MODESTO CITY SCHOOLS

PROPOSED

Job Description

JC# 10033

CBYER SECURITY ANALYST

OVERALL RESPONSIBILITY

Under general supervision, coordinate the development, implementation and evaluation of Information and Educational Technology Services (IETS) security standards, best practices, architecture and systems for the district to ensure the integrity and cyber security of the district's IETS infrastructure. Establish systems and procedures to ensure the protection and confidentiality of information assets spanning the entire enterprise system. Utilize expert technical skills and knowledge of enterprise work in networking and systems/servers administration is required.

SPECIFIC RESPONSIBILITIES

1. Provide in-depth level of daily server support and work for such items as active directory management, exchange/user group management, SQL, VMware, Storage systems, backups, cloud security, etc. *E*

2. Provide in-depth level of daily network support and work such items as router/switch/firewall configuration & support, VOIP management, WIFI configuration and management, Radius, etc. *E*

3. Develop and implement security applications, policies, standards and procedures intended to prevent the unauthorized use, disclosure, modification, loss or destruction of data; work with the Network and Systems Specialist and other staff to ensure the integrity and security of the department's IETS infrastructure; review the development, testing and implementation of IETS cyber security products and control techniques in all locations and departments throughout the district. *E*

4. Monitor security systems and identify, troubleshoot, diagnose, resolve and report IETS security problems and incidents; help coordinate and conduct investigations of suspected breaches in IETS security; respond to emergency IETS cyber security situations. *E*

5. Consult with application support and other Information Services staff to ensure production applications meet established IETS cyber security policies and standards; resolve as needed. *E*

6. Promote and coordinate the development of training and education on IETS cyber security and privacy awareness topics for district staff (including IETS staff); develop appropriate security-incident notification procedures for district management. *E*

7. Conduct vulnerability assessments to identify existing or potential electronic data and information system compromises and their sources; coordinate IETS investigative matters with the Human Resources department and appropriate law enforcement agencies as needed. *E*

8. Perform audits and periodic inspections of district information systems to ensure security measures are functioning and effectively utilized and recommend appropriate remedial measures to eliminate or mitigate future system compromises. *E*

9. Review, evaluate and recommend software products related to IETS systems security, such as virus scanning and repair, encryption, firewalls, internet filtering and monitoring, intrusion detection, etc. *E*

10. Assist 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; ensure secure, highly reliable delivery of services to meet business requirements; ensure the core infrastructure is robust, scalable and efficient in supporting district applications and support services, and is in accordance with industry standards and best practices. *E*

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

12. Maintain participation in CA DMV Assessment System/Automatic Pull Program.

13. Effectively communicate and maintain cooperative relationships with those contacted during the course of work.

14. Perform other related duties as assigned.

WORK YEAR

Approved days as specified on the Management Salary Schedule

SALARY

Management Salary Schedule

QUALIFICATIONS

Knowledge/Ability

Minimum Requirements:

Knowledge of current trends and advancements in enterprise-wide technology security management, including IT security risk identification and mitigation for all areas of Cyber Security.
Knowledge of information systems cyber security architecture and compliance.
Knowledge of disaster recovery planning and testing, auditing, risk analysis and business continuity planning.
Knowledge of advanced IT security and IT audit concepts and techniques.
Knowledge of advanced operating system architectures, characteristics, components and commands applicable to enterprise information systems.
Knowledge of enterprise physical and virtual data center infrastructure.
Advanced knowledge of operational knowledge and experience with Networking work, server administration, applications and database administration in a windows server environment.
Knowledge of network architecture principles of network design and integration; practices, tools and techniques of network administration and maintenance.
Knowledge of security technologies such as firewalls, intrusion detection and intrusion prevention.
Knowledge of principles and concepts of establishing and documenting baseline systems performance.
Knowledge of principles and practices of backup and disaster-recovery design and planning.
Ability to conduct timely investigations and responses to computer security-related incidents and threats including viruses, worms and other system compromises.
Ability to ensure compliance with all federal, state and local legislation related to information security.
Ability to provide comprehensive information security awareness and training.
Ability to assist with investigations initiated by internal and external authorities.
Ability to understand and implement complex oral and written directions given in English.
Ability to independently compose clear, complete and concise correspondence and reports.

QUALIFICATIONS (continued)

Knowledge/Ability

Minimum Requirements:

- Ability to monitor and identify any anomalous traffic and compromised systems on campus networks.
- Ability to work with a minimum of supervision.
- Knowledge of the CI (Confidentiality, Integrity, Authenticity) Triad Foundation
- Knowledge of security frameworks, e.g. NIST-800-53 or CIS Controls
- Ability to utilize security tools such as Nessus, OpenVAS, and Kali Linux to identify and remediate security related issues.
- Knowledge of and ability to support authentication methods such as multi-factor authentication, federation services, RADIUS, RADIUS, or 802.1x.
- Knowledge of both wireless and wired security best practices.
- Ability to perform all levels of daily work related to systems, networks and their daily operations (i.e., administration, troubleshooting, resolving, etc.).

Education

Minimum Requirements:

- High School diploma or General Education Development (GED) Certificate or California High School Proficiency Examination (CHSPE) Certificate.
- Successful completion of a fundamental computer literacy course.
- Successful completion of an accredited repair course.

Desirable Qualifications:

- Bachelor's degree and certifications highly desirable (i.e., Cisco Certified Network Professional (CCNP) Certificate or equivalent; Palo Alto Certified Network Security Administrator (PCNSA) Certificate or equivalent; Certified Information Systems Security Professional (CISSP) Certificate

Experience

Minimum Requirement:

- Five (5) or more years of progressively responsible experience involving all levels of networking (firewalls, WIFI, VOIP, Switched, AD, etc.) Systems administration, and applications support, including all levels of IETS infrastructure systems.

Desirable Qualifications:

- Two or more (2) years experience in IETS security-related work involving risk identification and mitigation, security architecture development and compliance and problem resolutions.

License(s)/Certificate(s)/Permit(s)

Valid California Driver's License

Must provide a DMV printout within five (5) work days of offer of employment.

Physical Requirements

With or without the use of aids:

- Sufficient vision to read small print.
- Sufficient depth perception to work on computers and related equipment.
- Sufficient hearing to hear normal and telephone conversations.

CYBER SECURITY ANALYST

QUALIFICATIONS (continued)

Physical Requirements

With or without the use of aids:

Ability to speak in an understandable voice and with sufficient volume to be heard at a normal conversation distance and on the telephone.
Sufficient dexterity to manipulate small objects, print or write legibly, or use a computer.
Sufficient physical ability to sit or stand for prolonged periods of time.
Sufficient physical ability to reach horizontally and vertically with arms.

REPORTS TO:

Chief Technology Officer, Information and Educational Technology Services or designee

Cabinet Approved: 2/11/20
Board Approved: