CLASSIFIED

Job Class Description

Equal Employment Opportunity

MADERA UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION
APPROVED MOTION NO.75-2022/23
DOCUMENT NO. 54-2022/23
DATED: 05/17/23

INFORMATION SECURITY ANALYST

DEPARTMENT/SITE: Information Technology and Support Services	**SALARY SCHEDULE:** Classified **SALARY RANGE:** 57 **WORK YEAR:** 261 Days
REPORTS TO: Director of Information Technology and Support Services	**FLSA:** Non-Exempt

PURPOSE STATEMENT:

Under the general direction of the Director of Information Technology or designee, the Information Security Analyst designs, facilitates and maintains network security polices, standards, forms, and procedures to protect District information systems against unauthorized access and attacks in order to ensure a safe and reliable learning and working environment; implements Board-approved Acceptable Use Policies for both student, parent and staff computer and network use; ensures that security policies and configurations are applied and maintained for routers, switches, remote access devices, firewalls, servers, desktops, laptops, and other network devices. The incumbents in this classification provide the school community with a safe and reliable technological environment that supports, facilitates, and promotes student learning.

DISTINGUISHING CHARACTERISTICS

This is the second level in the Information Security Series. The Information Security Analyst is at an advanced level and plans, designs, tests, implements and maintains security infrastructures to ensure the integrity, operation, functionality, reliability and redundancy of all technology-supported networks, servers, systems and data storage/retrieval capability of the District. The Information Security Analyst will provide the day to day work assignments to the Information Security Specialist.

ESSENTIAL FUNCTIONS, DUTIES AND TASKS:

The following alphabetical list of functions, duties and tasks is typical for this classification. Incumbents may not perform all of the listed duties and/or may be required to perform other closely related or department-specific functions, duties and tasks from those set forth below to address business needs and changing business practices.

- Analyzes, recommends, and implements changes to security configurations and executes changes as required.
- Analyzes, recommends, and implements changes to user permissions in District systems and cloud services.
- Assists with the implementation of network equipment as needed, including physical installation of network equipment.
- Configures RADIUS (Remote Authentication Dial-In User Service) and similar systems to facilitate secure network authentication on wireless access points, wired Ethernet connections, web servers, routers, switches, firewalls, as well as other network devices.
- Configures tests, updates, and monitors auditing systems and/or appliances that safeguard and maintain logs of students, teachers, outside contractors, and staff activities.
- Creates complex scripts for the purpose of monitoring systems, diagnostics, problem correction and for

MUSD BOARD APPROVED: DECEMBER 12, 2023
MOTION NO. 58-2023/24
DOCUMENT NO. 202-2023/24

automating routine tasks.

- Designs, configures, tests, updates and monitors auditing systems and/or appliances that safeguard and maintain logs of students, teachers, outside contractors, and staff activities.
- Designs, implements and reports on IT security performance results, audits, recommendations and end-user activity audits.
- Assist with the designs, and implementation, of the identity management systems that integrate with sources of authority systems, LDAP (Lightweight Directory Access Protocol) controls, and email services in relation to information systems security.
- Designs, implements, troubleshoots and maintains identity management systems that integrate with sources of authority systems, LDAP (Lightweight Directory Access Protocol) controls, and email services.
- Designs, tests, implements and maintains a variety of network equipment and configurations including, but not limited to cloud services, enterprise firewalls, content filters, core and edge routers, core and edge switches, wireless access points, network object groups, VoIP equipment, VLAN (virtual area network), NAT (Network Address Translation) addressing rulesets, RADIUS, and other access control lists in relation to network security.
- Develops and implements enforcement policies, procedures and associated plans such as but not limited to system security administration, user system access, disaster recovery, and incident response plans based on industry best practices and recommendations.
- Develops, trains and provides clear direction and guidance to staff and users as required regarding assigned programs and in support of professional learning, including cyber security awareness training.
- Plans, monitors, secures, tests, upgrades and maintains the District's network security infrastructures consisting of elements of networks, desktops, servers, cloud services, and other network-attached devices.
- Prepares written technical documentation, training materials, standards, reports, and other documents as assigned; reviews documents for accuracy and completeness.
- Provides technical assessments of information security alerts, including but not limited to malware analysis, packet-level analysis, and system level forensics analysis.
- Recommends and implements security-related policies for user account creation, user password standards, access control lists, software installation and standards, hardware security standards, and network access to ensure the safety, confidentiality and integrity of District information.
- Recommends, coordinates and implements group policies as applicable to support students, conducts computer forensic investigations on District hardware, software and/or cloud services as needed.
- Recommends email policies to ensure that computers and networks are used appropriately and to protect students and staff from receiving email from unapproved sources.
- Responds to help desk inquiries when required.
- Reviews and audits security policies and procedures to ensure policies are being implemented accordingly.
- Reviews, maintains, and modifies the District's data backup schedules to ensure District resources are properly and safely backed up based on the District's Standard Operating Procedures.
- Serves as project leader to support the effective operation of the department in collaborating with multiple stakeholders throughout the District during large, interdepartmental projects in relation to Information Security.
- Travels to user sites as appropriate to meet the needs of students and staff.
- Utilizes security tools to detect, investigate and defend against information and security incidents targeting the District's IT Systems and data.
- Works additional hours and on extended assignments, including evenings and weekends, to accommodate testing, support, maintenance, and potential call back for emergencies and project deadlines.
- Works with vendors to evaluate solutions to District needs.
- Perform other related duties as assigned for ensuring the efficient and effective functioning of the work unit

MUSD BOARD APPROVED: DECEMBER 12, 2023
MOTION NO. 58-2023/24
DOCUMENT NO. 202-2023/24

and the District.

KNOWLEDGE, SKILLS AND ABILITIES

(At time of application.)

Knowledge of:

- Principals of systems analysis
- MITRE ATT&CK framework techniques or similar frameworks
- Operating systems and scripting languages used by the District
- Enterprise Server environments and personal computers, LAN's (Local Area Networks), WAN's (Wide Area Networks) and convergent technologies, TCP/IP (Transmission Control Protocol/Internet Protocol), UDP (User Datagram Protocol) and ARP (Address Resolution Protocol)
- Layer 2-5 network security protocols
- Security analysis tools and methods
- Network protocol analyzers and packet decoding
- A variety of enterprise class server platforms, to include current Microsoft, Linux, VMWare or Unix variants
- Methods of managing large enterprise network and distributed system environments
- LAN/WAN protocols and topologies
- Network routing and switching technologies (HP and Cisco preferred)
- Firewalls, remote access, QoS (Quality of Service) and traffic management
- Network and server security policy implementation
- Disaster Recovery (DR) projects or maintenance of DR environments
- Layer 2 network technologies including switches, VLANs, QoS, spanning tree/RSTP/MSTP (rapid spanning tree/multiple spanning tree protocol) and 802.1q. Wireless management and related technologies
- Interpersonal skills using tact, patience and courtesy
- RADIUS servers and 802.1x network access protocols
- VoIP/SIP (Session Initiation Protocol) in a production environment
- Correct English usage, grammar, spelling, punctuation and vocabulary
- Oral and written communications skills
- Interpersonal skills using tact, patience and courtesy
- Operation of a computer to enter data, maintain records, and generate reports (proficiency required in Excel)
- Laws, codes, regulations, policies, procedures and best practices applicable to network security

Skills and Abilities to:

- Script in either PowerShell or PHP (Hypertext Preprocessor).
- Effectively utilize computer security monitoring and analysis tools
- Adhere to safety practices
- Operate computer equipment and related peripherals
- Plan and manage projects
- Install and maintain electronic equipment
- Communicate, understand and follow both oral and written directions effectively
- Analyze situations accurately and adopt an effective course of action
- Plan, prioritize and organize work to meet schedules and timelines
- Analyze system requirements and establish system procedures

MUSD BOARD APPROVED: DECEMBER 12, 2023
MOTION NO. 58-2023/24
DOCUMENT NO. 202-2023/24

- Communicate with and understand user needs and systems requirements
- Read, understand, explain and implement technical material from manuals and journals
- Work independently with little direction
- Prepare comprehensive narrative and statistical reports
- Multitask and perform in a fast paced, critical environment
- Initiate and demonstrate flexibility in the prioritization of responsibilities
- Analyze and troubleshoot situations accurately and adopt an effective course of action
- Establish and maintain cooperative and effective working relationships with a diverse range of people
- Communicate using patience and courtesy in a manner that reflects positively on the organization
- Actively participate in meeting District goals and outcomes
- Apply integrity and trust in all situations
- Learn District organization, operations, policies, objectives and goals
- Provide technical guidance and recommendations concerning existing computer security protocols, programs, systems, and possible upgrades
- Demonstrate organizational loyalty and high ethical standards
- Think critically and creatively to assess situations and provide novel solutions
- Analyze situations accurately and adopt effective courses of action
- Communicate effectively and efficiently and understand and appropriately follow oral and written directions
- Work independently and effectively with minimum direction despite many interruptions and under time constraints
- Plan and organize work to meet schedules and deadlines

RESPONSIBILITY

Responsibilities include working under limited supervision following standardized practices and/or methods; leading, guiding, and/or coordinating others; and operating within a defined budget. Utilization of resources from other work units is often required to perform the job's functions. There is a continual opportunity to have some impact on the organization's services.

JOB QUALIFICATIONS / REQUIREMENTS:

(*At time of application and in addition to the Knowledge, Skills and Abilities listed above*.)

EDUCATION REQUIRED:

Bachelor's degree from an accredited college or university with a major in Computer Science, Information Systems, or closely related field. Additional qualifying experience beyond the four (4) years required, may be substituted for the required education on the basis of one year of experience for 24 semester/45 quarter units of coursework; OR; Associates degree from an accredited college or university with a major in Computer Science, Information Systems, or closely related field AND possess an industry cybersecurity certification such as an SCCP (Systems Security Certified Practioner) offered by (ISC)² (International Information Systems Security Certification Consortium) or CompTIA Security+ or similar.

EXPERIENCE REQUIRED:

Four (4) years of professional experience in systems design, development, scripting, network design, administration, and optimization in a large LAN/WAN production environment. At least one (1) year of this experience must have included the primary responsibility for network, server, and systems security similar to those described in the essential functions above.

MUSD BOARD APPROVED: DECEMBER 12, 2023
MOTION NO. 58-2023/24
DOCUMENT NO. 202-2023/24

LICENSE(S) REQUIRED:

- Valid, current California Driver's License to drive to meetings, training sessions, and conferences away from the office such as at school sites.

CERTIFICATIONS AND TESTING REQUIRED:

- Pass the District's applicable proficiency exam for the job class with a satisfactory score.
- After offer of employment, obtain:
    - Criminal Justice and FBI Fingerprint Clearance
    - Negative TB test result plus periodic post-employment retest as required (currently every four years)

WORK ENVIRONMENT/PHYSICAL DEMANDS:

(*Must be performed with or without reasonable accommodations*)

- Work is primarily indoors in an office environment under minimal temperature variations and occasionally requires sitting for extended periods
- Lift and move equipment weighing up to 50 pounds
- Dexterity of hands and fingers to operate a computer keyboard and other office equipment and maintain paper files and documents
- Use hands and fingers to grasp, hold and manipulate objects
- Kneeling, bending at the waist, sitting, squatting, crawling, stretching and reaching overhead, above the shoulders and horizontally to retrieve and store equipment, files and supplies
- Hearing and speaking to exchange information in person or on the telephone
- Visual acuity to see/read documents and computer screen
- Frequent operation of a personal vehicle, and occasionally a District vehicle, to travel within and outside the district for meetings, training sessions and assisting staff at school sites.
- Exposure to intermittent noise and interruptions typical of a school environment
- Potential for contact with blood-borne pathogens and communicable diseases

MUSD BOARD APPROVED: DECEMBER 12, 2023
MOTION NO. 58-2023/24
DOCUMENT NO. 202-2023/24