KERN COUNTY SUPERINTENDENT OF SCHOOLS
APPROVED NOVEMBER 2026
RANGE: 58.5
CLASSIFIED
CODE: 2, 7

LEAD SECURITY SYSTEMS ENGINEER

DEFINITION
Under general supervision, the Lead Security Systems Engineer will lead security efforts of enterprise technology systems and applications supporting the technology needs of the organization, ensure system security and integrity by creation and implementation of department standards and procedures, and research and mitigation for new threats against the environment.

EXAMPLES OF DUTIES
Lead the design of technology security solutions for KCSOS and districts providing high availability, reliability, and security consistent with expectations and service level agreements;

audit systems for compliance with industry standards and applicable regulatory requirements and assist with changes to establish compliance;

perform or coordinate penetration testing of networks and systems periodically;

audit and maintain tools and systems for keeping operating systems patched and updated;

secure and manage access, services, and security of enterprise applications and cloud environments such as Azure, AWS, O365 and Google Workspace;

lead efforts in troubleshooting technology security issues and assume engineering responsibility for restoration of services and data;

audit backup and recoverability of network device configurations, servers, and data;

audit and assist with implementation of video surveillance and recording systems to guarantee compliance and continued operation;

audit accounts across significant events including creation, access, password and permission changes, and termination;

utilize help desk software for ticket and project functions, maintain infrastructure and business process relationships within a CMDB, and change management including review, impact analysis, and approvals;

lead tool selection and processes creation for internal vulnerability scanning and remediation;

lead the design and administration of directory services including data integrity, interoperability, policies, and authentication methods, including MFA, for elevated access to technology systems;

design and implementation of secure remote access to resources such as cloud-based and VPN;

configure and maintain network security appliances and services such as firewalls, IDS/IPS, and NAC;

conduct incident response for security-related issues including remediation and root cause analysis, and conduct risk assessments regarding technology systems;

available for after-hours and weekend work as required to minimize user impact for projects and tasks, troubleshooting and resolution of technical issues;

lead regular discussions regarding process improvement for technology needs as well as the needs of other departments and customers, including emerging technologies and concerns;

maintain cleanliness of technology spaces and ensure proper procedures and standards are applied in those spaces;

serve as a mentor and provide technical training and guidance to others on security-related projects and issues, customer service, and business operations;

communicate with appropriate organization, department, and district contacts regarding planned and unplanned service impacts;

assist with managing and assigning support tickets to ensure staff is being utilized efficiently to achieve high levels of both quality and quantity of work;

perform other related duties as assigned.

QUALIFICATIONS

Knowledge of:

Windows Server and Linux operating systems and distributions, hypervisors, and client operating systems;

major security frameworks and standards such as NIST and CIS, and regulatory requirements for state and federal privacy laws;

common tools and scripting languages used for data gathering, vulnerability discovery and testing, and identification of indicators of compromise;

firewall configuration and management of NGFW appliances such as Palo Alto, Cisco, and Fortinet;

strong identity and access management concepts including authentication hardening, RBAC, SSO using SAML and OAuth, and Zero Trust.

Ability to:

Communicate effectively in public, conferences, and in written materials;

work at various locations and be able and equipped to communicate as necessary with supervisor regarding whereabouts and task updates;

maintain the knowledge and ability to provide coverage for other engineers for brief periods as required;

stay current on industry trends, emerging technologies, and best practices in security engineering;

maintain knowledge of applicable funding sources and the rules and procedures to utilize them;

develop and maintain relationships with department, organization, and district leaders;

delegate tasks when directed, follow-up with coworkers, and communicate expectations;

excellent organizational skills and the ability to analyze, troubleshoot, and apply critical thinking skills in high-pressure situations;

follow department policies, procedures, and standards both technical and behavioral;

be professional in appearance, attire, communication, and punctuality.

lift 50 pounds, climb ladders, stoop, bend, kneel, squat, crawl, stand for long periods of time, and see and hear sufficiently to safely perform the duties listed above.

Experience:
Combined seven (7) years experience in an engineer role implementing and managing security of enterprise-level appliances, systems, and processes.

Education:
Graduation from a four-year (4) college or university with a bachelor's degree in computer science required.

Additional qualifying experience may be substituted for education on a year-for-year basis.

Conditions of employment:
Some positions may require proof of privately owned automobile insurance and possession of a valid California Motor Vehicle operator's license which must be maintained for the duration of the assignment.

Fingerprint clearance by both the Federal Bureau of Investigation and the California Department of Justice is a condition of appointment after all other required job conditions have been met.

Must present verification of completion of Child Abuse Mandated Reporter training or obtain verification within six (6) weeks of hire and annually thereafter, as required by the California Child Abuse and Neglect Reporting Act.

This position has a probationary period of six months or 130 days, whichever is longer.

CP:rn
11/3/2026
G:\Lead Security Systems Engineer.doc