USC University of Southern California

Information Security Lead
Job Description

JOB INFORMATION

Job Code:	166031
Job Title:	Information Security Lead
FLSA Status:	Exempt
Supervisory:	May oversee student, temporary and/or resource workers.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

Responsible for planning, designing, and executing security solutions, benchmarking technology strategies, and providing input for the selection and implementation of technology solutions. Accountable for identifying security deficiencies and recommending corrective actions of identified vulnerabilities. Creates and publishes internal controls, ensuring the development and maintenance of adequate compliance resources and training opportunities and fostering a risk and compliance-focused culture within the division. Works with IT internal support teams as well as external clients within the university to provide the highest standards of support relative to information security governance and risk management practices. Provides guidance on security solutions, preparing benchmarking reports and presentations, monitoring security metrics to evaluate efficacy of security programs, and supporting security incident response activities.&nbsp;

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	in IT	
X		2 years	in information security	
	X	5 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		Working knowledge of Windows-based platforms, application and TCP/IP network security technologies, information security concepts, principles and components of a comprehensive information security program.
X		Experience in Application Security concepts, Control frameworks and control objectives. Aptitude for and interest in information and application security.
X		Exceptional organizational skills to balance work and lead projects.
X		Strong, professional written and verbal communication skills.
	X	Advanced knowledge of common web technologies, enterprise and network architecture.
	X	Strong understanding of: modern security tools and controls, secure development life cycle methodologies, programming languages or other scripting languages, web-based application architectures (IIS, Apache, etc.), financial industry regulations such as GLBA, PCI, and SOX application protocols such as MS-SQL, LDAP, and SSO, data protection controls, applied use of cryptography.
	X	Advanced knowledge of or demonstrated experience with defense in depth, trust levels, privileges and Permissions.
	X	Advanced knowledge of or demonstrated experience in application penetration testing.
	X	Advanced knowledge of and experienced development of mainframe and Unix platforms. Large complex industry related experience.

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	*Essential*	*Marginal*	*N/A*
Leads planning, design and execution of appropriate technology security solutions. Examines technology vision, opportunities and challenges with regard to information security standards and their impact on technology, and reacts accordingly in alignment and support of the execution of the USC Information Security Program vision and strategy. Participates in developing security strategy, architecture and tools in accordance with university standards, policies, procedures and other formal guidance, ensuring security technology standards and best practices are maintained across the university.				
Provides assistance in benchmarking technology strategies and architectures. Monitors and anticipates trends and investigates organizational objectives and needs. Provides guidance on security solutions and prepares benchmarking reports and presentations.				
Interfaces with peers and senior leadership and communicates relative information at all levels. Provides Cybersecurity guidance to less-experienced Information Security team members and other technologists across the university. Meets with project teams and other system architects to develop system designs and project plans that include the appropriate security controls and meet security standards.				
Leads and contributes to the assessment of multiple project risks and complexities. Participates in project handoffs including document preparation, training and education, and support to ensure smooth transitions. Assists in the selection and design of tools that allow reuse of design components and plans between similar projects.				
Directs the research, evaluation, proof-of-concept, selection and implementation of technology solutions. Provides detailed pros-and-cons, build-vs-buy analyses of options. Facilitates flexible and scalable solutions. Ensures that the technical design considers security controls, performance, confidentiality, integrity, availability, access and total cost. Assists with working solutions or prototypes and resolves any issues that arise.				
Conducts highly technical/analytical security assessments of custom web applications, mid-tier application services and backend mainframe applications, including manual penetration testing, source code and configuration review using a risk-based intelligence-led methodology. Identifies potential misuse scenarios, and advises on secure development practices.				
Promotes implementation of new technology, solutions and methods to improve business processes, efficiency, effectiveness and security. Configures operational, architectural and design documentation including procedures, task lists, and roadmaps.				

JOB ACCOUNTABILITIES

	% Time	*Essential*	*Marginal*	*N/A*
Helps mature information security risk management processes, programs and strategies. Aligns information security activities with regulatory requirements and internal risk management policies. Identifies security gaps and deficiencies by conducting risk assessments and recommends corrective action of identified vulnerabilities and weaknesses. Leads the planning, testing, tracking, remediation, and acceptance level for identified security risks, and the creation and publication of internal controls. Ensures requisite compliance monitoring is in place to identify control weaknesses, compliance breaches and operational loss events. Ensures adequate compliance resources and training, fostering a risk and compliance focused culture and optimizing relations with team members and regulators.				
Conducts enterprise due-diligence activities, including security monitoring and security metrics, to evaluate effectiveness of the enterprise security program and established controls.				
Guides security incident response activities and post-event reviews of security incidents. Ensures the clear and professional documentation of root cause and risk analysis of all findings. Reviews action plans for issue resolution. Conducts investigation and reports contribution of security threats and incidents.				
Participates in security testing projects according to a structured process, including writing test plans, test cases and test reports. Conducts basic proof-of-concept exploits of vulnerabilities.				
Maintains awareness and knowledge of current changes within legal, regulatory, and technology environments which may affect operations. Ensures senior management and staff are informed of any changes and updates in a timely manner. Establishes and maintains appropriate network of professional contacts. Maintains membership in appropriate professional organizations and publications. Attends meetings, seminars and conferences and maintains continuity of any required or desirable certifications, if applicable.				

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.