Systems Administrator

higheredjobs.com/search/details.cfm



Position Summary

The Systems Administrator is responsible for maintaining, securing, and optimizing the University's core server and infrastructure environment. This position plays a critical role in ensuring the reliability, availability, and performance of enterprise systems, including authentication, file storage, virtualization, and cloud-based services. The Systems Administrator works closely with network, security, and support teams to deliver stable, scalable, and secure technology services that advance Lincoln University's academic and operational mission.

Key Responsibilities

Systems Management & Administration

- Administer and maintain Windows and Linux server environments, ensuring system reliability, security, and performance.
- Manage Active Directory, DNS, DHCP, Group Policy, and related identity infrastructure services.
- Maintain and monitor virtualized environments (VMware or Hyper-V), including provisioning, snapshots, and backup operations.

- Coordinate patch management, OS upgrades, and system hardening in alignment with University security standards, applying CIS Benchmark controls and NIST SP 800-123 guidance for server hardening.
- Implement and manage monitoring tools to proactively identify and resolve performance issues.
- Administer and support the Unified Endpoint Management (UEM) platform across Windows and mobile (iOS/iPadOS) endpoints, including policy enforcement, device enrollment, compliance reporting, and integration with identity services.

Storage, Backup, and Recovery

- Manage on-premises and cloud-based storage solutions, ensuring data integrity and capacity planning.
- Oversee backup schedules, disaster recovery planning, and restoration testing.
- Collaborate with Security and Compliance teams to maintain data protection and retention standards.

Security & Compliance

- Apply best practices for system hardening, access control, and vulnerability management.
- Monitor logs and alerts for signs of unauthorized access or system compromise.
- Support compliance with institutional, state, and federal security requirements (e.g., FERPA, HIPAA, NIST), and contribute to implementation and maintenance of the University's institutional cybersecurity framework.

Collaboration & Support

- Partner with the Network Administrator and Lead Technology Analyst to ensure cohesive end-to-end service delivery.
- Provide Tier 2 and 3 escalation support for infrastructure-related incidents.
- Participate in cross-departmental projects, contributing technical expertise and systems design insight.
- Document system configurations, procedures, and troubleshooting guides in the internal knowledge base.

Planning & Continuous Improvement

- Participate in capacity and lifecycle planning for servers, storage, and related infrastructure.
- Evaluate new technologies to improve efficiency, security, and reliability.
- Contribute to standardization and automation of recurring administrative tasks using PowerShell or equivalent tools.
- Provide infrastructure input to institutional AI governance initiatives, including system-level evaluation of AI tool deployments, data handling requirements, and compute resource planning in support of the University's AI Governance Council.

Minimum Qualifications

- Bachelor's degree in Computer Science, Information Systems, or a related field, **or** equivalent experience.
- Five (5) years of progressively responsible experience in systems administration or infrastructure support.
- Strong experience with Windows Server and Active Directory management.
- Working knowledge of virtualization (VMware or Hyper-V), storage technologies, and enterprise backup systems.
- Understanding of security fundamentals, including least privilege, Zero-Trust Architecture, network segmentation, and MFA integration.
- Excellent analytical, troubleshooting, and communication skills.

Preferred Qualifications

- Experience in a higher education IT environment.
- Working knowledge of Microsoft 365, Azure AD/Entra ID, and endpoint management platforms, including Microsoft Intune or equivalent UEM solutions.
- Experience with system monitoring tools such as SolarWinds or PRTG.
- Familiarity with scripting and automation (PowerShell, Python, or Bash).
- Relevant certifications (e.g., Microsoft Certified Systems Administrator, CompTIA Server+, or VMware VCP).

Core Competencies

- Technical Expertise and Problem Solving
- Security Awareness and Risk Management
- Collaboration and Teamwork
- Documentation and Knowledge Sharing
- Customer Service and Communication

Lincoln University is an equal opportunity, affirmative action employer.