ELK GROVE UNIFIED SCHOOL DISTRICT

CLASS TITLE: INFORMATION SECURITY SPECIALIST

BASIC FUNCTION:

Under the direction of the Chief Technology Officer or designee, the position of Information Security Specialist is responsible for establishing and managing the cyber-security 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 solutions for all aspects of the organization.

ESSENTIAL FUNCTIONS:

Directs, develops, and manages a strategic security vision and roadmap (physical and cyber solutions) 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 cyber-security 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 cyber security risks and recommends or implements systems to ensure security.

Implements monitoring systems and processes to detect and minimize 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.

Develops, audits, and recommends organizational policies related cyber security for the purpose expressing clear organization expectations.

Works with authorized District staff and legal counsel on requests for information.

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

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.
Multiple operating systems and commands.
Microsoft technologies (e.g. Active Directory, SQL database, Windows servers, 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.
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.
Security best practices from the Data Center down to the desktop level.
Perform system audits designed to test security.
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 technical information.
Compose a variety of documents and/or 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:
Three years' experience administering/managing large-scale technology infrastructure systems and services.

Preferred:
Bachelor's degree in computer science or related field
System security, and threat mitigation experience

LICENSES AND OTHER REQUIREMENTS:

Valid California Class C driver's license

WORKING CONDITIONS:

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

BOARD APPROVED: June 14, 2022