USC University of Southern California

Information Security Manager
Job Description

JOB INFORMATION

Job Code:	165583
Job Title:	Information Security Manager
FLSA Status:	Exempt
Supervisory:	Supervises employees and/or student workers.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	5 Manager

JOB SUMMARY

Provides extensive, specific technical information security expertise for development of USC's Information Security Program. Assists with designing and implementing a university wide information security compliance program, which includes risk assessments, education and awareness, policy and standards development, monitoring and security incident investigations and reporting. Assists with developing and implementing an enterprise wide information security strategy. Supervises subordinate staff. Directs and manages the delivery/deployment of complex projects and lends technical assistance to others as needed. Monitors compliance with HIPAA security, Gramm-Leach-Bliley, Red Flags Identity Theft, PCI standards and other federal, state and administrative regulations regarding information security. Communicates and reports appropriate metrics with management regarding status of the information security program. Coordinates with Information Technology Services, Administrative Information Services, General Counsel and Audit Services, and others regarding information security compliance issues. Reports to the Director, Information Security Officer in the Office of Compliance.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
X		Bachelor's degree		
	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

Req	*Pref*	*Work Experience*	*Experience Level*	
X		5 years		
	X	7 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

Req	Pref	Functional Skills
X		At least 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.
X		Significant experience with information security technologies, security architecture and design.
X		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.
X		Thorough knowledge of risk management, risk analysis and risk assessment methodology.
X		Working knowledge of information security frameworks e.g. NIST and ISO2700 series.
X		Excellent organizational skills, verbal and written communication skills.
X		Ability to triage/ prioritize.
X		Strong critical thinking and analytical ability.
X		Ability to work effectively with external vendors and all levels of management.
	X	Directly relevant supervisory-level experience in the information security field to provide technical expertise and direction.
	X	Exposure to developing or maintaining input to a department budget.
	X	Three or more years of experience developing an information security program in a research university and/or academic medical center.
	X	Working knowledge of the information security requirements within the applicable regulatory/business environment e.g. FERPA, HIPAA, and PCI.
	X	Working knowledge of processes which enable information security i.e. hardening of operating systems, change control management, identity provisioning, vendor risk management.
	X	Experience working with faculty, researchers, and physicians.
	X	Information security education/certifications: CISSP preferred and/or any combination of ISSA/ISACA/GSEC certifications.
	X	CISSP (security professional) or
	X	GSEC (security essentials) or
	X	GCIF (forensics) or
	X	GCIH (incident handling) or GCED (enterprise defender) or GCIA (intrusion analyst).

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Provides specific technical information security expertise for development of USC's Information Security Program. Assists with designing and implementing a university wide information security compliance program. Assists with developing and implementing an enterprise wide information security strategy. Directs and manages the delivery/deployment of complex projects and lends technical assistance to others as needed.				
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 Information Security Officer (ISO) and other levels of management as guided by management and makes recommendations, as appropriate.				
Assists with monitoring compliance with information security policies, standards and enterprise-wide strategy. Facilitates threat and vulnerability evaluations on a regular basis. Measures and reports on the effectiveness of information security controls. Makes recommendations to improve compliance with information system policies, standards and controls, as needed.				
Directly supervises all assigned 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.				
Participates in the creation and updating of information security policies, procedures and standards. Contributes to the Information Security Liaison Committee meetings and the integration of information security requirements into				

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
organizational operations, as applicable. Provides supervision of ISO Task Force activities and evaluation of new information security solutions, as needed.				
Assists with planning, development and ensuring proper functioning of ISO RAN network, training room, forensic lab, including all hardware and software.				
Contributes to development of departmental goals and objectives. Assists with implementation and communication to all staff. Oversees staff's utilization of technical skills and expertise. Makes recommendations to the ISO on priorities, as appropriate, in order to achieve performance objectives.				
Assists with planning and development of information security documentation/content for awareness, education and training programs. Conducts specialized technical information security training programs for targeted groups and/or specific individual sessions.				
Assists with security incident response and investigations. Conducts reviews to identify root causes of information security incidents and develops corrective action plans.				
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.				
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.				

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 following an emergency, the employee will be notified to assist in the emergency response efforts, and mobilize other staff members if needed.		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 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/

Campus Security Authority (CSA)	*Essential:*
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.