ASSISTANT DIRECTOR SECURITY NETWORK INFRASTRUCTURE

DEFINITION:

Under direction of the Chief Technology Officer, plan, coordinate, and supervise the programming, analysis, development, operations, and technical services functions of the District security and network infrastructure; fully monitoring, integrate, upgrade, maintain and ensure the stability, scalability, and security of the network infrastructure, including but not limited to District business and instructional systems, wired and wireless networks, servers, switches, routers, and related systems; keeping optimal systems operations and performance at maximum efficiency through the proper use of security and infrastructure operating standards; to include researching solutions, documentation, process improvement, and recommending more comprehensive and newly developed security and infrastructure technologies for future consideration and implementation; collaborate with cybersecurity local, state, and federal agencies, and prepare security plans and reports as needed; and principals of effective personnel leadership, management and supervision, maintain and improve District efficiencies through data analytics and security integration for District networks, systems and software; and perform other duties as assigned.

ESSENTIAL DUTIES AND RESPONSIBILITIES:

- Provides leadership in planning, organizing, coordinating, and managing the security and network infrastructure operation functions of the District's business and instructional systems.
- Analyze, prioritize, and assign projects to staff.
- Proven experience in managing and supporting large-scale network infrastructures, preferably in an educational or similar environment.
- In-depth knowledge of network protocols, cybersecurity, network infrastructure architectures, and technologies, including LAN, WAN, routing, switching, wireless, and network security.
- Proficiency in network management and monitoring tools, network performance optimization techniques, and network troubleshooting methodologies.
- Strong understanding of network security principles and best practices, including firewalls, VPNs, intrusion detection/prevention systems (IDS/IPS), and access controls.
- Familiarity with network virtualization, SD-WAN, cloud networking, and emerging network technologies.
- Experience in vendor management, contract negotiation, and procurement processes.
- Excellent leadership and team management skills, with the ability to mentor and guide a technical team.
- Strong analytical and problem-solving abilities to identify and resolve complex network issues.
- Effective communication and interpersonal skills to engage with stakeholders, including non-technical staff and external partners.
- Ability to prioritize tasks, manage multiple projects simultaneously, and meet deadlines in a fast-paced environment.
- Resolve difficult and complex application problems through analysis and effective utilization of technical staff, coordination with other Technology Services staff, and vendors.

- Analyze business and instructional security specifications, research and recommend information and technology security and infrastructure products or services and apply technical principals and concepts to develop secure system solutions.
- Constantly monitor security and infrastructure reporting data, system utilization and performance to ensure accurate security integration and system uptime and performance.
- Supervise and evaluate assigned staff.
- Prepare project plans to include analysis, time, and cost estimates.
- Monitor expenses of projects and ensure the completion is within budget specifications.
- Ensure adequate network assurance and security policies and procedures to secure District systems and data.
- Review procedures and document system security components for use by other department employees.
- Maintain current knowledge of security and network infrastructure trends in TK-12 technology, and methodologies, and attend professional development activities as necessary.

QUALIFICATIONS:

Knowledge of
> Complex enterprise security and network infrastructure design, analysis, integration, and operations to maximize security and system performance; understanding of security and technology integration in support of business and instructional programs, principles and practices of industry standard cybersecurity and infrastructure best practices; corrective action strategies to resolve problems; principles of data security and integrated infrastructure systems; data reporting; modern security and scripting practices and infrastructure administration; and principles of effective personnel management and supervision.

Ability to
> Develop plans for security and network infrastructure systems ; research, project manage, and deploy data and integrated system security; document security and application procedures; solve complex security and network integration problems; analyze and take corrective action to ensure maximum system security and uptime, availability and performance; have thorough knowledge of cybersecurity principles and network infrastructure integration and management practices.

Experience
> Five years of progressive supervisory and management experience with full responsibility for maintaining and ensuring maximum security, network infrastructure operations and integration, systems availability and performance; knowledge to seek and research all applicable security and infrastructure solutions; experience and knowledge of, security and network infrastructure principles and best practices.

Education
Graduation from an accredited university with a bachelor's degree, with specialization in computer science, information security, data analytics, or related field an advanced degree being preferred, or any combination of professional training or technical experience equivalent to a bachelor's degree; a demonstrated experience in security, network infrastructure operations, data analysis, data integration, system monitoring and alerting, with additional coursework in infrastructure, cybersecurity and information assurance. Relevant certifications including but not limited to a Certified Network Professional "CNP", Information Technology Infrastructure Library "ITIL", Certified Information Security Manager "CISM", CIS Critical Security Controls "CSC".

Physical Performance Requirements
Considerable standing, walking, or sitting much of the time with some bending, stooping, squatting and twisting. Lifting often involved. Weight of materials will vary, with employees regularly lifting and maneuvering 20 to 30 pounds.

Licenses
Possession of valid and appropriate California Driver's License.

Board Approved: August 3, 2023