

SENIOR NETWORK ENGINEER

DEFINITION:

Under direction of the Network and Information Technology Manager or designee, the Senior Network Engineer is responsible for designing, implementing, and managing the District's on-premise and cloud-based network infrastructure. The Senior Network Engineer will oversee the secure operation, performance and development of the network and telecommunications infrastructure, and ensure projects and district initiatives are managed according to enterprise information technology and security requirements and standards. This position will oversee all aspects of maintaining and improving security in network design, including establishing and enforcing technology standards, assisting with all levels of network and systems administration, operations support, and critical data and infrastructure.

QUALIFICATIONS:

Experience:

- Minimum five years of network design, administration, and maintenance in a multi-site enterprise network with Cisco and VOIP networking technologies.
- Advanced knowledge of communication routing protocols (OSPF, BGP, MPLS, and TCP/IP)
- In-depth experience with switches, load-balancers, firewall, VPN, and routers.
- Advanced knowledge in network security appliances (Cisco, Palo Alto) and cloud-based security.
- Advanced knowledge of enterprise wireless technology.
- In-depth knowledge of information security policies.
- In-depth experience with Servers, SANS, Access control, and Security Surveillance.

Education:

- Bachelor's degree from an accredited four-year institution in information technology or another technology-related field is preferred.
- Information systems certifications and college-level coursework is desirable.

DISTINGUISHING CHARACTERISTICS:

- Provide in-depth subject matter expertise in designing, implementing, managing, and securing the districts network infrastructure.
- Proactive in identifying, investigating, and resolving issues before they cause an outage event.
- Proficiency with vulnerability scanning solutions.

ESSENTIAL DUTIES AND RESPONSIBILITIES:

Under the direction of the Network and Information Technology Manager or designee, incumbent will:

- Provide design, documentation, and support for all internal network communications systems.
- Assist in conducting the development and implementation of an information security policy, standards, guidelines, and procedures to ensure ongoing maintenance of information security protection.
- Monitor cybersecurity requirements for local area networks (LAN), wide area networks (WANS'), virtual private networks (VPNs), routers, firewalls, and related network devices.
- Perform security assessments of applications and systems using penetration and vulnerability testing and risk analysis.
- Monitor the networks and systems, and telephony devices, ensuring performance, capacity, and security.
- Lead the day-to-day networking tasks to ensure network reliability and availability with limited down time.
- Evaluates the network technology architecture and develops a strategy to keep all systems up to date.
- Provide support, responds to work orders from the users, analyzes and solves reported network problems.
- Provide expert-level support to other engineers and network staff within the team.
- Act as a resource for ETIS system vendors, and other personnel, regarding problem identification and resolution, in all enterprise-wide network technologies.

SENIOR NETWORK ENGINEER

- Coordinate with District and ETIS staff to analyze requirements, recommend effective solutions, and implement appropriate technologies.
- Review architectural drawings and specifications for district projects, along with preparation of specifications.
- Perform other related duties as reasonably assigned.

KNOWLEDGE:

- Microsoft Operating Systems -All desktop and server versions
- Microsoft Azure and Office 365
- SAN/Storage such as Pure Storage, HP
- Data Backup and Recovery, Data Replication,
- Hypervisor technologies (VMWare, Microsoft Hyper-V)
- Networking – WAN/LAN TCP/IP, Routing Protocols, DHCP, VLANS, VPN, DNS, OSPF
- Cisco IP Telephony/Voice over IP (VoIP)
- Firewall Technologies- Palo Alto, Cisco
- Cisco based routing and switching experience
- Routing and Switching: (CCNP/CCNA level)
- Cisco WLC -Wireless LAN controller experience
- Cisco ISE experience (working knowledge)
- Experience with site-to-site VPN, remote access VPN

ABILITIES AND SKILLS:

- Plan, prioritize, and organize work to meet deadlines, schedules, and timelines
- Must be flexible and able to multi-task while responding to changing district demands

PHYSICAL REQUIREMENTS:

Physical abilities include the usual and customary methods of performing the job's functions and require the following physical demands: occasional lifting, carrying, pushing and/or pulling; some climbing and balancing, some stooping, kneeling, crouching; reaching, handling, touching and/or feeling; manual dexterity to operate a telephone and enter data into a computer.

Significant physical abilities include ability to sit at a desk, conference table, or in meetings of various configurations for extended periods of time; see and read, with or without visual aids, laws and codes, rules, policies and other printed matter, computer screens and printouts; hear and understand speech at normal room levels and hear and understand speech on the telephone; speak in audible tones so that others may understand clearly in normal conversations.

WORK ENVIRONMENT:

- The work environment characteristics described are representative of those an employee encounters while performing the essential functions of this job.
- Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.
- The noise level in the work environment is usually moderate.
- Employees in this position will be required to work indoors in a standard office environment and come in direct contact with district staff and the public.