SACRAMENTO CITY UNIFIED SCHOOL DISTRICT
Position Description

TITLE:	Cyber Security Specialist	**CLASSIFICATION:**	Non-Represented Management, Classified
SERIES:	Specialist III	**FLSA:**	Exempt
JOB CLASS CODE:	9892	**WORK YEAR:**	12 Months
DEPARTMENT:	Technology Services	**SALARY:**	Range 7 Salary Schedule A
REPORTS TO:	Director, Student & Data Systems / Chief Information Officer	**CABINET APPROVAL:**	5-7-2025, 4-19-2024
		HR APPROVAL:	5-8-2025, 9-21-2023
		BOARD APPROVAL:	5-15-2025

BASIC FUNCTION:

Plan, design, implement, monitor, and maintain cyber security programs for the Sacramento City Unified School District; identify and address critical systems and critical digital assets; maintain cyber security attack mitigation and incident response capability; and provide assistance to higher level management staff.
Under the direction of the Chief Information Officer or designee, the position of Cyber Security Engineer is responsible for establishing, coordinating, implementing, and managing the Sacramento City Unified School District's cyber-security strategy program across the organization. The incumbent will develop and implement processes to self-audit IT security systems and identify leading technology to prevent system incursions. The position will work directly with the leadership team to identify, implement, and maintain appropriate technology solutions for all aspects of the organization.

DISTINGUISHING CHARACTERISTICS:

Under specific guidance, the Cyber Security Specialist I functions at the entry-level position and has the most limited scope of any Cyber Security Specialist. The Cyber Security Specialist I is knowledgeable and capable of specific tasks within the cyber security, but is often not able to relate specific tasks into a broader picture of how a sub-area functions.

Under general guidance, the Cyber Security Specialist II functions at the journey-level and provides guidance to the entry-level position. The Cyber Security Specialist II is able to understand major sub-areas of the cyber security and/or environment. Cyber Security Specialists I and II support district security systems.

The Cyber Security Specialist III is the most knowledgeable and the most capable of any of the network specialists, and performs all of the duties of a Network Specialist III in addition to the duties listed below. The Cyber Security Specialist has a scope of knowledge and capability that includes the entire network and its environment. When a Cyber Security Specialist functions in a team lead or project leader capacity, the Cyber Security Specialist III will provide technical guidance to other network specialists.
Classes in this series are used to perform a variety of analytical activities in support of security processing systems. Incumbents develop problem solutions using security technology methods; conduct feasibility studies; assist or act as a project manager over information processing projects; work on analysis and support of district security processing systems; develop information processing standards and procedures.

REPRESENTATIVE DUTIES: (Incumbents may perform any combination of the essential functions shown

below [E]. This position description is not intended to be an exhaustive list of all duties, knowledge, or abilities associated with this classification, but is intended to accurately reflect the principal job elements.)

Develops and maintains centralized security alert logging and reporting systems, implements Data Loss Prevention (DLP) systems. **E**

Coordinates and conducts investigations of security events, responds to emergency cybersecurity situations. E Installs security measures and operating software to protect systems and information infrastructure, including firewalls and data encryption programs. **E**

Resolves detected vulnerabilities to maintain a high security standard. **E**

Monitor hardware, software, network traffic, and security systems and identity, troubleshoot, diagnose, resolve, and report security vulnerabilities and incidents. **E**

Manages various cybersecurity systems and provides guidance to technology staff for the integration of new systems. **E**

Reviews and analyzes system logs, SIEM tools, and network traffic for unusual or suspicious activity, and makes recommendations to restore secure operations. **E**

Reviews, tests, and recommends new security software, tools and/or technologies to determine applicability to SCUSD operations. **E**

Manages maintenance agreements, support contracts and software licensing regarding cybersecurity. **E**

Perform audits, periodic inspections, and penetration testing of district information systems to ensure security measures are functioning and effectively utilized. Work with outside consultants as appropriate on independent security audits. **E**

Develop and maintain incident response plan, and provides post-incident analysis. **E**

Monitor information security trends relevant to SCUSD, keeping management informed about information security-related issues and activities affecting the district. Identifies phishing and social engineering attacks targeting SCUSD and notifies staff of associated security risks; performs vulnerability scans on SCUSD and school district networks. **E**

Compiles and reports metrics and key performance indicators to senior management in all areas of responsibility. **E**

Designs, builds, documents, and implements a system security architecture and standard security operating procedures and protocols. **E**

Collaborates with the Network and Systems staff with the design, implementation, and management of the District's infrastructure and systems, encompassing virtual, physical, and cloud computing, storage, networks, and applications; ensuring secure, highly reliable delivery of services to meet district business requirements. **E**

Serve as Tier III escalation point for varied security, infrastructure and application problems; provide technical guidance to staff and others to resolve issues. **E**

Maintain up-to-date remains up-to-date on current cybersecurity best practices and policies; may work with local, state, and federal agencies related to security incidents technical knowledge by attending educational workshops and trainings, review professional publications, establish personal networks, and participate in professional associations. **E**

Performs related duties as assigned.

TRAINING, EDUCATION, AND EXPERIENCE:

The following combination of education, training, and experience sufficient to perform the representative duties and distinguishing characteristics of the position will be considered:

- A minimum of three years of progressively responsible experience in LAN and WAN networking, systems administration, and application support is required, with at least one year in a cybersecurity-related role.

- Applicants with a bachelor's degree in Computer Science or related field, may substitute this experience for at least two years of industry experience in cybersecurity, information systems, network management, or computer science. Higher education in cybersecurity is preferred.

- Experience shall include a broad range of computer hardware and software competencies, including installation, maintenance, and enhancement of network systems across LANs and WANs, as well as planning, supporting, and managing network infrastructure (firewalls, switches, storage devices, backup and recovery systems, network management tools, and various network protocols).

LICENSES AND OTHER REQUIREMENTS:

Must be available for mandatory overtime during critical times. Alternative work schedules and/or telecommuting may be mandatory to prevent end-user interference. Hold a valid California driver's license and provide proof of insurance.

Desired industry certifications and knowledge:

- Certifications: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), CompTIA Security+, Certified Ethical Hacker (CEH), CompTIA Advanced Security Practitioner (CASP+), GIAC Security Essentials Certification (GSEC)

- Networking: Switches, Routers, Servers, Firewalls, LAN, WAN, TCP/IP, Domain Name System (DNS), Active Directory, Wi-Fi, RADIUS, etc.

KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:

- Technical expertise on LAN, WAN, network operating systems, network cabling topologies, and industry standards and practices.
- Cybersecurity laws, regulations, policies, procedures, and standards.
- Cybersecurity methodologies and technologies.
- Network security and access control systems such as firewalls, endpoint protection systems (antivirus).
- Knowledge and ability to support authentication methods.
- Chromebook, Apple, Windows, and windows Server operating systems Firewall, router and switch configuration.
- Data systems back-up.
-

ABILITY TO:

- Conduct daily cybersecurity operations and services.
- Install, configure, and maintain firewalls and other cybersecurity systems.
- Perform vulnerability scans, configuration audits and security monitoring.
- Investigate suspicious network and user activity; maintain high level of attention to detail; make cybersecurity-related recommendations.
- Learn new hardware and software systems and adapt to changes in technology.
- Perform the basic function of the position.

- Develop network procedures and documentation that others can execute.
- Perform troubleshooting analysis of network infrastructure, servers, workstations, and associated systems.
- Make technical trade-off decisions that consider logistical and operational factors with cost factors and standardization efforts.
- Function in a team environment to balance technical factors with other organizational factors.
- Coordinate with other technical personnel to arrive at optimum solutions.
- Use commonly available office automation tools.
- Be available for mandatory overtime during critical times.
- Work in a manner and at a time so as not to interfere with customer productivity.
- Alternative work schedules and/or telecommuting may be mandatory to prevent end-user interference.
- Lift, move, re-position, and connect light to moderately heavy network and workstation equipment components according to safety regulations.
- Effectively work with program managers and site personnel.
- Maintain confidentiality of information
- Meet state and district standards of professional conduct as outlined in Board Policy.
-

WORKING CONDITIONS:

SAMPLE ENVIRONMENT:
Office and school site environment; drive a vehicle to conduct work; constant interruptions.

SAMPLE PHYSICAL ABILITIES:
Sit for extended periods of time; walk and stand to identify and diagnose networking issues; dexterity of hands and fingers to operate a computer keyboard; reaching overhead, above the shoulders, and horizontally; bend at the waist or crouch to troubleshoot and connect cables; hear and speak to exchange information in person or on the telephone; see to read various documents related to assigned activities; lift, move, re-position, and connect light to moderately heavy network and workstation equipment components; physical, mental and emotional stamina to endure long hours under sometimes stressful conditions.

SAMPLE HAZARDS:
Occasional contact with dissatisfied or abusive individuals; exposure to dust when equipment is installed or moved.