SANTA CLARA COUNTY OFFICE OF EDUCATION

CLASS TITLE: MANAGER – SECURITY, NETWORK & SYSTEMS ENGINEERING

BASIC FUNCTION:

Under the direction of the Director III-Information Systems, plans, organizes and directs the activities and operations of the security, network, and systems engineering team in the Information Systems Center (ISC) of the Technology Services Branch (TSB); creates and implements security systems to ensure the integrity of data and communications at the Santa Clara County Office of Education (SCCOE); prepares and maintains the systems and network engineering budget and expenditures; supervises and evaluates the performance of assigned personnel.

REPRESENTATIVE DUTIES:

The following duties are examples of assignments performed by incumbents in this classification. It is not a totally comprehensive list of duties, nor is it restrictive regarding job assignments.

ESSENTIAL DUTIES:

Plans, organizes and directs the activities and operations of the security, network, and systems engineering team of the ISC; conducts meetings to review ongoing issues and projects; works individually or in groups with team members to provide direction, assist with technical issues, facilitate and perform project planning and facilitate customer interactions; develops goals and objectives for the unit and department.

Creates, maintains, and documents the policies, procedures, guidelines and direction for information security to protect SCCOE assets from internal as well as external threats; plans and coordinates implementation of information security policies; develops and implements security solutions to align with SCCOE goals; works with appropriate legal counsel to ensure that security policies align with all applicable regulatory mandates.

Designs and documents system security architecture and develops detailed security designs; engineers, implements and monitors security measures for the protection of computer systems, networks and information; documents standard security operating procedures and protocols.

Monitors systems to safeguard information and technology infrastructure while allowing access to authorized users.

Creates and maintains a detailed security incident response plan; identifies and eliminates security risks and responds to security breaches, providing appropriate and timely updates to the Superintendent, Chief Technology Officer (CTO), other cabinet members, and all affected stakeholders.

Develops a security breach protocol and is responsible for its execution in a breach situation.

Creates and maintains a comprehensive disaster recovery plan, including build-out of disaster recovery infrastructure at colocation facilities as required.

With guidance from the Superintendent, Deputy Superintendent, and CTO, implements and maintains an enterprise information archiving (EIA) solution to manage electronically stored content based on retention policies and regulatory mandates.

Creates and maintains a reference architecture for the systems and network infrastructure of the SCCOE; using the reference architecture as a guide, engineers and implements all local and wide area network systems, server and storage systems, security systems, data center, Internet service, and cloud services required for the operations of the SCCOE, supported school districts and regional agencies.

Monitors the operations of the SCCOE regional data center and ensures that all hosted systems have optimal availability and performance, building out the data center as required to meet expanding needs.

Ensures that the security, network, and systems engineering team has the necessary training and experience to support all critical business system functions, including support for financial, administrative and other information systems that are integral to the business of the SCCOE and its clients.

Directs the operations of data, voice and telecommunications systems; assures the delivery of efficient and effective communications services and accurate call accounting; monitors additions, modifications and major repairs of telecommunication systems.

Attends local, regional, state, and national meetings and conferences as necessary to ensure that SCCOE systems utilize optimal technologies for delivery of economies of scale services to our clients and that all systems are compliant with regulatory mandates.

Supervises and evaluates the performance of assigned staff; interviews and selects employees and recommends transfers, reassignments, terminations and disciplinary actions.

Prepares and maintains a variety of reports, records and files related to assigned personnel and activities; creates and maintains server and network documentation including diagrams, spreadsheets and related documentation; manages maintenance agreements, support contracts and software licensing.

Reviews proposed technology purchases; identifies, evaluates and procures new hardware and software products; identifies necessary components and prepares related purchasing documents.

Provides technical information and assistance to the Director regarding assigned functions; assists in the formulation and development of policies, procedures and programs; participates in long term planning processes for SCCOE network, systems, and security infrastructures.

Communicates with appropriate SCCOE personnel and outside organizations to coordinate activities, resolve issues and conflicts and exchange information; communicates and meets with vendors to evaluate potential acquisitions, identify technology solutions, troubleshoot problems with existing installations and negotiate contracts and purchases.

Operates a computer and assigned software programs; operates other office equipment as assigned.

OTHER DUTIES:
Perform related duties as assigned.

KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:
Networking concepts and technologies including TCP/IP, IPv4, IPv6, DNS, routing protocols, Cisco IOS, Network Address Translation (NAT), Virtual Private Networks (VPN) and others.
Security systems, including next generation firewalls, content filtering, certificate management, public key infrastructure, encryption, intrusion detection systems, anti-virus software, authentication systems, log management, content filtering, best practices and procedures.
IT security standards including National Institute of Standards & Technology Cyber Security Framework (NIST CSF) and ISO/IEC 17024.
Technologies for data loss prevention, endpoint security, email security, network vulnerability scanning, incident management and disk encryption.
Latest security principles, techniques, and protocols.
Vulnerability and penetration tools.
Archival systems for electronic messaging and other electronically stored information (ESI).
Server operating systems and server technologies including Windows and UNIX-based systems, and directory services including Microsoft Active Directory and Group Policy.
E-mail systems including Microsoft Exchange.
Storage and backup concepts and technologies.
Server and system virtualization concepts and technologies, including VMWare, Hyper-V, and Virtual Desktop Infrastructure (VDI).
Budget preparation and control.
Principles and practices of administration, supervision and training.
Record-keeping and report preparation techniques.
Interpersonal skills using tact, patience and courtesy.
Excellent oral and written communication skills.
Technical aspects of field of specialty.

ABILITY TO:
Plan, organize and direct the activities and operations of the security, network, and systems engineering team of the ISC.
Oversee and participate in the planning, design, acquisition, implementation, development and modification of complex computer systems.
Create an organization-wide information security culture whereby the totality of behavior patterns contributes to protection of information of all kinds.
Perform vulnerability scans, configuration audits, and security monitoring.
Train and evaluate the performance of assigned personnel.
Provide consultation to SCCOE personnel and others concerning computer, network, and telecommunication systems equipment and malfunctions.
Plan and organize work.
Meet schedules and timelines.
Work independently with little direction.
Communicate effectively both orally and in writing.
Establish and maintain cooperative and effective working relationships with others.
Maintain records and prepare reports.

EDUCATION AND EXPERIENCE:

Any combination equivalent to: Master's degree in Computer Science or related field and six years of increasingly responsible experience in computer systems engineering, network engineering, and IT security, including at least three years in a supervisory capacity.

LICENSES AND OTHER REQUIREMENTS:

CISSP or NIST Cybersecurity Framework Practitioner certification is preferred.
Valid California driver's license.

WORKING CONDITIONS:

ENVIRONMENT:
Indoor environment.
Driving a vehicle to conduct work.

PHYSICAL DEMANDS:
Dexterity of hands and fingers to operate a computer keyboard.
Hearing and speaking to exchange information.
Seeing to read a variety of materials.
Sitting for extended periods of time.

Approved by the Personnel Commission: November 8, 2017

11/08/17

Jonathan Muñoz
Interim Director – HR/Classified Personnel Services

Date