CLARK COUNTY SCHOOL DISTRICT
HUMAN RESOURCES DIVISION

SENIOR INFORMATION AND TECHNOLOGY SECURITY MANAGER
Class Code: 1436
Job Family: Information Systems
Classification: Support Staff
Terms of Employment: Pay Grade 65 on the Support Staff 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 District security posture.

ESSENTIAL DUTIES AND RESPONSIBILITIES:
This list of Essential Duties and Responsibilities is not exhaustive and may be supplemented.
1. Serves as alternate Chief Information Security Officer of Clark County School District.
2. Assists the security Administrators in planning and architecting a security infrastructure.
3. Performs operations, maintenance, and repair of 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 the planning and implementation of computer hardware and system software installation and upgrades.
6. Assists in diagnosing computer system malfunctions, coordinating and implementing repair activities.
7. Assists in the preparation, monitoring, and managing of technical department budget.
8. Represents the District at meetings with the local, state, regional, and federal agencies to gather and discuss security landscape and threats.
9. Assists in the development of software and hardware disaster recovery plans for wide area network (WAN), local area network (LAN), and microcomputers computer systems.
10. Supervises the maintenance, updates and patching of all security infrastructure districtwide by District or contracted staff.
11. Supervises and assists in the installation, repair, and operation of all security hardware components by District or contracted staff.
12. Monitors and prepares required reports throughout implementation of projects to ensure compliance with the United States Computer Emergency Readiness Team (US-CERT) directives, alerts, and advisories.
13. Researches and directs the research of equipment needs pertinent to ensuring a sustainable security infrastructure.
14. Researches, evaluates, designs, and recommends acquisition of new and emerging technology hardware and software to be used to assist in security threat mitigation.
15. Assists in the development and final submittal of federal grant applications for new, replacement, and upgraded security and network systems and equipment.
16. Attends and directs staff to attend conferences, seminars, and trade shows to keep abreast of changing technologies in information and technology security.
17. Prepares required facility and operation reports.
18. Surveys and evaluates network schematics and design to ensure consistent security policies and scanning are done districtwide.
19. Monitors the design, evaluation, and management of the engineering and monitoring of the security infrastructure.
20. Maintains accurate documentation of information required by Children’s Internet Protection Act (CIPA), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights andPrivacy Act (FERPA) and any other Federal/State guidelines.
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 the analysis, installation, upgrading, and monitoring of the 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 local and wide area computer network technology.
4. Knowledge of microcomputer operating systems and applications.
5. Knowledge of Layer 7 Firewall Technology.
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 budget 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 experience in support and operation of 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
3. A total of ten (10) years experience, as outlined above, will fulfill the college and experience requirement.

Licenses and Certificates:
1. 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.
2. A valid driver’s license that allows the applicant/employee to legally operate a motor vehicle in Nevada. License must be maintained for the duration of the assignment.
3. Copy of current driving history issued by the Department of Motor Vehicles at time of application or Qualified Selection Pool (QSP) placement and at time of interview prior to final selection.

12/02/14
Preferred Qualifications:
   BS/BA degree in computer science or information security.

DOCUMENT(S) REQUIRED AT TIME OF APPLICATION:
1. High school graduation or other equivalent (i.e., GED, foreign equivalency, etc.).
2. College transcript(s), if applicable.
3. Copy of CISSP certification, if in possession at time of applicant.
4. A valid driver’s license that allows the applicant/employee to legally operate a motor vehicle in Nevada.
5. Copy of current driving history issued by the Department of Motor Vehicles.
6. Specific documented evidence of training and experience to satisfy qualifications.

EXAMPLES OF ASSIGNED WORK AREAS:
Clark County School District Central Information Systems Department, and travel to and from schools and other District office settings.

WORK ENVIRONMENT:
Strength: Medium/heavy - Exert force 50-100 lbs., occasionally; 25-50 lbs., frequently; or 10-20 lbs., constantly.

Physical Demands: 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.

AN AFFIRMATIVE ACTION/EQUAL OPPORTUNITY EMPLOYER

This employer does not knowingly discriminate on the basis of race, color, religion, sex, sexual orientation, gender identity or expression, age, disability, or national origin.