The Identity Access Management Engineer is responsible for designing, developing, testing, implementing and integrating Identity and Access Management systems and solutions. Responsibilities include identifying, analyzing and resolving systems design weaknesses, prioritizing troubleshooting efforts and pinpointing resolutions 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:**

<table>
<thead>
<tr>
<th>E/M/NA</th>
<th>% TIME</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Designs, develops, tests, implements, and integrates 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. Leverages problem solving and data analysis skills to ensure projects deliver on time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identifies, analyzes and resolves 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensures the maintenance, patching, operating, and monitoring of IAM systems. Troubleshoots, supports and resolves system incidents, problems and changes, as required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facilitate the continuous adoption, training, communication, and education of IAM capabilities, functions, and standards.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defines, promotes, and advises on solutions and best practices by using appropriate standards, processes, procedures, and tools throughout the system development life cycle.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Designs reusable strategies, decisions, service components, libraries and frameworks to support enterprise-level IAM services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

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: [ ] No  
[ ] 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:**

5 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:

- May oversee student and/or temporary 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