CLASSIFIED

Job Classification Description

Equal Employment Opportunity

MADERA UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION
APPROVED MOTION NO.76-2022/23
DOCUMENT NO. 55-2022/23
DATED 05/18/23

INFORMATION SECURITY SPECIALIST

DEPARTMENT/SITE: Information Technology & Support Department **REPORTS TO:** Director of Information Technology & Support	**SALARY SCHEDULE:** Classified **SALARY RANGE:** 47 **WORK CALENDAR:** 261 Days **FLSA:** Non-Exempt

PURPOSE STATEMENT:

Under the general direction of the Director of Information Technology & Support. The Information Security Specialist, facilitates and assists in maintaining the 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 students, parents and staff computer and network usage; 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 first level in the Information Security Series. The Information Security Specialist provides professional technical services and intermediate diagnostic response 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 day-to-day work assignments, priorities, and coordination are typically provided by the Information Security Analyst.

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 reconfigurations and assist with executing changes as required.
- Assists the Information Technology Analyst with management of information security projects.
- Assists with designing, implementing and reporting on IT security performance results, audits, recommendations and end-user activity audits.
- Assists with detecting, investigation and defending against information and security incidents targeting the District's IT Systems and data.
- Assists with developing conduction cyber security awareness training for District staff.
- Assists with developing and implementing enforcement policies, procedures and associated plans for system security administration and user system access based on industry best practices and recommendations.
- Assists with the implementation of network equipment as needed, including physical installation of network equipment.
- Assists with the technical assessments of information security alerts, including malware analysis, packet-

MUSD BOARD APPROVED: OCTOBER 24, 2023
MOTION NO. 39-2023/24
DOCUMENT NO. 144-2023/24

level analysis, and system level forensics analysis, technical assessments of information security alerts, including malware analysis, packet-level analysis, and system level forensics analysis.

- Configures RADIUS (Remote Authentication Dial-In User Service) and/or 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.
- Collaborates with a variety of internal and external parties (e.g., district personnel, programmers, programmers' analysts, database administrators, users) for the purpose of providing and/or receiving information and ensuring project success.
- Conducts computer forensic investigations on District hardware, software and/or cloud services as needed.
- Configures tests, updates, and monitors auditing systems and/or appliances that safeguard and maintain logs of students, teachers, outside contractors, and staff activities.
- Implements, troubleshoots, and maintains identity management systems that integrate with sources of authority systems, LDAP (Lightweight Directory Access Protocol) controls, and email services.
- Maintains working knowledge of emerging security alerts, issues threats and trends.
- Monitors, secures tests, evaluates, upgrades, and maintains the District's network security infrastructures consisting of elements of networks, desktops, servers, cloud services, and other network-attached devices, working knowledge of emerging security alerts, issues threats working knowledge of emerging security alerts, issues threats Maintain working knowledge of emerging security alerts, issues threats and trends
- 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.
- Performs regular testing of the District’s backups to ensure properly working backups.
- Prepares written technical documentation, training materials, standards, reports, and other documents as assigned; reviews documents for accuracy and completeness.
- Recommends email policies to ensure that computer and networks are used appropriately and to protect students and staff from receiving email from unapproved sources.
- 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, schedules and applies fixes, security patches, disaster recovery procedures, and any other measures required in order to maintain a healthy security posture and/or address security breach.
- 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.
- Tests, evaluates, 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.
- Trains and provides clear direction and guidance to staff and users as required regarding assigned programs in support of professional learning.
- Travels to user sites as appropriate to meet the needs of student and staff.
- 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 closely with interdepartmental staff to implement security policies and procedures and modifies the Districts data backup schedules to ensure District resources are properly and safely backed up based on District’s Standard Operating Procedures.
- Works with the Information Security Analyst to utilize complex scripts for the purpose of monitoring systems, diagnostics, problem correction and for automating routine tasks.

MUSD BOARD APPROVED: OCTOBER 24, 2023
MOTION NO. 39-2023/24
DOCUMENT NO. 144-2023/24

- Works with vendors to evaluate solutions to District's needs.
- Performs other related duties as assigned for ensuring the efficient and effective functioning of the work unit and the District, including various mandatory District training.

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, LANs (Local Area Networks), WANs (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
- 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, firewall technologies, remote access, ACLs, QoS (Quality of Service) and traffic management and security
- 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 or similar authentication tools
- Correct English usage, grammar, spelling, punctuation, and vocabulary
- Oral and written communications skills
- 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
- 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

MUSD BOARD APPROVED: OCTOBER 24, 2023
MOTION NO. 39-2023/24
DOCUMENT NO. 144-2023/24

- 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. Utilization of resources from other work units may be 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:

Associate's degree in Computer Science or a closely related field from an accredited college or university;
OR, High school diploma with 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+.

EXPERIENCE REQUIRED:

Three (3) years of experience in providing technical support to computer users in a network environment and in the maintenance, operation, and repair of computer systems, networks, and software, at least two of which must have included responsibility as the primary technical support for LAN/WAN systems. Course work in computer science, information security, or a closely related field may be substituted for up to one (1) year of the required experience based on 30 semester/45 quarter units for one year of experience.

LICENSE(S) REQUIRED:

- Valid, current California Driver's License to travel among District departments and sites to provide services as needed.

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)

MUSD BOARD APPROVED: OCTOBER 24, 2023
MOTION NO. 39-2023/24
DOCUMENT NO. 144-2023/24

- Pre-employment physical exam A through District's provider

WORK ENVIRONMENT / PHYSICAL DEMANDS:

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

- Work is primarily indoors in a technical environment under minimal temperature variations and occasionally requires sitting and standing for extended periods
- Lift and move computer equipment and other devices weighing up to 50 pounds
- Reaching overhead, above the shoulders and horizontally
- Kneeling, bending at the waist, sitting, squatting, crawling, stretching and reaching overhead, above the shoulders and horizontally to repair equipment, check wiring, retrieve and store equipment, files, and supplies
- Dexterity of hands and fingers to hold and operate repair tools and parts, use a computer keyboard to enter data, operate other office equipment, and maintain paper files and documents
- Hearing and speaking to exchange information in person or on the telephone
- Visual acuity to see/read documents and computer screen and work on equipment, small parts, and color- coded wires
- 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 and computer server rooms

MUSD BOARD APPROVED: OCTOBER 24, 2023
MOTION NO. 39-2023/24
DOCUMENT NO. 144-2023/24