JOB DESCRIPTION
San Diego County Office of Education

Cybersecurity Architect

Purpose Statement

The Cybersecurity Architect is responsible for planning, designing, building, testing, implementing, and maintaining information security systems within the San Diego County Office of Education (SDCOE) information system infrastructure, and will serve a resource for cybersecurity related matters for SDCOE and school district staff.

Diversity Statement:

Because each person is born with inherent worth and dignity, and because equitable access and opportunity are essential to a just, educated society, SDCOE employee commitments include being respectful of differences and diverse perspectives, and being accountable for one's actions and the resulting impact.

Essential Functions

- Develops and deploys Incident Response Plans and Cybersecurity procedures for information technology.
- Acts as a senior cyber security subject matter expert (SME) to communicate complex technologies and security issues to persons with non-technical backgrounds.
- Designs, builds, implements, and supports enterprise-class information security systems.
- Identifies and communicates current and emerging IT security threats.
- Designs security architecture elements to mitigate IT security threats.
- Plans, researches, and designs robust security architectures for assigned IT projects.
- Performs security assessments, including security program reviews, penetration testing, vulnerability testing, risk analysis, and provides recommendations related to findings.
- Creates IT security solutions that effectively balance business requirements with information and cybersecurity requirements.
- Identifies IT security design gaps in existing and proposed architectures and defines proposed changes or enhancements.
- Reviews and recommends security configuration and policies for firewalls, VPN systems, routers, IDS scanning technologies and servers.
- Defines and maintains security policies and procedures that are aligned to industry best practices.
- Serves as a resource and provides Tier-2 support to cybersecurity staff in response to security-related incidents.
- Communicates cybersecurity-related vital information, security needs and priorities to senior management on a regular basis.
- Monitors information security trends relevant to county office and school districts, keeping management informed about information security-related issues and activities affecting the organization and districts.
- Collaborates with network, application, systems and database teams to ensure SDCOE and participating districts' electronic systems are secure.

- Reviews and analyzes system logs, SIEM tools, and network traffic for unusual or suspicious activity, and make recommendations to restore secure operations.
- Reviews and tests new security software, tools and/or technologies to determine applicability to SDCOE operations.
- Conducts ongoing interviews and assessments with client groups for the purpose of learning how employees interact with technology and to integrate cybersecurity measures.
- Compiles and reports metrics and key performance indicators to senior management in all areas of responsibility.
- Collaborates with SDCOE internal auditing, legal, and IT teams to ensure compliance with applicable legal, regulatory, and industry requirements (e.g. FERPA, HIPAA, PCI-DSS, etc.).
- Identifies and validates security compliance and best practices for securing data, including encryption technologies and key management processes.

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

Knowledge and Abilities:

KNOWLEDGE of:

- SDCOE technology and information systems, and complex IT systems in general;
- Cybersecurity policies and procedures,
- Industry cyber security regulations and standards (e.g. OWASP, SANS, CIS, NIST etc.).
- Specific technology in use by SDCOE and local school agencies,
- Technical aspects of field of technical support and information technology;
- ITIL V4 Service management principles and procedures;
- Principles, methods, and procedures of operating computers, software, software systems, and peripheral equipment;
- Principles and practices of supervision, training, and performance evaluation;
- Principles of budget preparation and control.

ABILITY to:

- Conduct daily cybersecurity operations and services;
- Use current scripting languages and technologies to administer and automate information security systems.
- Interpret laws, regulations, policies, and procedures and apply to cybersecurity-related incidents.
- Work with a wide diversity of individuals;
- Work with similar types of data and utilize job-related equipment;
- Identify issues and select action plans;
- Problem solve with data;
- Be attentive to detail;
- Establish and maintain effective working relationships;
- Communicate with persons with diverse technical knowledge and skills;
- Maintain confidentiality;

- Work with frequent interruptions;
- Work both independently and as a member of a team to meet established goals, objectives, and vision of the unit.

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, some stooping, kneeling, crouching, and/or crawling and significant fine-finger dexterity. Generally, the job requires intermittent sitting, walking, and standing to perform assigned tasks. This job is performed in a generally clean and healthy environment.

Education: Bachelor's degree from an accredited college or university in Information Technology, Computer Science, or closely related field of study.

Experience: Four (4) years of work experience administering IT security controls and compliance assessments. Successful experience in a school environment and experience working in a PeopleSoft environment is highly desirable.

Equivalency: A combination of education and experience equivalent to bachelor's degree in information technology, computer science, or related field of study, and four (4) years of experience administering IT security controls and compliance assessments.

Required Testing
N/A

Certificates
Valid CA Driver's License
GIAC or CISSP certification in areas of Security or Incident Management

Continuing Educ./Training
As needed to maintain certificates

Clearances
Criminal Justice Fingerprint/Background Clearance
Tuberculosis Clearance

FLSA State: Exempt

Salary Range: Classified Management, Grade 044

Personnel Commission Approved: April 21, 2021