



Senior Engineer, Identity Access Management Job Description

JOB INFORMATION

<i>Job Code:</i>	166020
<i>Job Title:</i>	Senior Engineer, Identity Access Management
<i>FLSA Status:</i>	Exempt
<i>Supervisory:</i>	May lead one or more employees performing similar work.
<i>Job Family:</i>	IT Security
<i>Job Family Group:</i>	Information Technology
<i>Management Level:</i>	7 Individual Contributor

JOB SUMMARY

Designs, develops, tests, implements and integrates identity and access management systems and solutions. Responsible for managing multiple highly technical projects simultaneously, applying common engineering principles. 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 QUALIFICATIONS:

Education

<i>Req</i>	<i>Pref</i>	<i>Degree</i>	<i>Field of Study</i>
X		Bachelor's degree	

Additional Education

Check here if experience may substitute for some of the above education.

X Combined experience/education as substitute for minimum education

Work Experience

<i>Req</i>	<i>Pref</i>	<i>Work Experience</i>	<i>Experience Level</i>
X		5 years	

Additional Work Experience

Check here if education may substitute for some of the above work experience.

Combined experience/education as substitute for minimum work experience

Knowledge, Skills and Abilities

<i>Req</i>	<i>Pref</i>	<i>Functional Skills</i>
X		Hands-on technical experience in systems integration or software engineering of IAM solutions (e.g., BeyondTrust, CyberArk, Duo, Shibboleth).
X		Extensive experience with one or more programming languages (e.g., C#, C/C++, Python, Bash, PowerShell, Perl).
X		Experience managing multiple projects simultaneously.
X		Excellent organizational, problem solving and data analysis skills.

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Proven ability to manage multiple projects and priorities simultaneously.
X		Experience with information security concepts (e.g., authentication, access control, cryptography).
X		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.
X		Experience with Linux/Unix, Windows, scripting, SQL, LDAP and web services
	X	Bachelor's degree in information technology, computer science, or related fields.
	X	Extensive experience in information security operations at large research universities.
	X	Expertise in financial services, healthcare, or other regulated industries.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X		Certified Information Systems Security Professional (CISSP) certification or similar

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
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.				
Manages multiple IAM projects simultaneously, prioritizing, identifying, analyzing, and resolving 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.				

Other Requirements

Essential:	Emergency Response/Recovery	Essential:	Mandated Reporter
	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		A mandated reporter who in his or her professional capacity has knowledge of, or reasonably suspects a person who is under the age of 18 years, elderly, or a dependent adult has been the victim of abuse or neglect must report the suspected incident. The reporter must contact a designated agency immediately or as soon as practically possible by telephone or in writing within 36 hours. By virtue

Other Requirements

<i>Essential:</i>	<i>Emergency Response/Recovery</i>	<i>Essential:</i>	<i>Mandated Reporter</i>
	following an emergency, the employee will be notified to assist in the emergency response efforts, and mobilize other staff members if needed.		of the associated job duties, this position qualifies as a mandated reporter as required by state law and USC's policy at: https://policy.usc.edu/mandated-reporters/
<i>Campus Security Authority (CSA)</i>			<i>Essential:</i>
By virtue of the associated job duties, this position qualifies as a Campus Security Authority as required by law and USC's policy at: https://dps.usc.edu/alerts/clery/			No

ACKNOWLEDGMENTS

The above statements reflect the essential and non-essential functions as necessary to describe the principle contents of the job. They are not intended to be a complete statement of all work requirements or duties that may be required of the position. I understand that I may be asked to perform other duties as assigned. USC reserves the right to add or change duties at any time.

The University of Southern California is an Equal Opportunity Employer. USC prohibits discrimination on any basis protected under federal, state, or local law, regulation, or ordinance or university policies. All employment decisions are based on individual qualifications and business need.

I acknowledge receipt of this job description and its associated physical requirements. I have read and understand the job description and job requirements and agree to abide by their contents. I realize that duties may be requested of me that are not specifically stated herein. I understand that I will be expected to adjust to potential fluctuations in work volume. I understand that, if I have any questions about the essential functions or expectations of my position, my supervisor and/or HR partner are available to discuss them with me.

Print Employee Name

Signature

Date

Print Manager Name

Signature

Date

This job description describes the general nature and level of work required by the position. It is not intended to be an all-inclusive list of qualifications, skills, duties, responsibilities or working conditions of the job. The job description is subject to change with or without notice, and Management reserves the right to add, modify or remove any qualification or duty. Nothing in this job description changes the existing at-will employment relationship between the university and the employee occupying the position.