerShell.
* Strong knowledge of regulatory compliance frameworks (e.g., SOX, ISO 27001).
* Excellent problem-solving, communication, and interpersonal skills.

### **IAM Senior Engineer - Cloud IAM Team**

**Role:** The Senior IAM Cloud Engineer is a hands-on technical expert responsible for the design, implementation, and support of our organization's multi-cloud IAM solutions. This role will be focused on building and automating solutions, integrating applications into the IAM platform, and providing day-to-day operational support. The Senior Engineer will work closely with architects and cross-functional teams to ensure that IAM capabilities are successfully integrated across the organization and that our systems adhere to security and compliance standards.

**Responsibilities:**

* **Engineering and Implementation:**
  + Design, develop, test, and implement IAM systems and solutions to protect information resources.
  + Technically implement and provide support for the administration of on-premise and cloud-based platforms and solutions for workforce identity.
  + Develop and manage IAM automation processes using scripting and automation tools to support integrations and improve business experiences.
  + Onboard new applications and create custom workflows, rules, and reports based on business requirements.
  + Configure and maintain IAM tools and platforms (e.g., Okta, AWS, Azure EntraID).
* **Operational Support and Maintenance:**
  + Monitor and troubleshoot access issues and anomalies; support incident response related to identity and access.
  + Ensure the maintenance, patching, and monitoring of IAM systems.
  + Conduct detailed root cause analysis of technical problems and implement solutions to prevent recurrences.
  + Provide consultative and implementation support for identity-related issues for applications migrating to cloud solutions.
* **Collaboration and Documentation:**
  + Collaborate with IT, Information Security, and Internal Audit teams to ensure alignment with security policies and regulatory requirements.
  + Maintain documentation related to IAM architecture, processes, and standards.
  + Create or partner to create data visualizations supporting trend analysis to proactively address IAM challenges.

**Qualifications:**

* Bachelor's degree or equivalent work experience in a related field.
* 3-5 years of hands-on experience in IAM or information security roles.
* Proven experience implementing SSO application onboarding and MFA integrations with cloud-based identity providers.
* In-depth understanding of IAM, Single Sign-On, and Multi-Factor Authentication (MFA).
* Experience with one or more IAM platforms, such as Okta, Azure EntraID, SailPoint, or Ping Identity.
* Experience with scripting or automation using languages like Python, PowerShell, or Bash.
* Familiarity with cloud platforms such as AWS, Azure, or GCP and their IAM capabilities.
* Knowledge of security protocols and standards like SAML, OAuth, and OIDC.
* Strong communication and analytical skills.