Title: Senior Infrastructure Administrator

Unit: Supervisory & Professional

Job Code: D1833
Original Date: 11/2025
Last Revision: 11/2025
Staff Type: Classified
FLSA status: Exempt
Salary Range: 08

DEFINITION

Under the direction of the Manager, Network and PC Services, or assigned manager, install, configure and maintain specialized operating systems (such as EXOS, VOSS, and Gaia Linux) and perform senior level network engineering activities; monitor and analyze network traffic; maintain security; resolve complex hardware and software problems; design analyze, and deploy wired and wireless enterprise network infrastructure services; work with vendors; provide technical advice and training.

DISTINGUISHING CHARACTERISTICS

The Senior Infrastructure Administrator is responsible for enterprise infrastructure network analysis, security, technical design, planning, implementation, and the highest level of performance tuning and recovery procedures for mission critical enterprise network infrastructure systems and for serving as a technical expert in enterprise infrastructure network operating systems.

EXAMPLES OF DUTIES

1. Oversee the logical and physical design, implementation and expansion of the enterprise networking infrastructure. Monitor and analyze usage for optimal availability and performance. Maintain cloud-based and on-premises networking control systems. Work closely with external network service providers to coordinate and implement services.

2. Oversee and maintain robust perimeter and edge security systems, including firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS), to protect the district's network infrastructure from potential threats, and other advanced features including but not limited to Site-to-Site VPN tunnels, and managing a firewall DR site.

3. Design and support the enterprise wireless (WIFI) technology infrastructure, including authentication, security, hardware and software maintenance. Monitor and analyze client usage for optimal availability and performance.

4. Manage virtual environments and ensure the smooth operation of virtualized systems, including troubleshooting, upgrading, and scaling virtual infrastructure.

5. Lead the integration, implementation and optimization of hardware and software, including but not limited to servers, storage solutions, load balancer, DNS security, file server management, UPS management, email security, and network security appliances, to support efficient district operations.

6. Manage and optimize enterprise services including but not limited to Microsoft Exchange Unified Messaging platforms, Microsoft Teams, and SharePoint, ensuring email and messaging distribution services are running efficiently, securely, and integrated with cloud-based solutions.

7. Develop, implement and maintain a robust and evolving authentication schema to include Single Sign-On (SSO) for available applications and multi-factor authentication protocols and methods.

8. Lead the configuration, access control and optimization of cloud services, such as Microsoft Azure / Entra to ensure distributed user access, scalability, security, and seamless integration with local systems.

9. Maintain telephony systems, including VoIP and traditional telephony solutions, ensuring high availability and reliability of communication infrastructure across the district.

10. Design and implement comprehensive disaster recovery and business continuity strategies for all network systems.

11. Oversee the configuration, management, and security of remote (work from home) access solutions, ensuring secure and reliable access for faculty and staff.

12. Manage and optimize Storage Area Networks (SAN) to ensure efficient data storage, backup, and disaster recovery capabilities for critical systems.

13. Work with applicable vendors to provide support for hosted enterprise application updates when necessary. These usually involve a complete rebuilding of both hardware and software infrastructure and involve a considerable amount of coordination and planning.

14. Research and development of PowerShell and Python scripting in support of automation and customized reporting initiatives across all integrated systems.

15. Act as the final escalation point for complex Information Technology Services systems technical issues.

16. Perform related duties as assigned.

Knowledge:

- Advanced principles of LAN/WAN architecture.
- Current and emerging technologies relevant to education networks.
- Enterprise and networking infrastructure, analytics, and strategic objectives.
- Enterprise-level telecommunication systems, emergency broadcasting system, automation tools, and monitoring platforms.
- Enterprise-level services and applications including but not limited to Microsoft Entra, servers, virtualized servers, backup, disaster recovery, firewall, load balancer, DNS security, email security, Gaia
- Fabric technologies (SPBM, IS-IS), multi-site networking and cloud-hybrid integration.
- High-availability network design, and disaster recovery planning.
- Industry standards for cybersecurity, compliance, and access control.
- Linux, logging and monitoring, Security Operations Center, and other relevant security services.

Skills and Abilities:

- Audit and analyze existing infrastructure to align with future-proofing goals and cybersecurity needs.
- Deliver executive-level reports, risk assessments, and strategic recommendations.
- Design, implement, and optimize complex, large-scale network systems.
- Develop documentation to guide ongoing network development and maintenance.
- Lead major initiatives, migrations, and upgrades involving multiple departments and stakeholders.
- Mentor campus network staff, developing growth paths and technical competencies.
- PowerShell and Python script development, troubleshooting and implementation for reporting, automation and maintenance.
- Represent the district in high-level technical discussions with external partners, agencies, or vendors.
- Serve as a final escalation point for all enterprise infrastructure and network-related issues; technical, operational, or architectural.

Training and Experience:

Any combination of training and experience equivalent to a bachelor's degree in computer science, Information Systems, or a related field and more than ten (10) years of progressive experience in enterprise infrastructure and networking.

Certifications such as Cisco Certified Network Professional (CCNP), Certified Information Systems Security Professional (CISSP), or equivalent, is highly desirable.

WORKING CONDITIONS

Physical Requirements:

Category II: Lift heavy objects up to 50 lbs. Climbing and manual dexterity required for cabling and installing electronic components.

Environment:

Work environment includes typical computer-related noise levels and paper printing equipment. Potential electrical hazards exist if precautions are not observed. Exposure to computer monitors occurs on a regular basis.