JOB DESCRIPTION
San Diego County Office of Education

Cybersecurity Officer

Purpose Statement

The job of Cybersecurity Officer is done for the purpose/s of directing, planning, developing and maintaining a comprehensive, enterprise-wide cybersecurity program to protect SDCOE electronic data and network infrastructure from external and internal security breaches, data loss, and privacy violations; ensuring cybersecurity measures taken are in compliance with statutory and regulatory requirements regarding information access, security, and privacy; and providing cybersecurity services to SDCOE county school districts.

Essential Functions

- Collaborates with outside law enforcement agencies for the purpose of investigating electronic security breaches.
- Conducts ongoing security monitoring of electronic information systems, threat and vulnerability assessment for SDCOE and County school districts for the purpose of overseeing remedial action as needed and ensuring timely development and implementation of corrective action plans.
- Coordinates business continuity and data recovery policies with appropriate units across the organization division for the purpose of supporting organization goals.
- Creates audit and security reports for the purpose of identifying needed response to unusual or suspicious activity, exceptions and abnormalities in the SDCOE computing environment.
- Develops, implements, and monitors an ongoing risk assessment program and information security management system for the purpose of targeting electronic information, and infrastructure security, and security breach prevention, detection and remediation.
- Directs and maintains configuration management of electronic security systems, applications, and data encryption for the purpose of providing total data security including policy assessment and compliance tools, network security appliances, and host-based systems.
- Establishes information and infrastructure security controls, including log monitoring procedures, identification of unnecessary services/applications, redundant accounts, risky applications, etc for the purpose of identifying unnecessary services/applications, redundant accounts, risky applications, etc. to support system hardening and policy and procedure alignment.
- Implements practices and standards for user access, operating systems, applications, network security devices, appliance, server patching, etc. for the purpose of incorporating changes to policies, standards, and procedures of the SDCOE and industry best practices.
- Leads an incident response team for the purpose of investigating electronic security breaches.
- Leads the development, maintenance and dissemination of electronic information security, policies, standards, procedures, and practices for the purpose of identifying issues, developing recommendations, enhancing existing systems and/or providing solutions to current processing problems.
- Manages the scoping of necessary hardware and software for the purpose of supporting the uninterrupted availability of an integrated ERP system.
- Provides training programs on information security for IT staff and end users for the purpose of establishing and overseeing an institutionalize knowledge-base of current and emerging electronic

information security technologies, security issues, and information privacy legislation and regulations.

- Serves as a technical resource to SDCOE and County-wide staff for the purpose of providing consultation, advice, and services on data security management, privacy, disaster recovery, and emergency preparedness planning.

Other Functions

- Performs other related duties as assigned for the purpose of ensuring the efficient and effective functioning of the work unit.

Job Requirements: Minimum Qualifications

Skills, Knowledge and Abilities

SKILLS are required to perform multiple, highly complex, technical tasks with a need to occasionally upgrade skills in order to meet changing job conditions. Specific skill based competencies required to satisfactorily perform the functions of the job include: planning and managing projects; preparing and maintaining accurate records including developing and maintaining time estimates and schedules; reading entity-relationship diagrams; supervising staff and project groups; and using pertinent software applications.

KNOWLEDGE is required to perform algebra and/or geometry; review and interpret highly technical information, write technical materials, and/or speak persuasively to implement desired actions; and analyze situations to define issues and draw conclusions. Specific knowledge based competencies required to satisfactorily perform the functions of the job include: current generation and legacy application programming languages; system design; process and data modeling techniques; database theory; processes and practices in developing technical system documentation; software, hardware and related equipment used in large-scale data centers; database management software; practices and procedures for testing disaster recovery plans; principals and techniques of computer applications development and data security in a complex client-server system and multi-platform environment; risk assessment methods and techniques; cybersecurity issues, requirements and trends; and applicable codes/laws/rules/regulations/policies.

ABILITY is required to schedule a number of activities, meetings, and/or events; gather, collate, and/or classify data; and use job-related equipment. Flexibility is required to work with others in a wide variety of circumstances; analyze data utilizing defined but different processes; and operate equipment using a variety of standardized methods. Ability is also required to work with a diversity of individuals and/or groups; work with data of varied types and/or purposes; and utilize a wide variety of types of job-related equipment. Problem solving is required to analyze issues and create action plans. Problem solving with data requires independent interpretation of guidelines; and problem solving with equipment is moderate to significant. Specific ability based competencies required to satisfactorily perform the functions of the job include: setting priorities; communicating effectively with persons of varied technical background; meeting deadlines and schedules; and working with frequent interruptions; and communicating effectively and proactive orally and in writing.

Responsibility

Responsibilities include: working independently under broad organizational guidelines to achieve unit objectives; managing a department; tracking budget expenditures. Utilization of resources from other work units is often required to perform the job's functions. There is a continual opportunity to impact the organization’s services.

Working Environment

The usual and customary methods of performing the job's functions require the following physical demands: some lifting, carrying, pushing, and/or pulling, and significant fine finger dexterity. Generally the job requires 80% sitting, 10% walking, and 10% standing. This job is performed in a generally clean and healthy environment.

Experience Job related experience within a specialized field with increasing levels of responsibility is required.

Education Bachelors degree in job-related area.

Equivalency Bachelor’s degree in computer science or a closely related field from an institution of higher learning accredited by a regional accrediting organization. Master’s degree in computer science or equivalent highly desirable. Professional certification from GAIC or CISSP in one or more of the following areas: Incident Handling, Secure Programming, Security Leadership required. Three (3) to five (5) years working in a technical capacity in one or more of the following areas: database, programming, networking and at least one (1) year management experience managing in a technical capacity.

Required Testing

Certificates

Driver’s License & Evidence of Insurability

GAIC or CISSP Certifcation

Continuing Educ./Training

Maintains Certificates and/or Licenses

Clearances

Criminal Justice Fingerprint/Background Clearance

Tuberculosis Clearance

FLSA State: Exempt

Salary Range: Classified Management, Grade 47

Personnel Commission Approved: October 19, 2016