JOB DESCRIPTION
San Diego County Office of Education

Supervisor II, Cybersecurity Services (M34)

Purpose Statement

The job of Supervisor II, Cybersecurity Services is done for the purpose/s of leading, managing, and planning daily operations for the Information Technology Cybersecurity Team; implementing ongoing enhancements to services; and supervising and evaluating assigned staff.

Essential Functions

- 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.
- Provides security guidance to operations staff for the integration of new systems.
- Acts as an information security liaison during significant information security risk events for both ongoing and planned operations.
- Monitors and reports on information security activities and compliance.
- Monitors system logs, SIEM tools, and network traffic for unusual or suspicious activity, and analyzes data to make recommendations to restore secure operations.
- 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.
- Manages mitigation solutions for penetration test and vulnerability assessments on information systems and infrastructure.
- Monitors security vulnerability information from vendors and third parties.
- Manages incident response team and related activities.
- Participates in the ongoing security monitoring of electronic information systems and ensures timely development and implementation of corrective action plans 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 cybersecurity-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.
- Assists in the formulation and development of policies, procedures, and programs for the purpose of ensuring efficiency and quality of cybersecurity services, including development and implementation of workflow process improvements.

- Communicates with administrators, personnel, and outside organizations for the purpose of coordinating activities, resolving issues and conflicts, and exchanging information as it relates to cybersecurity.
- Conducts ongoing interviews and assessments with client groups and management for the purpose of learning how employees interact with technology and to integrate cybersecurity measures.
- Coordinates delivery of centrally managed support services and service-level processes for all information technology services for new systems and special projects for the purpose of implementing cybersecurity service desk management strategies and processes to ensure the service desk is the single point of contact and service delivery channel for the ITS division in treating cybersecurity threats.
- Designs and/or obtains training materials (e.g. FAQs, support forums, support websites, knowledge base, documentation, etc.) for the purpose of providing a variety of presentation media for in-service trainings to staff, end users, and client districts.
- Interprets and implements laws, regulations, policies, and procedures pertinent to cybersecurity-related incidents.
- Monitors and analyzes technical support effectiveness, efficiency, and customer satisfaction for the purpose of developing and implementing strategies for continuous improvement of the unit.
- Oversees service requests, incidents, and problem resolutions for the purpose of managing and coordinating urgent and complicated support issues, and incidents including managing first- and second-level problem resolution efforts provided by other IT groups, and coordinating third-level problem resolution.
- Participates in professional group meetings, workshops, and/or trainings for the purpose of serving on committees as required and staying abreast of new trends and innovations as it relates to cybersecurity.
- Performs personnel functions (e.g. interviewing, selecting, training, scheduling, mentoring, evaluating, supervising, etc.) for the purpose of monitoring the work flow of assigned staff, reviewing, and evaluating work products and methods of staff.
- Prepares and maintains a variety of reports, records, and files related to personnel and assigned division activities (e.g. Service Level Agreements (SLAs), customer service feedback surveys, work flow process, etc.) for the purpose of evaluating metrics produced from various systems, making recommendations for changes, and implementing changes to improve customer service.
- Utilizes appropriate systems to manage customer requests for technology support for the purpose of facilitating customer interactions and assuring appropriate resources are available and applied to meet customer needs.

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, 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: operating standard office equipment using pertinent software applications; planning and managing projects; preparing and maintaining accurate records; organizing, preparing and summarizing data for presentations and reports; and interpreting, explaining and applying appropriate laws, codes, rules, regulations, policies and procedures.

KNOWLEDGE is required to perform basic math, including calculations using fractions, percents, and/or ratios; read technical information, compose a variety of documents, and/or facilitate group discussions; and solve practical problems. Specific knowledge-based competencies required to satisfactorily perform the functions of the job include: activities related to organizing and directing the installation, configuration, maintenance, troubleshooting, diagnosis, and repair of computer hardware, software, peripherals, network, and systems; technical aspects of field of technical support and information technology; ITIL V3 Service Desk 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; and principles of budget preparation and control.

ABILITY is required to schedule activities; gather, collate, and/or classify data; and use basic, job-related equipment. Flexibility is required to work with others in a wide variety of circumstances; work with data utilizing defined and similar processes; and operate equipment using standardized methods. Ability is also required to work with a wide diversity of individuals; work with similar types of data; and utilize job-related equipment. Some problem solving may be required to identify issues and select 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: being attentive to detail; establishing and maintaining effective working relationships; communicating with persons with diverse technical knowledge and skills; maintaining confidentiality; working with frequent interruptions; and working 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: GIAC or CISSP certification in areas of Security or Incident Management is required.

Experience: Candidates must have a minimum of four years experience administering IT security controls and compliance assessments, including supervisory experience. Successful experience in a school environment and experience working in a PeopleSoft environment is highly desirable.

Equivalency: Any combination of education and experience equivalent to four years experience administering IT security controls and compliance assessments, including supervisory experience.

Required Testing	Certificates
N/A	Valid CA Driver's License & Evidence of Insurability GIAC or CISSP certified in areas of Security or Incident Management

Continuing Educ./Training

Maintains Certificates and/or Licenses

Clearances

Criminal Justice Fingerprint/Background Clearance

Tuberculosis Clearance

FLSA State: Exempt

Salary Range: Classified Management, Grade 34

Personnel Commission Approved: June 21, 2017

Revised: 9/2017