LifeSource ORGAN, EYE AND TISSUE DONATION 2225 West River Road North Minneapolis, MN 55411 1.800.24.SHARE	POSITION DESCRIPTION	
	PD-0092	Rev 4
	Systems Administrator	

DEPARTMENT: Information Services
STATUS: Exempt; Salaried
EXPOSURE RISK: Category III
SALARY GRADE: 22
REPORTS TO: Information Services Manager
SUPERVISES: N/A

GENERAL JOB FUNCTION

The Systems Administrator maintains the environment of desktop hardware, software applications, operating systems and network connectivity as well as engages in supporting cybersecurity efforts. Provides a high level of customer service responding to requests for technical support while ensuring timely resolution. Manages projects involving the design, analysis, maintenance, and implementation of Windows Servers and network applications (Office 365, VM, Antivirus, MDM, Network Monitoring, Customer Relations Management (CRM), backup and recovery, wireless infrastructure, Nutanix). Implementation and administration of network level applications including but not limited to messaging systems, virtual server infrastructure (VM Ware), remote connectivity, DNS, system software reporting and compliance, and database server administration. Ensures detailed documentation for problem resolution and internal system processes following ITIL standards. Aligns daily activities with the strategic and operational goals of the organization.

JOB DUTIES AND RESPONSIBILITIES

Responsible for IS team collaboration in providing helpdesk support for all team members.

1. Actively engages in responding to and effectively resolving helpdesk issues submitted through email, IM, voice or in person.
2. Produces high-quality documentation that meets applicable standards and is appropriate for its intended audience, including maintaining Technical Knowledgebase (TKB)'s Article's.
3. Identifies issue trends and devises preventative solutions.
4. Responds to high priority issues during non-business hours when assigned.
5. Leads Root Cause Analysis (RCA) and ensures communication of report findings is understood by team members.
6. Provides monthly technical support sessions for all team members.
7. Resolves more complex issues and elevates requests when appropriate to vendor support, or manager.

Responsible for end-to-end system administration of all LifeSource Windows Infrastructure.

1. Administers and makes recommendations for VM, database, file storage, backup and recovery, CRM, and Office 365; including associated servers, operating systems, and infrastructure.
2. Updates servers and applications with regularly scheduled patches, including network security operations, including virus scanning, antispam and firewall.
3. Oversees execution of vendor maintenance including, configuration, client server installs, network and VOIP-based telecommunication systems, including moves, additions, and changes.
4. Analyzes and makes recommendations for hardware and software implementation and standardization.
5. Responsible for managing and updating all IS documentation and IS work processes.
6. Oversight, management and execution of timely IS regulatory audits and requirement changes. Specifically, requirements from Centers for Medicaid and Medicare Services (CMS), other agencies and internal policies.
7. Possesses a thorough understanding of the internet and cloud computing including DNS, security, IP routing, http, VPN, email routing, spam and maintain up to date best practices.
8. Oversees vendor maintenance and ensures the quality of all aspects of VOIP phone system, including configuration, patches, disaster recovery\planning and change requests

Engages in partnerships with vendors on network infrastructure management including, LAN/WAN hardware, hubs, bridges and routers.

1. Works with vendors, clients, carriers and technical team members on network implementation, optimization and ongoing management.
2. Administers local telecommunications system through moves, additions, and changes.
3. Assists in the maintenance and testing of network servers and associated equipment.
4. Assists in performing system and data backups and recovery.
5. May assist with evaluation and recommendations for enterprise wide network improvement and upgrades, including trending analysis and capacity planning, LAN/WAN hardware, firewalls, switches and routers.
6. As needed, monitors LAN/WAN availability ensuring client access to limit security threats.

Other responsibilities

1. Engage in cybersecurity incident detection process and response actions.
2. Assist with creating rules for cybersecurity detection responding to and driving the remediation of critical incidents according to standard operating procedures (SOP).
3. Ensure cybersecurity incidents are handled in a manner that is consistent with LifeSource policies.
4. Performs team member orientation and provides ongoing training opportunities.
5. Remains current on industry and technology trends. Reviews corporate needs and makes recommendations to the Information Services Manager.
6. Collaboratively maintains an inventory of organizational hardware and installed software.
7. Provides backup coverage for other information technology positions as needed.
8. Collaborates with other LifeSource team members to ensure best use of resources and technology.
9. Responds to high priority issues during non-business hours when assigned.

STANDARD RESPONSIBILITIES

1. Perform work while demonstrating a commitment to excellence and performance improvement.
2. Update clinical and administrative documentation, including electronic systems, with accurate, real-time, appropriate information according to established practices and procedures.
3. Represent LifeSource in a professional manner with both internal and external customers, ensuring professional appearance and communication.
4. Participate in all appropriate meetings, in-person, on-site, or remote, as defined by leader.
5. Routinely share feedback, solutions and ideas to leadership, including identification of training needs.
6. Exhibit outstanding clinical, customer service and collaboration skills as required by position.
7. Maintain confidentiality and respect of information obtained within purview of position, as defined by policy and procedure expectations and in accordance with HIPAA.
8. Demonstrate LifeSource Values in work behaviors and actions.
9. Actively participate on assigned committees, work groups and project teams.
10. Execute job responsibilities in accordance with established Standard Operating Procedures (SOPs), Policies (POL), and practices as trained.
11. Perform other duties as required and assigned by leader.

QUALIFICATIONS

1. Requires a minimum of 5 years of computer systems and network applications experience and some education in computer science or related field.

2. Relevant Information Services Certification, prefer Windows System Administration or Active Directory Certification, or ability to obtain within 1yr is required. Passing of exams toward certification is strongly preferred. Once certified, you must obtain the required continuing education for recertification credits/process.
3. Demonstrated high level of expertise with Windows Server 2008 to 2019, Nutanix, Active Directory, VMware is required.
4. Experience working with an MDM solution and Antivirus in Enterprise environment is preferred.
5. MSCSE or MCP certification preferred.
6. Strong working knowledge of Microsoft Office including Project and SharePoint.
7. Proven effective at establishing rapport and working relationships with peers, customers and vendors.
8. Must be organized, detail oriented, and have excellent critical thinking and analytical skills.
9. Strong written and verbal communication and collaboration skills are essential
10. Proven ability to reduce technical information into non-technical language.
11. Ability to establish priorities and function independently with a strong initiative.
12. Proven ability to problem-solve effectively and efficiently.
13. Demonstrated ability to exhibit a high degree of quality, integrity, and honor confidentiality of appropriate information including, but not limited to, personal team member data, organizational operations or work processes, donor and donor family information, contributor details, any financial information and medical or protected health information (PHI) in accordance with HIPAA.
14. Proven skilled and competent in using technology-based tools such as personal computers and related software, mobile devices and electronic medical record systems as appropriate for position.

WORKING CONDITIONS

1. Able to work a minimum of 40 hours per week with schedule adjusted to accommodate organizational needs.
2. Engages in regular rotation of on-call Information Services support.
3. Occasional travel may be required. Must maintain a valid driver license and have reliable personal automobile to be used with company reimbursement using IRS guidelines.
4. Affected team member in Category III never or rarely have exposure to bloodborne pathogens and do not have a potential for this exposure or handle materials that could spread infection (less than one opportunity per month). Additionally, they rarely interact with staff in patient or donor areas in a hospital or clinic setting while performing their assigned job duties.
5. Frequently lift objects up to 50 pounds and carry short distances.
6. Must be able to follow and successfully complete category immunization, health screening and background check requirements.

Senior Systems Administrator – Grade 23

ADDITIONAL JOB DUTIES, KNOWLEDGE, SKILLS and ABILITIES

Leads and manages partnerships with vendors clients, carriers and technical team members on network implementation, optimization and ongoing management

1. Manage network infrastructure, LAN/WAN hardware, firewalls, VPN, voice systems and routers.
2. Oversee local telecommunications system through moves, additions, and changes.
3. Monitor LAN/WAN availability ensuring client access to limit security threats.
4. Execute full disaster recovery testing including bringing up processes at an offsite location and failback.
5. Engage in ongoing enterprise wide network improvement and upgrades, including trending analysis and capacity planning.

Leads and manages of cyber security infrastructure including monitoring, threat intelligence, counter measure development (Counter Threat), and incident handling of LifeSource cyber threats.

1. Manage incident detection process and response actions.
2. Analyze security events from various sources and determine if it qualifies as a legitimate security incident.
3. Create rules to enable detection tools to look for an indicator of compromise on assets.
4. Respond to and drive the remediation of critical incidents according to standard operating procedures (SOP).
5. Initiate escalation procedures to counteract potential threats/vulnerabilities.
6. Ensure incidents are handled in a manner that is consistent with LifeSource policies.
7. Perform comprehensive threat intelligence assessments. This may include providing reporting on assessment results as well as risk mitigation and remediation recommendations and plans.
8. Communicate known security risks and solutions to leadership in order to mitigate risks to business and technology partners as needed.

Team Member Statement of Acknowledgement and Understanding

Acknowledgement of this job description is performed electronically via Q-Pulse—the LifeSource document control system. A team member's electronic signature will represent the following statement of understanding:

I acknowledge that I have received and reviewed the job description for my position and I feel that I can meet the requirements with or without reasonable accommodations. I understand that this job description is intended to describe the general content and requirements of the job and that it is not an exhaustive list of all duties, responsibilities and requirements of this position. Additionally, I understand the general description of the expectations related to work hours and absences, attached herein, are subject to change based on department and organizational requirements. I understand that LifeSource has the right to revise this job description at any time.

The following is a general description of the expectations related to work hours and absences. This is subject to change based on department and organizational requirements.

POSITION EXPECTATIONS

Job Title: Systems Administrator
Reports To: Information Services Manager
Exemption Status: Exempt; Salaried

WORK

Work Day: Monday-Friday
Hours: 0800-1700
Lunch/Breaks: Self-directed
Overtime: N/A
On-Call: 1 week after hours call every 3-4 weeks.
Flexible Hours: Yes
Flexible Location: Yes
Weekends: N/A
Travel: Yes—some travel to satellite offices
Mandatory Meetings: Yes—LifeSource team and departmental meetings
Shift Relief: N/A

ABSENCE

Planned Absence *(Vacation, Holiday, Leave of Absence, etc.)*
Short-term: Vacations via HRIS; Team member plans and prioritizes around other team planned absences.
Long-term: Manager or bring in temporary help.
Unplanned Absence *(Injury, Illness, Leave of Absence, etc.)*
Short-term: Usually do not make arrangements; work gets completed when employee returns
Long-term: Manager or bring in temporary help.

COMMENTS