UNIVERSITY OF SOUTHERN CALIFORNIA
Information Assurance Specialist
Job Code: 165563

Grade: 00
OT Eligible: Yes
Comp Approval: 12/11/2013

JOB SUMMARY:
Brings technical information security experience to the development of USC’s Information Security Program. Assists in providing support and assistance in the design and implementation of technical systems to promote the university’s information security strategy and compliance with regulatory and legal requirements. Assists in developing and implementing an enterprise wide information security strategy. Communicates and reports appropriate metrics regarding the status of the information security program to ITS risk and compliance, audit and others. Coordinates closely with the school/unit ITS liaisons, Compliance, General Counsel and Audit Services, and others regarding information security issues. Reports to the Director, Information Security.

JOB ACCOUNTABILITIES:

<table>
<thead>
<tr>
<th>E/M/NA</th>
<th>% TIME</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Assists with periodic risk assessments to determine and prioritize information security risks to the university. Identifies and evaluates information security controls to mitigate risk. Reports significant changes in information risk to the Director, Information Security and other levels of management as guided by management.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assists with monitoring compliance with information security policies, standards and enterprise wide strategy and facilitates threat and vulnerability evaluations on a regular basis. Measures and reports on the effectiveness of information security controls.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assists with creating and updating information security policies, procedures and standards. Contributes to the Information Security Liaison Committee and the integration of information security requirements into organizational operations, as applicable. Provides supervision of the ISO Task Force and the evaluation of new information security solutions as needed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Conducts vulnerability scanning for IT departments to identify deficient information security controls. Identifies process functions, security weaknesses and controls; presents security challenges and recommendations to other IT technical members in formulating security solutions and requirements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identifies deficiencies and recommends corrective action to strengthen information security controls to decrease the risk of data breach. Discusses recommendations with supervisor and reviews the appropriateness of subsequent action taken to improve information security posture.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides specific technical information security expertise for function supervised. Assists with the delivery/deployment of complex projects and lends technical assistance to others as needed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contributes to the development of departmental goals and objectives. Assists with the implementation and communication to all staff and supervises technical skills and expertise. Makes recommendations to the Director, Information Security on priorities, as appropriate, in order to achieve performance objectives.</td>
</tr>
</tbody>
</table>
Assists with the planning and development of the information security documentation/content for the awareness, education and training programs. Conducts specialized technical information security training for targeted groups and/or specific individuals.

Assists with security incident response and investigations. Conducts reviews to identify root causes of information security incidents and develops corrective action plans in conjunction with compliance and/or audit services.

Participates in periodic audits in conjunction with Audit Services to assure compliance with security policies and standards. Recommends enhancements in such areas as personnel, communication networks, data access, and confidentiality.

Stays informed of new developments and technologies by reading journals and other pertinent publications, and participating in professional organizations, meetings and seminars.

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:  

- 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

**Minimum Experience:**

- 5 years

**Minimum Field of Expertise:**

Five years overall experience in a technical support and operations or design and engineering role within information technology of which at least three years must be in information security in an advisory/internal consultant/subject matter expert capacity. Significant experience with information security technologies, security architecture and design. Extensive experience conducting assessments, digital forensic investigations, vulnerability remediation, incident response and handling zero day attacks, advanced persistent threats, intrusion detection/prevention, email encryption and data loss prevention. Thorough knowledge of risk management, risk analysis and risk assessment methodology. Working knowledge of information security frameworks e.g. NIST and ISO2700 series. Excellent organizational skills, verbal and written communication skills. Ability to triage/prioritize. Strong critical thinking and analytical ability. Able to work effectively with external vendors and all levels of management.

**Preferred Education:**
Preferred Field of Expertise:

Information security education/certifications: CISSP (security professional) and/or any combination of ISSA/ISACA/GSEC certifications such as GSEC (security essentials), GCIF (forensics), GCIH (incident handling), GCED (enterprise defender), GCIA (intrusion analyst). Directly relevant supervisory-level experience in the information security field to provide technical expertise and direction. Exposure to developing or maintaining input to a department budget. Three or more years of experience developing an information security program in a research university and/or academic medical center. Working knowledge of the information security requirements within the applicable regulatory/business environment e.g. FERPA, HIPAA, and PCI. Working knowledge of processes which enable information security i.e. hardening of operating systems, change control management, identity provisioning, vendor risk management. Experience working with faculty, researchers, and physicians.

Skills: Administrative:

- Communicate with others to gather information
- Customer service
- Gather data
- Research information
- Understand and apply policies and procedures

Skills: Other:

- Analysis
- Assessment/evaluation
- Coaching
- Conceptualization and design
- Conflict resolution
- Consulting
- Counseling
- Human resource process and employment knowledge
- Interpretation of policies/analyses/trends/etc.
- Interviewing
- Knowledge of applicable laws/policies/principles/etc.
- Networking
- Organization
- Planning
- Problem identification and resolution
- Project management
- Public speaking/presentations
- Scheduling
- Teaching/training

Skilled in:

- 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)
- Computer peripheral equipment
- Fax
- Personal computer
- Personal mobile communication devices
- Photocopier

Supervises: Level:
May oversee student, temporary and/or resource workers.

Comments:
Evening or weekend work may be necessary to meet deadlines or solve specific problems. Provide 24/7 on-call support as needed.

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