POPE COUNTY
MINNESOTA

Senior Systems Engineer
Job Description

Title: Senior Systems & Network Design Engineer **FLSA Status: Exempt**

Department: Information Technology **Updated: 03/2023**

General Definition of Work

Performs difficult work under the limited direction of the IT Director. Plans, researches, designs, installs, implements, trains, documents, and maintains technology related projects and enhancements supporting the County's overall business process throughout the project lifecycle. This includes robust organizational wide area networks (WAN), local area networks (LAN), and wireless local area networks, and involves the development of computer operations, systems/data integrity, and monitoring techniques, identifying and resolving intermediate and complex computer, network, and systems issues; configuration of back up systems, implementation, and disaster recovery mechanisms; maintenance of technical manuals, licensing compliance, network diagrams; management of security systems, policies, and best practices; communication and delegation of tasks, training and communicating with all Administration, staff, and third party agencies.

Supervision is exercised over department personnel.

Essential Functions

To perform this job successfully, an individual must be able to perform each essential function satisfactorily. The requirements listed below are representative of the knowledge, skill, and/or ability required. Reasonable accommodations may be made to enable an individual with disabilities to perform the essential functions.

- **Documentation** – Provides end users and Information Technology staff with up-to-date policies, procedures, and other information related to current active projects. • Communicates with staff, end users, contracted agencies, and vendors via phone, email, and inperson. • Accurately documents all changes, adds, removals of updates, networks, systems, hardware, and software. • Creates training materials and hosts training seminars for technology that Information Technology has implemented, the technology has changed significantly, where changes required by statute dictate changes to the technology, or when the department feels it is necessary for the education of staff or partner agencies. • Frequently communicates with officials of all levels on matters requiring cooperation, explanation and persuasion, or work requiring enforcement of laws, ordinances, policies, or procedures, including but not limited to: County Commissioners, County Administrator, County Sheriff, County Recorder, County Auditor, County Attorney, County Assessor, support agents, all tiers of technical support, engineers, developers, advisors, executives, team leads, applications development, Security Operations Centers, network designers, security analysts, network engineers, voice application engineers, hardware engineers, project managers, regional sales managers, system engineers. • Has major individual impact and must be accountable for end results affecting the entire organization, community, and partners.
- **Security** – Monitors real-world threats against organizational adopted technologies and develops strategies to mitigate vulnerabilities. Researches common threat vectors made available by U.S. security organizations such as MS-ISAC, FBI, CISA, BCA, peer forums, and other reputable

online sources to stay up-to-date on current threats. • Attends and participates in security training and awareness seminars regularly and as needed when more serious threats have been identified. • Evaluates, develops, and adopts security policies to align with partners agencies and vendors to ensure both sides are only accessing required resources to perform a function. • Monitors clients, servers, and networks for threats. Responds to and fully evaluates reported threats by users, monitoring tools, and cybersecurity agencies in real-time. • Communicates any confirmed breaches of security to the appropriate agencies/resources such as BCA, FBI, MNIT, and/or appropriate internal personnel. • Educates end users on their role in maintaining a secure enterprise and hosts quarterly security awareness training to reinforce best practices for securing our organization. • Evaluates users' proficiency with technology and security awareness and assigns additional training as needed. • Manages organizational and partner users, including digitally through a directory server and any applications that require rights management and/or network access. • Identifies potential security risks and recommends the correct changes and actions based on current security knowledge and in-place policies. These decisions are often difficult because in order to maintain organizational integrity it often ends up being more work for the end user and the Information Technology staff implementing the changes.

- **Support** – Assists the Information Technology Director in delegating assignments as able in order to deal with all problems in a complex environment and is able to make educated decisions in their absence. • Schedules and performs after hours maintenance to minimize downtime during core business operating hours and is available the next business day morning in the event there are any undocumented issues caused by the changes. • Assists all supported agencies with county provided technology needs and offers guidance on new and existing solutions that align with our organizations technology, security, and policies. • Works with partner agencies and their support to solve complex infrastructure related issues that can greatly affect both agencies. • Works with many different vendor support staff to help assist in problem solving issues related to proprietary solutions adopted by individual departments.
- **Infrastructure** – Designs and maintains secure networks with the least privileged approach to host connections to the internet, partner agencies, vendors, local network segments, wireless networks, servers, client devices such as computers, phones, printers, and any other technologies in place throughout the organization. • Researches, evaluates, implements, and monitors intermediary security appliances and creates policies to ensure systems and networks are protected. • Manages all wide-area-network (WAN) connections, redundant connections, wireless technologies, printers, phones, network segmentations, security systems, and email infrastructure. • Performs critical infrastructure upgrades, patches, changes as needed. Many times, these are performed after hours and on weekends to prevent exploits and downtime for the organization and partners. • Performs well under pressure and can establish baselines for problem solving during a crisis. This is a critical skill for this position because any outages/downtime can directly affect the entire organization and can reflect poorly on the department. • Manages a high-end, cutting-edge infrastructure while maintaining a 99.999% uptime. This includes but is not limited to physical servers, hypervisors, storage devices, networking equipment, security appliances, backup devices, and email systems.
- **Disaster Recovery** – Evaluates, designs, implements, and supports multiple backup systems to ensure the integrity of all county, partner agencies, and hosted data. • Monitors all backup jobs daily to validate success and processing times. • Maintains a complete plan of action for "best-case" "worse-case" disaster recovery scenarios based off backup and retention policies. • Hosts department disaster recovery scenarios annually to prepare for real-world outages. • Plans, documents, and practices disaster recovery scenarios in a controlled environment.

- **Research and Development** – Communicate with clients regarding technologies, their needs and desires then build a plan of action to design a technology filled solution. These projects can be built on current adopted technologies or may require researching solutions to fulfill the clients needs. The goal is to provide the requestee with a simple, cost-effective solution that will meet their needs without consuming their time. A recommendation is given with one or more solutions and the client is allowed to decide how they would like to proceed. Based on their decision a plan is made, software/hardware is purchased (if necessary), and the solution development begins. • Evaluate support requests and user stories on technology and research how to make processes better and easier for end users. Designs networking solutions including researching, planning, testing, gathering, and reviewing feedback, and implementing. • Continued education and training in relevant areas required to enhance adoption of new technologies and build the foundation in which to support them.
- **Data Integrity and Longevity** – Validates the integrity of the data, backup jobs, and copies; evaluates retention policies; monitors backup and replication jobs and processing times for each. • Develops backup procedures, guidelines, documentation in accordance with the organizations backup and retention policies. • Performs user requested data recovery. • Creates circumstantial backups/recovery points prior to any major system changes. • Manages organizational storage systems by monitoring use, documenting changes, loadbalancing based on performance needs, and developing new storage strategies to address the exponential growth of data throughout the organization.
- **Active and Preventive Maintenance** – Schedules upgrades and maintenance with the organization and partner agencies during the least impactful service window. This includes after-hours work and flexible scheduling. • Works with vendors/consultants during and after hours to coordinate maintenance and changes. • Researches, tests, and deploys active security/system patches for clients. • Researches, tests, and deploys active security/system patches for servers, storage, edge equipment, and network/security appliances. • Evaluates resources, including but not limited to servers, systems, applications, and verifies integrity. This includes cleanup, disk management, service validation, network monitoring, reviewing logs, and ensuring the servers/systems/applications are running within the expected parameters.
- **Systems** – Designs and maintains a secure and robust server infrastructure that supports all county and hosted agencies. • Monitors and maintains servers and storage systems to ensure resource availability and that systems are running efficiently. • Tracks storage usage and scales out repositories to ensure adequate disk-space for all systems. • Configures and maintains both physical and virtual server resource allocation, redundancy, load balancing, and failover clustering. • Evaluates current and projected futures needs and performs research to present a plan of action for procurement and implementation of physical and virtual servers, storage systems, maintenance systems, applications, and cloud solutions. • Tracks all system and application licensing to ensure organizational compliance.

Knowledge, Skills and Abilities

Extensive knowledge of information systems including designing, incorporating, documenting, and maintaining a complex, secure, robust organizational network; broad understanding of wide area networks (WAN), local area networks (LAN), and wireless local area networks (WLAN); thorough knowledge of computer operations, systems/data integrity, and monitoring techniques; comprehensive understanding of problem solving intermediate and complex computer, network, and system issues; in-depth knowledge of backup systems, implementation, and disaster recovery techniques to ensure organization cohesiveness; comprehensive knowledge of technical manuals, licensing compliance, network diagrams, administrative guides for software, hardware, programming, and web design; in-depth understanding of security systems and best practices; ability to compute rates, ratios, and percentages; must be able to communicate and delegate tasks effectively while under-pressure both in oral and written formats; ability to establish and maintain symbiotic relationships with administration, staff, third party agencies, and the general public through communications and trainings; extensive understanding of, and the ability to research available software and hardware and their applicability to the organization.

Minimum Qualifications

Associates Degree in a Systems or Network related field and extensive experience, or a combination of equivalent education and experience.

Special Qualifications

Minimum experience of five (5) years working with network, system, and security administration, Cisco CCNA Courses, Web Development/Programming, Network LAN/WAN Infrastructure, GIS and Armer Administration Training (within 6 months).
Background and fingerprint mandatory.
Valid driver's license in the State of Minnesota.

Working Conditions

The characteristics listed below are representative of the physical demands, physical agility, sensory requirements, and environmental exposures required by an individual to successfully perform the essential duties of this position. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential duties.

- Employees sit some of the time but may walk or stand for some periods of time.
- This classification Light involves physical agility requirements such as: climbing, stooping, kneeling, crouching, crawling, reaching, pushing, pulling,
- This classification involves repetitive motions and manual dexterity most of the time.
- Sensory requirements include standard vision requirements; vocal communication is required for expressing ideas by means of the spoken word; and hearing is required to perceive information at normal spoken word levels.

Physical Exertion (Pounds)	
Up to 10	Regular
Up to 25	Frequent
Up to 50	Occasional
Up to 100	Occasional
100 or more	Seldom

Environmental Exposures	
Work near moving mechanical parts	Frequent
Work in high, precarious places	Seldom
Toxic or caustic chemicals	Frequent
Outdoor weather conditions	Frequent
Extreme Cold, non-weather	Seldom
Extreme Heat, non-weather	Occasional
Noise Level	Loud

The duties listed above are intended only as illustrations of the various types of work that may be performed. The omission of specific statements of duties does not exclude them from the position if the work is similar, related, or a logical assignment to the position.