

JOB DESCRIPTION
San Diego County Office of Education

Executive Director, Cybersecurity and Digital Privacy

Purpose Statement

Under administrative direction the Executive Director, Cybersecurity and Digital Privacy is responsible for directing, designing, developing, implementing and maintenance of SDCOE's cyber security systems, operating policies and procedures; oversees the SDCOE Cybersecurity department and all internal, external security and digital privacy activities; cultivating an evolving diverse high-performing team to address the information security needs of the SDCOE, school districts and charter schools; serves as technical expert of complex IT systems, cybersecurity, privacy standards, and technology used by SDCOE and local educational agencies within San Diego County and across the State of CA.

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.

Representative Duties

This position description is intended to describe the general nature and level of work being performed by the employee assigned to the position. This description is not an exhaustive list of all duties, responsibilities, knowledge, skills, abilities, and working conditions associated with the position. Incumbents may be required to perform any combination of these duties.

Essential Functions

- Defines, and maintains security policies and procedures aligned to industry best practices.
- Ensures third-party vendors adhere to the organization's security policies and standards by examining vendor security reviews, risk assessments and/or community feedback.
- Interprets laws, regulations, policies, and procedures and applies to cybersecurity-related incidents.
- Compiles and reports metrics and KPIs to management in all areas of responsibility.
- Works closely with internal auditing, legal, and ITS teams to ensure compliance with applicable legal, regulatory, and industry requirements (e.g., FERPA, HIPAA, PCI-DSS, etc.).
- Oversees and coordinates robust vulnerability management and threat intelligence programs to mitigate potential cyber risks.
- Designs and leads security training initiatives for employees across the organization, increasing awareness and understanding of cybersecurity threats and policies.
- Directs the development and maintenance of Incident Response Plans and Cybersecurity procedures for information technology.
- Collaborates with SDCOE departments to promote awareness of data privacy objectives in the organization.
- Maintains knowledge of industry cybersecurity and digital privacy regulations and standards.
- Directs the design, build, implementation, and support of enterprise-class security systems based on the Center for Internet Security (CIS) controls and related standards.
- Initiates and leads open conversations with teams, clients, and stakeholders to build trust and

understanding around cybersecurity and digital privacy initiatives.

- Identifies and communicates current and emerging security threats.
- Designs security architecture elements to mitigate threats as they emerge.
- Plans, researches, and designs robust security architectures for assigned IT projects.
- Anticipates stakeholder needs and develops and discusses potential security and privacy solutions.
- Oversees and analyzes security assessments, including security program reviews, penetration testing, vulnerability testing, risk analysis, and provides recommendations related to findings.
- Creates solutions that balance business requirements with information and cybersecurity requirements.
- Regularly communicates vital information, security needs and priorities to management.
- Monitors information security trends relevant to county office and Local Education Agencies, 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 makes recommendations to restore secure operations.
- Reviews and tests new security software, tools and/or technologies to determine applicability to operations.
- Directs ongoing interviews and assessments with client groups and management for the purpose of learning how employees interact with technology and to integrate cybersecurity measures.
- Identifies and validates compliance and best practices for securing data to include encryption technologies and key management processes.
- Builds, leads, and mentors a high-performing team of information security professionals, fostering a culture of accountability, continuous improvement and professional development.
- Identifies and validates compliance and best practices for securing data to include encryption technologies and key management processes.
- Engages with LEAs and professional organizations (e.g., CITE, TSC, etc.) in meetings, workshops, conferences, and other events as directed.
- Performs personnel administrative functions for assigned personnel (e.g. hiring, counseling, training, supervising, evaluating, providing professional development opportunities, etc.) for the purpose of maintaining necessary staffing, enhancing productivity of staff, and ensuring necessary department/program outcomes are achieved.

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:

Human centered and socially conscious leadership;

Complex IT systems, cybersecurity policies and privacy standards;

Configuration, maintenance, troubleshooting, diagnosis of information security systems and

tools;

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:

Promote a human-centered culture that elevates the strengths of others creating a sense of belongingness;

Practice cultural competency while working collaboratively with diverse groups and individuals;

Use pertinent network, application, and operating system monitoring and troubleshooting software;

Adhere to safety practices;

Prepare and maintain accurate records;

Problem solve to identify issues and select action plans;

Meet deadlines and schedules;

Communicate effectively orally and in writing;

Communicate with individuals of varied technical knowledge and backgrounds;

Establish and maintain effective working relationships;

Set priorities, meet deadlines and schedules;

Working with detailed information/data; applying logical processes and analytical skills;

Work with frequent interruptions;

Independently work and as a member of a team to meet established goals, objectives, and vision of the unit.

Working Environment:

ENVIRONMENT:

Duties are typically performed in an office setting.

May be designated in an alternate work setting using computer-based equipment to perform duties.

PHYSICAL ABILITIES:

Must be able to hear and speak to exchange information; see to perform assigned duties; sit or stand for extended periods of time; possess dexterity of hands and fingers to operate computer and other office equipment; kneel, bend at the waist, and reach overhead, above the shoulders and horizontally, to retrieve and store files; lift light objects. All requirements are subject to possible modification to reasonably accommodate individuals with a disability.

Education and Experience:

Education: A Bachelor’s degree in information technology, Computer Science, or related field.

Experience: A minimum of four (4) years of experience in administering IT security controls and compliance assessments. Successful experience in a school environment and experience working with the current Center for Internet Security (CIS) Controls is highly desirable.

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

Required Testing

N/A

Certificates, Licenses, Credentials,

A minimum of two (2) valid certifications in the following:

- CISSP – Certified Information Systems Security Professional
- GSLC - GIAC Security Leadership
- CISM - Certified Information Security Manager
- CCSP – Certified Cloud Security Professional
- Other related privacy and cybersecurity certifications may be considered.

Valid CA Driver’s License

Continuing Educ./Training

Maintains Certificates and/or Licenses

Clearances

Criminal Justice Fingerprint/Background Clearance
Physical Exam including drug screen
Tuberculosis Clearance

FLSA State: Exempt

Salary Grade: Classified Management Grade 056

Personnel Commission Approved: March 19, 2025