ELK GROVE UNIFIED SCHOOL DISTRICT

CLASS TITLE: CYBERSECURITY SPECIALIST

BASIC FUNCTION:

Under the direction of the Chief Technology Officer or designee, the position of Cybersecurity Specialist is responsible for managing the cybersecurity strategy program across the organization. The incumbent will develop and implement processes to self-audit IT security systems and identify leading technology to prevent system incursions. The position will work directly with the leadership team to identify, implement, and maintain appropriate technology security solutions for all aspects of the organization.

ESSENTIAL FUNCTIONS:

Informs, develops, and manages a strategic security vision and roadmap to ensure cyber and physical security of all enterprise systems, applications, and data.

Develops cross functional team within the District to perform security verification activities including measurement, verification, validation, and reporting of enterprise compliance with cybersecurity policies, technical security control requirements, security risk assessment and application security.

Research current security solutions to ensure the most efficient and effective security solutions are in place to prevent unauthorized access, use, disclosure, modification, or disruption to systems.

Assists internal teams with identification, evaluation and mitigation of physical and cybersecurity risks and recommends or implements settings, policies, and solutions to ensure security.

Implement and sustain security frameworks to enhance the District’s overall cybersecurity.

Implements, configures, and manages specific cybersecurity solutions, including Data Loss Prevention (DLP) systems, endpoint protection, and centralized security alert logging and reporting systems (SIEM).

Oversees, monitors, and configures managed detection and response (MDR) solution, working closely with the service provider to mitigate malicious cyber threats.

Oversees security event investigations and auditing of all systems and security policies.

Monitors information security and data security management to ensure privacy, integrity, and regulatory compliance.

Ensures compliance with requirements for cyber insurance coverage.

Develops, documents, and routinely audits and tests the District's Incident Response, Disaster Recovery, and Business Continuity Plans, including gap assessments and tabletop exercises.

Develops, audits, and recommends organizational policies related to cybersecurity for the purpose of expressing clear organization expectations.

Works with authorized District staff and legal counsel fulfilling litigation holds and responding to requests for information.

Performs technical security and vulnerability assessments to identify, investigate, and take preventive measures against any potential security threats.

Designs and executes staff security awareness programs, including simulated phishing and social engineering campaigns, to promote security and privacy best practices district wide.

Attends meetings as assigned for the purpose of conveying and/or gathering information required to perform functions.

Assists District administrators as necessary in investigation of security breaches, resource misuse and associated disciplinary and legal matters.

Develops long and short-range plans and programs for the purpose of ensuring that District resources are effectively utilized.

Monitors hardware, software, network devices, applications, web traffic, and databases to determine system vulnerabilities.

Performs related duties as assigned.

DEMONSTRATED KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:
Security best practices, security and compliance frameworks, infrastructure, practices for employing security in a variety of settings from the datacenter to the device level.
Litigation hold processes, eDiscovery procedures, and Public Records Act requests.
Multiple operating systems and commands.
Microsoft technologies (e.g. Active Directory, SQL database, Windows servers, etc.).
Best practices for securing cloud environments (Azure, Google, VMWare, etc.)
Firewalls, intrusion detection systems, advance malware protection, web and email protection.
Complex architected enterprise IT infrastructure and system engineering activities including security threats and security protocols.
Best practices for Data Loss Prevention (DLP)
Federal, state and local laws, rules and regulations related to the scope of responsibilities.
Report writing.
Effective communication strategies both written and oral.
Principles and methods for establishing goals, objectives and implementation plans to accomplish data processing solutions for identified needs.
Emerging security technologies and best practices.
Business process documentation.

ABILITY TO:
Maintain system security for complex architected enterprise IT infrastructure.
Formulate and implement organizational security goals, objectives, and schedules; develop and implement strategic plans and changes required to achieve goals and objectives.
Perform system audits designed to test security.
Effectively convey complex technical concepts to non-technical audiences.

Analyze data and form sound conclusions and recommendations.
Communicate effectively both orally and in writing.
Establish and maintain an effective working relationships with staff, school district personnel, and other agency personnel.
Communicate clearly, effectively, and comprehensively regarding assigned projects, progress and work completed.
Coordinate and conduct workshops and in-services.
Problem solve and analyze issues, create plans of action and reach solutions.
Read, interpret, and understand technical information.
Compose a variety of documents.
Facilitate group discussions.
Work collaboratively on sensitive or critical projects and tasks exhibiting complexity or operational risk.
Respond to emergency situations as needed.

EDUCATION AND EXPERIENCE REQUIRED:

REQUIRED:
Minimum of three years of professional experience administering large-scale technology infrastructure systems and services with a focus on information security, data security, or cybersecurity.

PREFERRED:
Bachelor's degree in computer science or related field.
System security and threat mitigation experience.
Experience in an educational environment.

LICENSES AND OTHER REQUIREMENTS:

Valid California Class C driver's license

WORKING CONDITIONS:

ENVIRONMENT:
Office environment.
Driving a vehicle to conduct work.

BOARD APPROVED: November 4, 2025