LOS ALAMITOS UNIFIED SCHOOL DISTRICT
Office of the Personnel Commission

CLASS TITLE: Network Security Analyst

BASIC FUNCTION:

Under the direction of the Director of Information Technology, performs specialized duties in the design, installation, configuration, and operation of the enterprise-wide network and cyber security solutions to protect all physical and digital assets; monitors, troubleshoots, and responds to incidents of hardware and software related to network infrastructure (NGFW, WLAN, WAN, LAN, and VoIP), cyber security solutions, and end-point client protection systems; participates in advanced technical support and documentation of network equipment, data center systems, on-premise/cloud solutions, and backups; provides lead technical support to other technology staff; and provides customer service support to all staff members.

REPRESENTATIVE DUTIES:

1. Perform a variety of specialized duties in the installation, configuration, maintenance and operation of the District's cyber-security prevention, on-premise and cloud network, firewalls, wide area and local area networks, voice-over-IP, wireless local area network, video surveillance, access control permission, and related equipment; assure compliance with applicable laws, codes, rules and regulations.
2. Assist in a coordinated response to cyber-attacks; identify threats and develop suitable defense measures; respond immediately to emergencies; evaluate system changes for security implications, and recommend enhancements.
3. Install and maintain next generation firewalls, routers, switches, servers/virtual-servers, e-mail systems, identity directory services, VoIP and unified communications, databases, storage solutions, disaster recovery sites, and backup solutions.
4. Assess and implement 24/7 monitoring and security alerting tools including aggregation of system logs regarding network infrastructure and software services.
5. Investigate, assess, and document daily cybersecurity events and incidents. Report findings immediately to supervisor.
6. Create and prepare regular reports to document and process implementation, improvements made, and potential security breaches that may cause damage District assets. Create and document practices and procedures to address cyber security issues.
7. Run vulnerability, risk, and penetration assessment tests of District’s hardware, software, and cloud solutions that are aligned to industry security framework standards (i.e. CIS, NIST, ISO, etc.).
8. Work in collaboration with county specialists in cyber security and information technology departments, District consulting partners, and immediate supervisor to implement security and network best-practices.
9. Maintains effective communication with administrators, support staff, end users, and technology partners.
10. Transports small equipment to and from various district locations.
11. Train and assist district staff on cyber security prevention, software applications, hardware systems, and cloud solutions to support district-wide instructional and business operations.
12. Perform related duties as assigned.

KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:

- Information technology security standards and requirements, LAN/WAN, operating systems, VoIP and unified communications, cloud services, and data center solutions.
- Design, development, and implementation of security solutions for complex and large networks.
- Firewalls, intrusion detection and prevention systems, end-point protection, MDR, auditing and scanning systems, VPN, and remote access systems.
- Vulnerability assessment tools including but not limited to Nessus, Metasploit, Nmap, Kali Linux Toolsets. Specific security issues associated with common operating systems, networking, server/storage, and virtualization software.
- Risk and threat assessment processes and practices.
- Malware including computer viruses, worms, trojan horses, spyware, and ransomware; phishing and other social engineering strategies.
- Concepts, procedures, and controls relating to CIS, ISO, NIST, and other industry accepted Information Security Frameworks.
- Core security tools including, but not limited to, intrusion detection systems, security information and event management, firewalls, and vulnerability assessment tools.
- State, federal, and local laws and regulations related to cybersecurity, data privacy and protection, and data breach notification, including COPPA, FERPA, HIPAA, CSDPA.
- Principles, practices, and techniques of database structures and computer programming.
- Change control and incident response concepts and procedures.
- Project management concepts and terminology. Manage multiple competing priorities efficiently and effectively.
- Analyze problems, identify alternative solutions, project consequences of proposed actions, and implement recommendations in support of goals
- Proper English usage including grammar, spelling, punctuation and sentence structure.
- Interpersonal skills using tact, patience, and courtesy

ABILITY TO:

- Maintain awareness and knowledge of contemporary standards, practices, procedures, and methods related to cybersecurity.
- Understand and apply laws, regulations, policies, and procedures pertinent to cybersecurity incidents for educational institutions.
- Perform enterprise security analyses, including threat modeling, specifications, implementation, testing, and vulnerability assessment.
- Organize, coordinate, and document technical vulnerability assessments, including systems and network vulnerability assessments, penetration testing, web application assessments, social engineering assessments, physical security assessments, and wireless security assessments.
- Quickly respond to, diagnose, and resolve security breaches. Clearly explain to management and show forensically how an attack was conducted or how a security breach occurred, and what steps should be taken to reduce the likelihood of similar events in the future.
- Interpret technical procedures and documentation, and explain technical concepts in non-technical terms to team members, administrators, and staff.
- Design and configure complex network and software solutions to support infrastructure, voice systems, data center solutions, and WAN/LAN solutions.

- Install, test and maintain network security solutions, network infrastructure hardware, and software applications related to instructional and business operations.
- Maintain current knowledge of technological advances in security, complex networks, and cloud solutions, and related fields.
- Perform complex problem solving as well as critical thinking, using logic and reasoning to identify strengths and weaknesses to solutions and approaches.
- Work with management, administrators, and other team members to solve complex challenges.
- Communicate effectively in both oral and written form

EDUCATION AND EXPERIENCE:

Any combination equivalent to: A Bachelor's degree from an accredited four-year institution in information technology, computer science, or another technology related field; **and** five years of progressive responsible experience in cyber security administration, network technician/analyst, and systems administration. One or more years of network security support experience. Industry certifications (i.e. Cisco, Palo Alto, Security+, CySA+, CISSP, CISA/M, etc.) highly desirable.

LICENSES AND OTHER REQUIREMENT:
Possess and maintain a valid California Driver's License (Class "C" minimum) and remain insurable at the standard insurance rate.

PHYSICAL DEMANDS:
The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of the job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essentialfunctions.

While performing the duties of this job, employees are regularly required to bend, stoop, push, pull, grasp, squat, twist, kneel, walk, sit, and reach to access materials or equipment and complete other tasks as assigned; lift and/or move up to 50 pounds; and lift up to 75 pounds with assistance from ground, waist, chest, shoulder, and above shoulder level.

WORKING CONDITIONS:
The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job in the office and field. Driving to various locations is required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee occasionally works near moving mechanical parts and is occasionally exposed to fumes or airborne particles and vibration. Employee will occasionally work in small and confined environments and can also be subject to dust, heat, and cold working conditions. Also, the employee occasionally works in outside weather conditions.

The noise level in the work environment is usually moderate.

SALARY RANGE: 106

ADOPTED BY PERSONNEL COMMISSION: May 11, 2022
ADOPTED BY BOARD OF EDUCATION: May 24, 2022