USC University of Southern California

Senior Director, Information Security Strategy & Governance

Job Description

JOB INFORMATION

Job Code:	168026
Job Title:	Senior Director, Information Security Strategy & Governance
FLSA Status:	Exempt
Supervisory:	Manages through subordinate supervisors.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	4 Administrator

JOB SUMMARY

Provides leadership and direction for security advisement, university-wide security strategy and governance, and leads security practices which reduce risk and improve regulatory and contractual compliance for information security across the university. Manages and oversees multiple programs (e.g., data protection, enterprise awareness and training, cybersecurity metrics, cyber resilience, cyber emergency preparedness), building and enabling divisional and departmental cyber strategies, training, processes, and fundamentals to increase and mature the university's cyber risk posture.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
X		Bachelor's degree		
X		Bachelor's degree	Information Science	Or
X		Bachelor's degree	Computer Science	Or
X		Bachelor's degree	in related field(s)	
	X	Master's degree	Information Science	Or
	X	Master's degree	Computer Science	Or
	X	Master's degree	in related field(s)	

Additional Education

Check here if experience may substitute for some of the above education.

	Combined experience/education as substitute for minimum education

Work Experience

Req	*Pref*	*Work Experience*	*Experience Level*	
X		10 years	in IT, information security, privacy and risk management across all domains	

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		Experience developing and managing relevant products and services (e.g., EDR/XDR, Cloud security tools, file integrity monitoring, information security configuration, data security platforms, CASB, DLP, IDS/IPS, firewalls).
X		Extensive experience with relevant regulatory requirements (e.g., GLBA, PCI, FERPA, HIPAA).
X		Excellent understanding of security controls frameworks (e.g., CIS Top20, NIST CSF, 800-53).
X		Extensive experience defining and deploying security hardening guidelines.
X		Proven subject matter expertise in different technology stacks (e.g., OS, system, network, application).
X		Excellent leadership and people management skills.
X		Proven understanding of CIS benchmarks and customer service metrics.
X		Experience managing different operating systems and configuration standards.
X		Ability to plan, organize and document complex system design activities.
X		Excellent written and oral communication skills, able to interact with a broad spectrum of people on a technical and professional level to share complex information.
X		Proven analytical, consulting and problem-solving skills, with exceptional attention to detail.
X		Excellent organizational skills and proven ability to manage multiple projects and priorities simultaneously.
X		Ability to manage, teach and train others.
X		Experience with database administration, access management and systems/data backup, storage and recovery.
	X	Extensive experience working in regulatory environments and in large/federated enterprises.
	X	Experience in higher education.

Certifications

Req	*Pref*	*Select Certifications*	*Enter Additional Certifications*
	X		Certified Information Systems Security Professional (CISSP) certification

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	*Essential*	*Marginal*	*N/A*
Provides leadership and directs university-wide cybersecurity strategy and unit-level roadmaps, in support of the department's vision and mission. Leads coordination and response for high-impact initiatives (e.g., cyber emergency preparedness, cyber insurance renewal, third party audits).				
Leads and directs university-wide cybersecurity governance, reporting on maturity, risk performance and effectiveness of information security programs and services and collaborating with others in setting, evaluating, and managing goals and priorities. Leads the security advisory program, providing strategic leadership to executive-level units/stakeholders on improving cybersecurity resiliency. Leads university-wide cyber emergency preparedness program (e.g. ransomware resiliency program, cyber emergency business response plan) and university-wide requirements gathering for cybersecurity external requirements (e.g., contractual, regulatory).				
Provides leadership and expertise for risk management, security metrics, and effective controls to maintain risk levels at acceptable thresholds. Partners with senior leadership on the maintenance of university-wide, central information risk management programs. Provides leadership and expertise for resiliency and business continuity planning, overseeing preparedness for senior leadership response to university-wide crises, (e.g., resource management).				
Provides leadership and expertise for the development and implementation of risk management (e.g., policies and standards, awareness programs, risk mitigation priorities, cybersecurity metrics) and compliance program. Oversees the data protection and high value asset program strategy and classification.				
Stays current with proven/emerging technologies that could strengthen security posture, as well as with any changes in legal, regulatory, and technology environments which may affect operations. Develops and maintains internal/external partnerships with relevant stakeholders to drive effective				

JOB ACCOUNTABILITIES

	% Time	*Essential*	*Marginal*	*N/A*
incident resolutions and the deployment of new security solutions. Ensures senior leadership and staff are informed of any changes and updates in a timely manner.				
Recruits, hires, trains and directly supervises all assigned staff. Evaluates performance and provides feedback. Promotes an environment that fosters inclusive relationships and creates unbiased opportunities for contributions through ideas, words, and actions that uphold principles of the USC Code of Ethics. Establishes and maintains appropriate network of professional contacts and memberships in professional organizations. Attends meetings, seminars and conferences, and maintains required/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/	Yes

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.