Network Systems Analyst

Pulaski County, Indiana

Department	Information Technology
Reports To	IT Director
FLSA Status	Non-Exempt
Employment Type	Full-Time

Position Summary

The Network Systems Analyst is responsible for the administration, maintenance, security, and optimization of the County's information technology infrastructure. This position supports county departments by managing network operations, servers, storage environments, cybersecurity systems, cloud services, telecommunications, and critical business applications. The Network Systems Analyst ensures reliable and secure access to technology resources while assisting with technology planning, disaster recovery, and strategic initiatives.

Essential Duties and Responsibilities

Network Administration

- Configure, monitor, maintain, and troubleshoot countywide network infrastructure, including switches, routers, firewalls, wireless access points, VPN services, and network security appliances.
- Monitor network performance, availability, and reliability across county facilities.
- Implement network upgrades, improvements, and standardization efforts.
- Maintain network documentation, diagrams, equipment inventories, and configuration records.

Systems Administration

- Install, configure, and maintain physical and virtual servers.
- Manage Windows Server environments, Active Directory, Group Policy, DNS, DHCP, and file services.
- Monitor system performance, storage usage, and capacity needs.
- Perform server patching, routine maintenance, and lifecycle replacement planning.
- Support cloud-hosted services and county business applications.

Cybersecurity

- Implement and maintain cybersecurity controls that protect county systems and data.
- Monitor security alerts, investigate incidents, and coordinate remediation activities.
- Manage endpoint protection, email security, vulnerability remediation, and access controls.
- Assist in developing and maintaining cybersecurity policies, procedures, and user awareness practices.
- Support compliance with state, federal, and CJIS security requirements where applicable.

End User and Department Support

- Provide advanced technical support for county departments and elected offices.
- Troubleshoot network, server, workstation, application, and connectivity issues.
- Coordinate with software vendors, managed service providers, and other technology partners.
- Assist with deployment of new technology solutions, hardware, and applications.
- Serve as an escalation point for complex technical issues.

Backup and Disaster Recovery

- Manage system backup solutions and verify backup completion.
- Conduct recovery testing and assist with disaster recovery exercises.
- Maintain business continuity and technical recovery documentation.
- Ensure critical systems can be restored effectively following outages, cyber incidents, or emergencies.

Project Management and Planning

- Participate in IT infrastructure projects and countywide technology initiatives.
- Research emerging technologies and provide practical recommendations to improve reliability, security, and cost efficiency.
- Assist with budgeting, procurement, license tracking, and technology planning.
- Develop and maintain technical documentation, procedures, and reports.
- Support strategic technology initiatives across county government.

Knowledge, Skills, and Abilities

- Strong knowledge of Windows Server, Microsoft 365, Active Directory, Group Policy, DNS, DHCP, and file services.
- Strong understanding of TCP/IP networking, routing, switching, wireless networks, VPNs, and firewalls.
- Experience with virtualization platforms such as VMware or Hyper-V.
- Experience with backup, disaster recovery, and business continuity practices.
- Ability to diagnose and resolve complex technical issues across network, server, cloud, and endpoint environments.
- Strong documentation, communication, customer service, and vendor management skills.
- Ability to manage multiple priorities, projects, and support requests with limited supervision.
- Ability to work independently and collaboratively with county departments, public safety partners, vendors, and elected officials.

Minimum Qualifications

Education

- Associate's Degree in Information Technology, Computer Science, Network Administration, or a related field required.
- Bachelor's Degree preferred.

Experience

- Three (3) to five (5) years of progressively responsible experience in network administration, systems administration, cybersecurity, or technical infrastructure support.
- Public-sector, county government, law enforcement, court, or public safety technology experience preferred.

Preferred Certifications

- CompTIA Network+
- CompTIA Security+
- Microsoft Certified Professional or Microsoft Azure certification
- Cisco CCNA
- VMware certification or equivalent

Other Requirements

- Valid driver's license.

- Ability to occasionally work outside normal business hours for system maintenance, outages, or emergencies.
- Ability to lift and move technology equipment up to 50 pounds.
- Ability to travel between county facilities as needed.