

**UNIVERSITY OF SOUTHERN CALIFORNIA**

**Engineer, Identity Access Management**

**Job Code: 166019**

---

**OT Eligible:** No

**Comp Approval:** 1/11/2022

---

**JOB SUMMARY:**

Responsible for designing, developing, testing, implementing and integrating identity and access management systems and solutions. Identifies, analyzes and resolves systems design weaknesses, prioritizing troubleshooting efforts and pinpointing resolutions to complex access issues. Works with internal/external stakeholders to provide support, advising on IAM solutions and best practices.

**JOB ACCOUNTABILITIES:**

**\*E/M/NA % TIME**

- |       |       |  |
|-------|-------|--|
| _____ | _____ | Designs, develops, tests, implements, and integrates IAM systems and solutions, ensuring they protect data resources against unauthorized use, inappropriate access, disclosure, damage, and/or loss. Defines, promotes, and advises on solutions and best practices by using appropriate standards, processes, procedures, and tools throughout the system development lifecycle.   |
| _____ | _____ | Identifies, analyzes, and resolves system design weaknesses. Facilitates the continuous adoption, training, communication, and education of IAM capabilities, functions, and standards.  |
| _____ | _____ | Troubleshoots and manages issue resolution regarding identities, systems, access, accounts, authentication, authorization, entitlements, and permissions. Determines and recommends the most appropriate responses to more complex identified problems, issues and/or defects by assessing impact and prioritization.  |
| _____ | _____ | Designs reusable strategies, decisions, service components, libraries, and frameworks to support enterprise-level IAM services. Ensures IAM systems maintenance, patching, operating, and monitoring. Troubleshoots, supports, and resolves systems incidents, problems, and changes, as required.   |
| _____ | _____ | Stays current with any changes in legal, regulatory and technology environments which may affect operations. Ensures senior management and staff are informed of any changes, data breaches and updates in a timely manner. Establishes and maintains appropriate network of professional contacts and memberships in professional organizations. Attends meetings, seminars and conferences and maintains continuity of any required/desirable certifications, if applicable. |
| _____ | _____ | Promotes an environment that fosters inclusive relationships and creates unbiased opportunities for contributions through ideas, words, and actions that uphold principles of the USC Code of Ethics.  |
|       |       | 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:**

3 years

**Minimum Field of Expertise:**

Hands-on technical experience in systems integration or software engineering of IAM solutions (e.g., BeyondTrust, CyberArk, Duo, Shibboleth). Extensive experience with one or more programming languages (e.g., C#, C/C++, Python, Bash, PowerShell, Perl). Experience managing multiple projects simultaneously. Excellent organizational, problem solving and data analysis skills. Proven ability to manage multiple projects and priorities simultaneously. Experience with information security concepts (e.g., authentication, access control, cryptography). Excellent written and oral communication skills, able to interact with a broad spectrum of people on a technical and professional level to share complex information. Experience with Linux/Unix, Windows, scripting, SQL, LDAP and web services.

**Preferred Education:**

Bachelor's degree

**Preferred Field of Expertise:**

Bachelor's degree in information technology, computer science, or related fields. Extensive experience in information security operations at large research universities. Expertise in financial services, healthcare, or other regulated industries. Certified Information Systems Security Professional (CISSP) certification or similar.

**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