
IT INFRASTRUCTURE/SECURITY MANAGER

Definition:

Under limited direction, the IT Infrastructure/Security Manager is responsible for all aspects of data network and communications infrastructure utilized by the Sonoma County Office of Education (SCOE) and supported agencies. Fulfilling a senior role within the IT Department, this position will function as a technical, engineering, and operational subject matter expert as it relates to enterprise network and communication technology. This includes participating in project planning, designing, capacity projections, hands-on implementation, complex integration work, security assessment, hardening of configurations, trouble shooting, maintaining, upgrading, and defining policy/procedure for all LAN/WAN infrastructure in use. This includes, but is not limited to, peripheral systems that rely on LAN/WAN architecture such as enterprise telephony needs, wireless networking, and unified communication services.

Distinguishing Characteristics:

This job class exercises responsibility for the integrity, security, reliability and availability of all internal and external network and communication systems as well as all core SCOE data systems. This job class requires specialized knowledge in the areas of telecommunications, server hardware and software as well as voice, video, and data networks. The IT Infrastructure/Security Manager is distinguished from the Network Administrator in that this position is responsible for more complex systems; requiring more knowledge and independent judgment; and is a management level position with supervisory responsibilities.

Supervision Exercised and Received:

Employees in this class receive minimal supervision within a broad framework of policies and procedures, Employees in this class may direct, supervise and formally evaluate the work of others. The incumbent receives direction and training from the Director, Information Technology.

Example of Duties and Responsibilities:

Duties and responsibilities may include, but are not limited to the following:

- Designs and architects complex highly available heterogeneous LAN/MAN/WAN data and communication network infrastructure with dark fiber as well as managed or lit Ethernet service, a variety of data transport media/mediums, a wide range of service providers, diverse interface types, interior gateway protocols, exterior gateway protocols, multiple ingress/egress paths to the Internet, and satellite/branch office connectivity to hundreds of locations;
- Establishes organizational wide standards for products, platforms, software, hardware, or appliance based solutions related to network and communication technologies that are adopted;
- Maintains routers, switches, firewalls, remote VPN connectivity, VoIP/IP telephony technologies, wireless networking, unified communication solutions, and other network appliance offerings;
- Oversees the entire life cycle of technology solutions acquired including budgetary expense planning, product demonstrations, comparative analysis, RFP/RFI requirements/criteria/scoring, cost benefit analysis, annual ongoing maintenance agreements/contracts for daily operation, future expense planning for replacement/refresh, and the final retirement of and/or secure disposal of anything in active production;
- Manages security of Consortium's routers and servers from unauthorized intrusion by either physical or by remote electronic means;
- Performs complex configuration on a variety of devices and/or platforms running Cisco IOS, Juniper JUNOS, Palo Alto Networking, and other similar offerings to ensure proper system operation;
- Analyzes and troubleshoots the network logs and tracks the nature and resolution of problems; monitors usage to ensure security of data and access privileges; monitors data to optimize network performance; and resolves critical network failures;
- Maintains network management tools and/or utilities related to proactive monitoring, reactive notification during outages, historical trending, and capacity utilization;
- Maintains centralized network-based intrusion detection systems (IDS) for security threat management, and fosters security best practices within all areas of direct responsibility;
- Performs in a team role as the foremost expert/resource to accomplish high risk and/or high impact software, hardware, and firmware updates that affect operationally critical services;

- Develops and maintains archiving procedures: researches and evaluates new technologies related to computer networking;
- Produces documentation, diagrams, creates, and maintains both written and electronic repositories of documentation concerning day-to-day network operations and change management to assure consistency in daily operations;
- Monitors the billing for network-related services provided to district customers;
- Participates in community and statewide work groups relevant to his/her areas of expertise; conducts local and regional technical workshops as directed;
- Serves as a primary contact with networking service providers and customers, and plays a key role in negotiating and developing plans for future services; keeps abreast of new hardware or software products for system enhancements;
- Responds to emergencies as needed to assure continuous system operation;
- Performs other related duties.

Employment Standards:

Knowledge of:

- Mastery level routing and switching concepts with detailed knowledge of protocols and/or configuration including but not limited to D/DNS, DHCP, SMTP, IMAP, POP, STP, GVRP, LACP, EIGRP, OSPF, BGP, HSRP, VRRP, VRF, IPv4, IPv6, Multicast communication, the entirety of the TCP/IP specification, and an in-depth understanding of network security and access control best practices;
- Juniper, Cisco, and HP product offerings and platforms specifically JunOS, Juniper's MX line, Juniper's EX line, ASAs, and HP's ZL family of switches;
- Network data communications and computer system diagnostic aids and tools and the ability to isolate and resolve hardware and software problems;
- Server and client virtualization;
- Voice over IP technology;
- Mobile technology and network management;
- Wireless network design, architecture and operations;
- Principles and practices of management and supervision, including employee selection, evaluation, training and development;
- Technical problem solving techniques;
- Wiring specifications and capabilities;
- Modern office practices, procedures, and equipment.

Ability to:

- Diagnose severity of WAN/LAN problems and make repairs with little or no assistance;
- Works collaboratively on sensitive or critical projects and tasks exhibiting complexity or operational risk;
- Develop network performance/security reports including compilation, analysis and interpretation of results;
- Respond promptly to requests of internal and external clients; provide needed information, assistance, and training resources;
- Be flexible, use ingenuity and imagination to solve complex problems, and receptive to change;
- Understand, follow and apply documentation standards and requirements;
- Work under pressure and meet tight deadlines;
- Communicate effectively in oral and written forms in technical and non-technical terms to clients and staff;
- Learn new skills to keep current with technology changes;
- Maintain confidential and sensitive information;
- Work effectively as part of a team devoted to customer service;
- Respond promptly to requests of clients, both inside and outside the County Office and provide needed assistance and support to clients;
- Plan, direct, and organize the work of assigned personnel;
- Provide advisory services to school districts IT departments;
- Think logically and pay close attention to detail;
- Administer day-to-day operation of networks;
- Work with numerous interruptions;
- Plan and organize work to meet priorities and time lines;

- Attend seminar workshops - Specific to knowledge and expertise to keep skills and knowledge current with industry trends;
- Prepare and deliver effective oral presentations;
- Work additional hours during the week and/or weekend infrequently.

Education and Experience:

Experience:

- Minimum of five years' experience of enterprise-level network design, implementation, and management.
- Prior experience maintaining a WAN is highly desirable.
- Experience with or in a Linux/Unix/BSD environment highly desirable.
- Prior networking experience in a schools setting is highly desirable.

Education:

- Bachelor's degree from an accredited college or university in Computer Science, Information Science, or Engineering.
- Experience beyond the minimum requirement may be substituted year-for-year for the minimum educational requirement.

Licenses or Certificates:

- Certifications included but not limited to JNCIE, JNCIS, JNCIP, JNCIA, CCNP, CCDP, CCIE, CWNA are strongly desired.

Physical Demands:

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job.

- Must have normal (20/20) vision, corrected or uncorrected;
- Visual acuity sufficient to work at a computer screen frequently and throughout the day, near and far visual acuity, depth perception, color vision sufficient to recognize people, words, and numbers;
- Frequent standing and walking, and occasional bending, stooping, kneeling;
- Occasional crawling in confined spaces in buildings;
- Lifting up to twenty-five (25) pounds frequently, fifty (50) pounds on an occasional basis, and in excess of fifty (50) pounds with assistance. The heavy objects to be lifted include personal computers, printers, and related equipment;
- Speaking and hearing ability sufficient to hear over phone and carry on routine conversations
- See to read manuals, video display screens, and other related material;
- Drive an automobile and transport equipment and documents;
- Sit for extended periods in a typing position;
- Hand-eye-arm and finger dexterity to use a personal computer keyboard, ten-key, and other common office equipment for long periods of time.

Work Environment:

The following conditions may be present:

- Work is performed in an office and classroom environment with minimal exposure to health and safety considerations.

Other Requirements:

- Must be fingerprinted and a satisfactory Department of Justice records check must be received by SCOE, prior to employment.
- TB testing will be required upon employment.
- Must pass a pre-employment physical (if applicable).
- May be required to obtain first aid and CPR certificates within the first 6-12 months of employment.
- May be required to drive with or without students; some positions may require a current California drivers license, proof of insurance, and possible participation in the DMV Pull Notice Program once employed.