SAN DIEGO COUNTY OFFICE OF EDUCATION
Personnel Commission

CLASS TITLE: Cybersecurity Analyst, Grade 58

DEFINITION:

Under general supervision, provides support to SDCOE and participating district personnel in identifying and assessing their cybersecurity needs; assists in developing and testing new cybersecurity related applications and provides training to SDCOE and participating district personnel in cybersecurity related matters.

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. All requirements are subject to possible modification to reasonably accommodate individuals with a disability.

ESSENTIAL FUNCTIONS:

Provides security guidance to operations staff for the integration of new systems.

Acts as an information security liaison during significant information security risks for both ongoing and planned operations.

Monitors information security trends relevant to SDCOE and county school districts, keeping management informed about information security-related issues and activities affecting the organization and districts.

Works with internal audits and outside consultants as appropriate on independent security audits.

Monitors and reports on information security activities and compliance.

Produces and maintains reports related to cybersecurity.

Monitors system logs, SIEM tools and network traffic for unusual or suspicious activities and interprets such activity and makes recommendations for resolution.

Investigates and resolves security violations by providing analysis to reveal issues and identify solutions.

Monitors internal control systems to ensure that appropriate access levels and security clearances are maintained.

Downloads and tests new security software and/or technologies.

Performs system and application vulnerability testing.

Reviews, assesses, and suggests mitigation solutions for penetration test and vulnerability assessments on information systems and infrastructure.

Monitors security vulnerability information from vendors and third parties.

Participates in information security working group.

Participates in incident response planning and investigation of electronic security breaches.

Participates in the ongoing security monitoring of electronic information systems and ensure timely development and implementation of corrective action plan in response to monitoring deficiencies and complaints.

Participates in security related training.

Collaborates with network and application teams to ensure SDCOE and participating district electronic systems are secure.

Delivers cyber security related training to individuals, small and/or large groups in both informal and formal settings using a variety of presentation media.

Communicates orally and in writing using a variety of media.

NON-ESSENTIAL FUNCTIONS:

Performs related duties as assigned.

CREDENTIALS, CERTIFICATES, LICENSES OR OTHER REQUIREMENTS:

California Driver’s License to travel to districts.

GAIC or CISSP certified in areas of Security Essentials or incident handling highly desirable.

EDUCATION AND EXPERIENCE:

A combination of education, training and/or experience that clearly demonstrates possession of the knowledge and abilities detailed below. A minimum of two (2) years of experience in cybersecurity related fields is required. A typical qualifying background would include two or more years related work experience including significant work within a technical environment in the area of network, application development, computer support, or other complex technical environment.

KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:

Large-scale, complex technical environments including network, infrastructure, data center, desktop support.

Analytical techniques

Application development

Database and data handling practices

Security practices and procedures

Training and development practices

Security tools and applications

Network and data center operations

Desktop support

ABILITY TO:

Quickly develop a thorough technical and working knowledge of the technical environment of SDCOE and county school districts

Identify and analyze potential security breaches and issues and identify mitigation solutions

Use computer equipment, peripherals and software applications

Make effective technical presentations to individuals and groups

Utilize a variety of software applications and hardware

Work effective independently and as part of a team with minimum supervision

Organize and prioritize work

Exercise appropriate judgment in making decisions

Maintain confidentiality of information

Demonstrate attendance sufficient to complete the duties of the position as required

Complete tasks thoroughly, accurately, and with attention to detail

WORKING CONDITIONS & PHYSICAL ABILITIES:

ENVIRONMENT:

Office environment

PHYSICAL DEMANDS:

Must be able to hear and speak to exchange information; see to perform assigned duties; sit for extended periods of time; possess dexterity of hands and fingers to operate a computer and other office equipment.

Established	**Revised**	**Approved by Personnel Commission**	**FLSA Status**	**Salary Grade**
4/2016	03/2021	April 20, 2016	Non-Exempt	Classified Support Grade 058