Title: Enterprise Network Specialist III

Unit: Office Technical

Job Code: J1436
Original Date: 11/2025
Last Revision: 11/2025
Staff Type: Classified
FLSA status: Non-exempt
Salary Range: 35

DEFINITION

Enterprise Network Specialists III are experienced professionals with a high degree of technical expertise and innovation in enterprise network design, operations, security and application support. They are responsible for overseeing the district's enterprise network infrastructure and serve as the final point of escalation for all network systems technical support. Individuals in this classification lead major infrastructure initiatives, provide systems subject matter expertise across all technical tiers and play a critical functional role in aligning the district's networking infrastructure environment with long-term educational and operational goals.

DISTINGUISHING CHARACTERISTICS

Employees in this classification are the districtwide networking technical leaders responsible for designing, maintaining, and evolving the enterprise network infrastructure, leading large-scale projects, solving the highest level, complex technical problems.

EXAMPLE OF DUTIES

1. Oversee the logical and physical design, implementation, expansion, and ongoing management of districtwide network infrastructure. Monitor and analyze usage for optimal availability. Maintain centralized cloud and on-premises control systems.

2. Design and support the enterprise wireless technology infrastructure, including authentication, security, hardware and software maintenance. Monitor and analyze usage for optimal availability. Maintain centralized cloud and on-premises control systems.

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

4. Lead the integration, maintenance, and optimization of hardware, including servers, storage solutions, and network optimization appliances, to support district operations.

5. Manage and optimize 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.

6. 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.

7. Lead the administration, access controls and optimization of cloud services, such as Microsoft Azure and Oracle Cloud Infrastructure to ensure distributed user access, scalability, security, and seamless integration with local systems.

8. Manage and maintain telephony systems, including VoIP and traditional telephony solutions, ensuring high availability and reliability of communication infrastructure across the district.

9. Design and implement comprehensive disaster recovery and business continuity strategies for all systems, including remote failover for critical applications.

10. Act as the final escalation point for complex technical issues.

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. Implement and manage emergency location and notification services systems for real-time identification and coordination during emergencies, ensuring district safety protocols are met.

14. 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.

15. Oversee and perform regular operating system updates and patch management for all servers and endpoints, ensuring security patches, software updates, and system optimizations are applied consistently.

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

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

18. Perform related duties as assigned.

DESIRABLE QUALIFICATIONS

Knowledge:

- Advanced principles of LAN/WAN architecture, fabric technologies (SPBM, IS-IS), and multi-site networking.
- Cloud infrastructure knowledge such as Oracle Cloud Infrastructure(OCI) and Microsoft Azure
- Current and emerging technologies relevant to education networks (e.g., SD-WAN, Wi-Fi 6/6E, IPv6, zero-trust frameworks).
- Districtwide infrastructure, governance, and strategic objectives.
- Enterprise-level telecommunication systems, network automation tools, and monitoring platforms.
- High-availability network design, disaster recovery planning, and cloud-hybrid integration.
- Industry standards for cybersecurity, compliance, and access control.
- Knowledge of Microsoft Sql*Servers technology and connectivity

Skills and Abilities:

- Audit and evaluate 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, districtwide 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 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 final escalation point for all 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 networking.
Certifications such as Cisco Certified Network Professional (CCNP), Certified Information Systems Security Professional (CISSP), or equivalent are highly desirable.

WORKING CONDITIONS

Physical Requirements:

Category II: Requires climbing, crawling, and physical dexterity for tasks such as cabling, equipment installation, and lift/carry duties up to 50 lbs.

Environment:

May be assigned to specific sites or departments; may require off-hours work, on-call availability, and travel to nearby facilities. Potential electrical hazards exist if safety procedures are not followed. Work may be performed in server rooms, IDFs, ceilings, or outdoor enclosures.