USC University of Southern California

Manager, Information Security Engineering
Job Description

JOB INFORMATION

Job Code:	166112
Job Title:	Manager, Information Security Engineering
FLSA Status:	Exempt
Supervisory:	May oversee staff, students, volunteers, agencies and/or resource employees.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	5 Manager

JOB SUMMARY

Oversees management and integrity of security infrastructure and related tools. Responsible for managing technology deployed to protect systems from security threats, data exfiltration, and other information risks. Develops and maintains operational processes, leads information security engineering team, and serves as a technical escalation point for investigative support.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
X		Bachelor's degree		
	X	Bachelor's degree	Computer Science	Or
	X	Bachelor's degree	Information Science	

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		7 years		
	X	8 years		

Additional Work Experience

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

X	Combined experience/education as substitute for minimum work experience

Knowledge, Skills and Abilities

Req	*Pref*	*Functional Skills*
X		Seven years' experience with security engineering technologies and solutions (e.g., EDR/XDR, Cloud security tools, file integrity monitoring, information security configuration, data security platforms, CASB, DLP, IDS/IPS, firewall).

Knowledge, Skills and Abilities

Req	*Pref*	*Functional Skills*
X		Demonstrated understanding of information security engineering processes (e.g., acquisition, design, build, operation).
X		Experience creating RFI/RFPs (request for information/proposal).
X		Demonstrated understanding of security controls frameworks (e.g., CIS Top20, NIST CSF, 800-53). Experience defining and deploying security hardening guidelines.
X		Demonstrated understanding of the technology stack from 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. 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 teach/train others.
X		Experience with database administration, access management and systems/data backup, storage and recovery.
	X	Bachelor’s degree in information technology, computer science, or a related field.
	X	Extensive experience in information security operations at large research universities.

Certifications

Req	*Pref*	*Select Certifications*	*Enter Additional Certifications*
	X		Certified Information Systems Security Professional
	X		Red Hat Certified Systems Administrator
	X		Linux Foundation Certified Systems Administrator

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	*Essential*	*Marginal*	*N/A*
Holds overall responsibility for daily information security engineering functions. Manages technology deployed to protect systems from security threats, data exfiltration and other information risks. Monitors performance and ensures tools have applicable patches/updates and are not reaching EOL (end of life) or EOE (end of effectiveness). Provides technical recommendations in security device selection, configuration and maintenance (e.g., network access control, data loss prevention).				
Leads and supports information security engineering team, relaying expectations and leading initiatives and activities. Drives strategy and performance objectives, establishing team and individual goals. Coaches and mentors staff, providing career development guidance. Recruits, hires, trains and directly supervises all subordinate staff. Evaluates performance, provides feedback, and disciplines and/or terminates staff as required.				
Serves as a technical escalation point for investigative support of security events, alerts, and anomalous activity. Provides input on reporting and metrics captured by governance and risk management. Authors and coordinates reports on system security status and potential/actual violations with procedural recommendations provided. Responsible for driving implementation of daily, weekly and monthly metrics for statistical threats and key performance indicators.				
Develops and maintains operational processes. Ensures procedures and service level agreements are defined, tracked and met. Collaborates with various departments (e.g., security architecture, governance and risk management) to ensure all operations and tasks meet established policies and standards. Maintains currency with any changes in legal, regulatory, and technology environments which may affect operations.				

JOB ACCOUNTABILITIES

	% Time	*Essential*	*Marginal*	*N/A*
Establishes regular communications and conducts resource planning. Ensures senior management and staff are informed of any changes in a timely manner. Recommends departmental goals and objectives (e.g., workforce planning, compensation). Maintains and develops strong internal/external partnerships with business leaders and other units (e.g., threat intelligence, vulnerability assessment) to drive effective incident resolutions.				
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 network of professional contacts and participates in professional organizations (e.g., attends seminars and conferences, maintains required/desirable certifications).				

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/	

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.