CCSD
CLARK COUNTY
SCHOOL DISTRICT

Senior Information Technology and Security Manager

Position Details

Class Code: 1436
Job Family: Information Systems
Classification: Support Professional
Terms of Employment: Pay Grade 65 on the Support Professional Salary Schedule
FLSA STATUS: NON-EXEMPT

Position Summary

Under general direction, responsible for the operation, maintenance, and planning of the Clark County School District's Information and Technology Security infrastructure including networks, Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS), firewalls, advanced threat detection, and attack mitigation techniques. Interprets national and global threat analysis communications and assists in developing the District's security posture.

Essential Duties and Responsibilities

This list of Essential Duties and Responsibilities is not exhaustive and may be supplemented.

1. Serves as the District's alternate Chief Information Security Officer.
2. Assists security administrators in planning and architecting security infrastructure.
3. Operates, maintains, and repairs equipment, firewalls, domain name systems (DNS), security information and event management (SIEM) logging servers, computer systems, and integrated servers/software platforms.
4. Participates in the development of equipment and operating software security specifications for new systems across the District.

5. Assists in planning and implementing computer hardware and system software installation/upgrades.
6. Assists in diagnosing computer system malfunctions and coordinating/implementing repairs.
7. Assists in preparing, monitoring, and managing the department budget.
8. Represents the District at meetings with local, state, regional, and federal agencies to gather and discuss security landscape and threats.
9. Assists in developing software and hardware disaster recovery plans for wide area network (WAN), local area network (LAN), and computer systems.
10. Supervises maintenance, updates, and patching of security infrastructure by District or contracted staff.
11. Supervises and assists in the installation, repair, and operation of security hardware components by District or contracted staff.
12. Monitors and prepares required reports throughout project implementation to ensure compliance with the United States Computer Emergency Readiness Team (US-CERT) directives, alerts, and advisories.
13. Researches and directs research of equipment needs pertinent to ensuring a sustainable security infrastructure.
14. Researches, evaluates, designs, and recommends acquisition of new and emerging technology to assist in security threat mitigation.
15. Assists in development and final submission of federal grant applications for new, replacement, and upgraded security/network systems and equipment.
16. Attends and directs staff to attend conferences, seminars, and trade shows to maintain awareness of new developments in information and technology security.
17. Prepares required facility and operation reports.
18. Surveys/evaluates network schematics and design to ensure consistent security policies and scanning are implemented Districtwide.
19. Monitors the design, evaluation, and management of security infrastructure engineering/monitoring.
20. Maintains accurate documentation of information required by Children’s Internet Protection Act (CIPA), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), and any other Federal/State guidelines.
21. Operates Security Operations Center; provides tier three and four support for security technology assistance.
22. Prepares work schedules, trains, supervises, and provides input into the evaluation of assigned staff (i.e., Information and Technology Security Manager, Information and Technology Security Technician I, II, & III).
23. Conforms to security standards, as prescribed.

24. Performs other tasks related to the position, as assigned.

Distinguishing Characteristics

Involves development and implementation of computer network security procedures; supervises and participates in analyzing, installing, upgrading, and monitoring security infrastructure including, firewall systems, virtual private network (VPN) systems, content filtering hardware and software, intrusion detection devices, and associated systems.

Knowledge, Skills, and Abilities (Position Expectations

1. Knowledge of project management principles and practices.
2. Knowledge of WAN and LAN technology.
3. Knowledge of Intrusion Prevention and Detection Systems.
4. Knowledge of microcomputer operating systems and applications.
5. Knowledge of Layer 7 Firewall Technology.
6. Knowledge of Advanced Threat Protection.
7. Ability to configure object-based firewalls.
8. Ability to read schematics.
9. Ability to read, interpret, and apply US-CERT alerts and advisory information to systems.
10. Ability to analyze electronic data process (EDP) systems specifications for all computer systems.
11. Ability to operate and maintain security hardware and software from multiple vendors.
12. Ability to interpret financial and budgetary issues.
13. Ability to prepare and write grants.
14. Ability to work cooperatively with employees, other agencies, vendors, and the public.
15. Ability to recognize and report hazards and apply safe work methods.
16. Possess physical and mental stamina commensurate with the responsibilities of the position.

Position Requirements

Education, Training, and Experience

1. High school graduation or other equivalent (i.e., General Educational Development (GED), foreign equivalency, etc.)
2. Three (3) years of college courses in computer science or information security from an accredited college or university; and, Five (5) years of experience supporting/operating telecommunications and networking security, application and systems security, application development security, user authentication and authorization management, information systems vulnerability assessment, and physical data security, with supervision of technical staff; or
   A total of ten (10) years of experience, as outlined above.

Licenses and Certifications

1. A valid driver's license or state-issued identification card.
2. Certified Information Systems Security Professional (CISSP) certification. If certification is not in possession at time of application, it must be obtained within six (6) months of hire date.

Preferred Qualifications

Bachelor's degree in computer science or information security.

Document(s) Required at Time of Application

1. Copy of a valid driver's license or state-issued identification card.
2. High school transcripts or other equivalent (i.e., GED, foreign equivalency, etc.)
3. College transcript(s), if applicable.
4. Copy of CISSP certification, if applicable.
5. Specific documented evidence of training and experience to satisfy qualifications.

Examples of Assigned Work Areas

Central Information Systems Department, and travel to and from schools and other District office settings.

Work Environment

Strength

Medium/heavy - exert force of 50-100 lbs., occasionally; 25-50 lbs., frequently; or 10-20 lbs., constantly.

Physical Demand

Frequent sitting, standing, walking, pushing, pulling, stopping, kneeling, climbing, crouching, reaching, handling, and repetitive fine motor activities. Mobility to work in a typical office setting and use standard office equipment. Stamina to remain seated and maintain concentration for an extended period of time. Hearing and speech to communicate in person, via video conference and computers, or over the telephone. Vision: Frequent near and far acuity, and color vision. Vision to read printed and online materials, a Video Display Terminal (VDT) screen, or other monitoring devices.

Environmental Conditions

Climate-controlled office setting with temperatures ranging from mild/moderate to extreme cold/heat. Exposure to noise levels ranging from moderate to loud for occasional to frequent time periods.

Hazards

Furniture, office equipment, communicable diseases, chemicals and fumes (as related to specific assignment), and power/hand-operated equipment and machinery (as related to specific assignment).

Examples of Equipment/Supplies Used to Perform Tasks

Various computers, printers, modems, telephones, fax machines, copy machines, digital multi-meters, data system and communication test equipment, hand and power tools, etc.

AA/EOE Statement

The Clark County School District is proud to be an equal opportunity employer. The Clark County School District is committed to providing all applicants and employees equal employment opportunities without regard to race, color, religion, sex, gender identity or expression, sexual orientation, national origin, genetics, disability, age, military status, or other characteristics protected by applicable law. Here at Clark County School District, we are a diverse group of people who honor the differences that drive innovative solutions to meet the needs of our students and employees. We believe that through a culture of inclusivity, we have the power to reflect the community we serve.

Job Revision Information

- Revised: 05/25/23
- Created: 12/02/14