UNIVERSITY OF SOUTHERN CALIFORNIA

Lead Engineer, Identity Access Management

Job Code: 166023

OT Eligible: No
Comp Approval: 9/25/2017

JOB SUMMARY:
This position acts the lead engineer in designing, developing, testing, implementing, and integrating Identity and Access Management systems and solutions. Responsibilities include identification, analysis and resolution of system design weaknesses including troubleshooting and managing the resolution of issues. The IAM Lead Engineer is responsible for guiding and facilitating successful and on-time completion of major projects, and finding solutions to complex issues surrounding access to systems. This position works with IT internal support teams as well as external clients within the university to provide the highest standards of support relative to identity access management practices. Other responsibilities include monitoring and maintenance of IAM systems, training and communication of IAM processes, and advising on IAM solutions and best practices.

JOB ACCOUNTABILITIES:

*E/M/NA  % TIME

______  ______  Leads the design, development, testing, implementation, and integration of Identity and Access Management (IAM) systems and solutions. Ensures that solutions protect information resources against unauthorized use, inappropriate degrees of access, disclosure, damage and/or loss.

______  ______  Guides and facilitates the successful and on-time completion of major programs and projects. Facilitate the continuous adoption, training, communication, and education of IAM capabilities, functions, and standards.

______  ______  Leads the identification, analysis, and resolution of system design weaknesses. Troubleshoots and manages the resolution of issues related identities, systems, access, accounts, authentication, authorization, entitlements, and permissions. Determines and recommends the most appropriate response to identified more complex problems, issues and/or defects by assessing impact and prioritization.

______  ______  Serves as an IAM Subject Matter Expert (SME). Drives the alignment of IAM solution requirements and best practices by using appropriate standards, processes, procedures, and tools throughout the system development life cycle.

______  ______  Ensures the maintenance, patching, operating, and monitoring of IAM systems. Troubleshoots, supports and resolves system incidents, problems and changes, as required.

______  ______  Collaborates with technology, functional, and business partners to improve communication, ensure alignment, and achieve shared objectives. Serves as a point of contact for information security.

______  ______  Establishes and implement frameworks, methodologies, and systems to continuously improve the delivery and quality of IAM solutions. Designs reusable strategies, decisions, service components, libraries and frameworks to support enterprise-level IAM services.

______  ______  Mentors other team members in systems integration, software engineering, systems administration, IT operations, and information security.
Maintains awareness and knowledge of current changes within legal, regulatory, and technology environments which may affect operations. Ensures senior management and staff are informed of any changes and updates in a timely manner. Establishes and maintains appropriate network of professional contacts. Maintains membership in appropriate professional organizations and publications. Attends meetings, seminars and conferences and maintains continuity of any required or desirable certifications, if applicable.

Performs other related duties as assigned or requested. The university reserves the right to add or change duties at any time.

*Select E (ESSENTIAL), M (MARGINAL) or NA (NON-APPLICABLE) to denote importance of each job function to position.

**EMERGENCY RESPONSE/RECOVERY:**

Essential:  
- Yes  In the event of an emergency, the employee holding this position is required to "report to duty" in accordance with the university’s Emergency Operations Plan and/or the employee’s department’s emergency response and/or recovery plans. Familiarity with those plans and regular training to implement those plans is required. During or immediately following an emergency, the employee will be notified to assist in the emergency response efforts, and mobilize other staff members if needed.

**JOB QUALIFICATIONS:**

**Minimum Education:**
- Bachelor’s degree
- Combined experience/education as substitute for minimum education

**Minimum Experience:**
- 7 years

**Minimum Field of Expertise:**
- Hands-on technical experience in systems integration or software engineering of identity and access management (IAM) solutions (such as BeyondTrust, CyberArk, Duo, Fischer International, ForgeRock, Grouper, ISIM, OIM, OUD/OVD, Ping Identity, RadiantLogic, SailPoint, Saviynt, Shibboleth, Thycotic). Experience with one or more programming languages such as Java, C#, C/C++, Python, or JavaScript. Experience with information security concepts such as authentication, access control, and cryptography. Experience with Linux/Unix, Windows, scripting (with programming languages such as Bash, PowerShell, Perl, or Bash), SQL, LDAP, and web services.

**Preferred Education:**
- Bachelor’s degree

**Preferred Field of Expertise:**
- Expertise in financial services, healthcare, or other regulated industries. CISSP certification.

**Skills:** Administrative:
- Communicate with others to gather information
- Customer service
- Research information
- Understand and apply policies and procedures
Skills: Other:

- Analysis
- Assessment/evaluation
- Consulting
- Organization
- Problem identification and resolution
- Teaching/training

Skills: Technology:

- Configuration management
- Database administration and management
- Database and application security
- Groupware applications
- Incident/problem management
- Network administration
- Network administration reporting
- Network communications technologies
- Network security access, management and testing
- Network systems/data backup, storage and recovery
- Server security policies and procedures, access management
- Technical documentation
- Technical training and instructional design
- Troubleshooting

Skills: Machine/Equipment:

- Computer network (department or school)
- Computer network (university)
- Computer peripheral equipment

Supervises: Level:

- Leads one or more employees performing similar work.
- May oversee student, temporary and/or resource workers.

Comments:

- Ability to work evenings, weekends and holidays as the schedule dictates.

SIGNATURES:

Employee: ___________________________ Date: ___________________________

Supervisor: ___________________________ Date: ___________________________

The above statements are intended to describe the general nature and level of work being performed. They are not intended to be construed as an exhaustive list of all responsibilities, duties and skills required of personnel so classified.

The University of Southern California is an Equal Opportunity Employer