UNIVERSITY OF SOUTHERN CALIFORNIA
Information Security Governance and Risk Management Director
Job Code: 168025

OT Eligible: No
Comp Approval: 4/27/2017

JOB SUMMARY:
This position is responsible for developing the strategy and vision for the governance and risk management team, and the execution of the responsibilities within the governance and risk management directorate. The Information Security Governance and Risk Management Director is accountable for the key governance and risk management areas, including but not limited to, security training and awareness, policy management, information security metrics, data protection, security risk management, information security consulting, third party management, software security and security architecture. This position oversees the data protection program, monitors the effectiveness of the security risk management and third party management functions, and oversees the management of the security architecture function, while providing security risk management consulting and structure from a cyber-governance perspective for key stakeholders across the university. The Information Security Governance and Risk Management Director 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:

<table>
<thead>
<tr>
<th>*E/M/NA</th>
<th>% TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>_______</td>
<td>_______</td>
</tr>
</tbody>
</table>

Serves as a Subject Matter Expert (SME). Provides expertise and understanding of all aspects of the Information Security Governance and Risk Management (ISGRM) landscape, working with senior leadership to mold and shape the ISGRM footprint.

Defines an ISGRM strategy, with a roadmap of key deliverables and timelines, and delivers consistently. Leads large cybersecurity initiatives with a focus on risk management and compliance. Oversees the design of best practice solutions and work plans for the University’s governance and risk management in collaboration with internal and external resources.

Oversees the policy, standards and policy exceptions management process and coordinates approval and updates with appropriate parties. Involves relevant parties for security risk and compliance issues that span legal, compliance and regulatory requirements.

Oversees the data protection program, including assessing the level and quality of service provided by professional services. Evaluates and determines new goals and objectives. Creates, prepares and delivers reports to senior management. Makes recommendations, as necessary.

Oversees the development and delivery of all security training and awareness campaign.

Oversees the needs assessment of information consulting for all schools, units and hospitals. Evaluates and determines new goals and objectives. Creates, prepares and delivers reports to senior management. Makes recommendations, as necessary.
Provides input to the selection of key metrics to monitor and oversees the implementation of metrics capturing, including technology solutions across the university.

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.

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.

Monitors the effectiveness of the security risk management and third party management functions, including assessing the level and quality of service provided by professional services, including software security and security controls assessment services.

Oversees the management of the security architecture function and the integration with risk assessment processes and activities across the university.

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 risk management and governance.

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

**E** 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.

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

**EMERGENCY RESPONSE/RECOVERY:**

<table>
<thead>
<tr>
<th>Essential</th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
</table>

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 key Information Security Governance concepts, including but not limited to security training and awareness, policy management, metrics, and data protection. Understanding and technical knowledge of key Risk Management concepts, including but not limited to security risk management, information security consulting, third party management, software security, and security architecture. Strong technical understanding of enterprise computing solutions including cloud hosting, SAS models and oversight responsibilities. Strong written and executive communication, including up to the C-level.

Preferred Education:

Master's degree

Preferred Experience:

10 years

Preferred Field of Expertise:

CISSP preferred. Experience in the implementation and/or management of Governance, Risk, and Compliance (GRC) 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
Personal mobile communication devices
Photocopier

Supervises: Level:
Manages through subordinate supervisors.

Supervises: Nature of Work:
Administrative
Professional/Paraprofessional
Technical

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