UNIVERSITY OF SOUTHERN CALIFORNIA

Identity and Access Management Director

Job Code: 168031

OT Eligible: No

Comp Approval: 5/1/2017

JOB SUMMARY:

This position is responsible for overseeing the safeguarding of information and systems assets against unauthorized use, disclosure, modification, damage or loss. The Identity and Access Management (IAM) Director serves as a Subject Matter Expert (SME), leading the team responsible for the design, engineering, deployment and support of the university’s comprehensive IAM strategy, processes, and technologies. The position also monitors the access review process, determining and implementing training programs. The Identity and Access Management Director oversees the development and implementation of new applications, manages the relationship with service providers, and responds to formal and informal requests concerning the IAM infrastructure, while providing concerning identity and access management for key stakeholders across the university. The position directly or indirectly manages all program staff and develops and administers a budget, while maintaining up-to-date knowledge in the field of specialty.

JOB ACCOUNTABILITIES:

*E/M/NA % TIME

________  ________ Serves as a Subject Matter Expert (SME). Provides expertise and understanding of all aspects of the Identity and Access Management (IAM) landscape, working with senior leadership to mold, shape and expand the IAM service footprint.

________  ________ Defines an IAM engineering strategy, with a roadmap of key deliverables and timelines, and delivers consistently. Oversees the design of solutions and work plans for the University’s identity and access management in collaboration with internal and external resources.

________  ________ Leads the team responsible for engineering, deploying and supporting best practice identity and access management processes and technologies used by University employees, partners, contractors, and visitors across an extended infrastructure of internal, cloud, mobile, and partner-supplied applications and platforms, where applicable.

________  ________ Directly or indirectly manages program and administrative staff, usually through subordinate managers and supervisors. Recruits, screens, hires, and trains staff, as necessary. Evaluates employee performance and provides guidance and feedback. Counsels, disciplines and/or terminates employees as required. Recommends departmental goals and objectives, including workforce planning and compensation recommendations. Reassesses or redefines priorities as appropriate in order to achieve performance objectives. Recommends, approves and monitors professional training and development opportunities for staff.

________  ________ Participates in the development and administration of the department budget. Approves/disapproves department expenditures. Develops short and long-term budget projections and plans. Provides financial status reports as needed.

________  ________ Oversees operations team to implement IAM systems and manage access review process. Evaluates training effectiveness and determines new training goals and objectives. Gathers training support and provides hiring support to develop skills for new tools and technologies.
Oversees the development and implementation of new applications or infrastructure platforms into the IAM processes. Evaluates application efficacy and determines corrective action, as necessary.

Oversees the designs and implementation of functional requirements within a suite of IAM technologies that are in alignment with IAM strategy of the university.

Reviews IAM status reports. Incorporates input and evaluates program accordingly. Determines corrective action, as necessary.

Engages and monitors professional services providers who support the build of next generation IAM capabilities.

Collaborates cross-functionally with other technology teams and security policy organizations. Represents the unit or university on internal and external committees, task forces, or boards, as assigned. Provides consultation across the university to stakeholders concerning identity and access management.

Formally and informally responds to customer and regulatory requests with regard to IAM security services, mechanisms and safeguards.

Maintains up-to-date knowledge by researching new technologies and software products, participating in educational opportunities and conferences, and reading professional publications.

Develops and implements security related procedures such as office opening and closing routines, recognition of duress signals and key controls. Coordinates security activities with Department of Public Safety. Promotes and maintains standards for security conscious awareness and behavior. Maintains knowledge of University's crime prevention and suppression programs and services. Ensures dissemination of security related information to staff.

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:**
- 8 years

**Minimum Field of Expertise:**
Understanding and technical knowledge of Identity and Access Management concepts, including but not limited to, front line operations, deployment engineering and Next Generation IAM, etc. Demonstrable strong management skills, including the ability to develop, mentor and coach others. Experience in the management and/or implementation of IAM technologies. Strong written and oral executive communication, including up to the C-level. Strong understanding of risk, compliance and ability to define and operationalize cybersecurity processes.

**Preferred Education:**

Master's degree

**Preferred Experience:**

10 years

**Preferred Field of Expertise:**

CISSP preferred. Experience in the implementation and/or management of Identity Access (IAM) technologies and supporting processes. Experience working in a regulatory environment and working in large or federated enterprises, preferably in the university environment.

**Skills: Other:**

- Analysis
- Assessment/evaluation
- Budget control
- Budget development
- Coaching
- Communication -- written and oral skills
- Conceptualization and design
- Conflict resolution
- Consulting
- Counseling
- Customer service
- Human resource process and employment knowledge
- Interpretation of policies/analyses/trends/etc.
- Interviewing
- Knowledge of applicable laws/policies/principles/etc.
- Lead/guidance skills
- Managerial skills
- Negotiation
- Networking
- Organization
- Planning
- Problem identification and resolution
- Project management
- Public speaking/presentations
- Research
- Scheduling
- Staff development
- Statistical analysis
Teaching/training

Skills: Technology:
- Applications/systems development methodologies
- Change management
- Configuration management
- Database design tools and techniques
- Enterprise/information architecture
- Incident/problem management
- Network communications technologies
- Network design, connectivity and capacity configuration
- Operating systems
- Project management tools and techniques
- Release management
- Server applications and hardware
- Technical documentation

Skills: Machine/Equipment:
- Calculator
- Computer network (department or school)
- Computer network (university)
- Fax
- Personal computer
- Photocopier

Supervises: Nature of Work:
- Administrative
- Professional/Paraprofessional
- Technical

Comments:
Evening or weekend work may be necessary to meet deadlines or solve specific problems. On call 24/7 to manage problems.

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