UNIVERSITY OF SOUTHERN CALIFORNIA

Supervising Information Security Specialist

Job Code: 165579

<table>
<thead>
<tr>
<th>Grade:</th>
<th>TL</th>
</tr>
</thead>
<tbody>
<tr>
<td>OT Eligible:</td>
<td>No</td>
</tr>
<tr>
<td>Comp Approval:</td>
<td>9/26/2008</td>
</tr>
</tbody>
</table>

**JOB SUMMARY:**
Supervises the design, development and implementation of information security procedures, systems and related technology.

**JOB ACCOUNTABILITIES:**

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

- Supervises subordinate staff. Recruits, screens, hires and trains staff. Evaluates employee performance and provides guidance and feedback to assigned staff. Counsels, disciplines, and/or terminates employees as required.
- Plans, organizes, coordinates, assigns and evaluates the work of security analysts and technical team members.
- Prepares annual budgets and oversees expenditures related to assigned projects.
- Manages contracts; directs technical teams to produce deliverables within the project plan timeline and budget.
- Prepares training plans for staff, allocates ongoing training for personnel on new computer systems or technologies being implemented which require security administration.
- Analyzes security risks and requirements and rates the importance of university data and services to the related design, implementation and maintenance of the security infrastructure to protect from security breaches.
- Supports integration of information security solutions including security architectures, firewalls, security products, and security implementation plans.
- Reviews security challenges and resolutions; develops implements plans, manages deployment of new technologies, and oversees transition to operational service.
- Reviews and contributes to the security activities portions of application development project plans.
- Interacts with other departments and vendors to gather data, resolve and document complex technical issues for implementation of security products.
- Supervises security management services, forensic analysis, cyber-crime investigation, incident emergency response and investigations.
- Works with senior leadership to determine acceptable levels of risk for university computing platforms and to discuss security implications of new information technology uses being considered.
- Reviews and contributes to the improvement and standardization of the security administration process across all departments.
______  ____  Networks with professional counterparts inside and outside the university. Participates in professional associations to stay informed of new developments and technologies. Makes recommendations to senior management regarding technology changes based on developments in field and business needs.

___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 University Public Safety Department. 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:**

- 5 years

**Minimum Field of Expertise:**

- Understanding of and strong technical knowledge of and experience with network engineering, operating systems, equipment and protocols. Supervisory experience.

**Preferred Education:**

- Master’s degree

**Preferred Experience:**

- 7 years

**Preferred Field of Expertise:**

- Security specific certification and understanding and experience with information security architecture.

**Skills:** Other:

- Analysis
- Assessment/evaluation
- Budget control
- 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.
Organization
Planning
Problem identification and resolution
Project management
Public speaking/presentations
Research
Risk Management
Scheduling
Staff development
Supervisory skills
Teaching/training

Skilled in:

Mathematics
Network security access, management and testing
Programming languages

Skills: Machine/Equipment:

Calculator
Computer network (department or school)
Computer network (university)
Computer peripheral equipment
Fax
Personal computer
Photocopier

Supervises: Level:

Supervises employees and/or student workers.

Supervises: Nature of Work:

Professional/Paraprofessional
Technical

Comments:

May work unpredictable hours. Provide 24/7 on-call support as needed.

SIGNATURES:
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