Posted: August 21, 2026

NEW MEXICO TECH
SCIENCE • ENGINEERING • RESEARCH UNIVERSITY

POSITION ANNOUNCEMENT

TITLE: SENIOR SYSTEM AND NETWORK ADMINISTRATOR II DEPT: ICASA

REG ☑ **TEMP** ☐ **FULL TIME** ☑ **PART TIME** ☐

STARTING RATE or SALARY RANGE $98,500 - $110,000
Employees being promoted to a higher classified position receive the minimum for the position or a pay rate adjustment of 8% whichever is greater.
All regular positions also entitle the employee to several benefits including health, dental, vision, life insurance, and retirement which is largely paid by New Mexico Tech for the employee and dependents.

INTERNAL POSTING THROUGH: Concurrent* CONSIDERATION WILL BE GIVEN FIRST TO TEMPORARY AND REGULAR TECH EMPLOYEES WHO APPLY WITHIN THE 7 DAY INTERNAL POSTING. APPLICATIONS RECEIVED AFTER THE 7 DAY POSTING MARGIN WILL BE CONSIDERED WITH OTHER OUTSIDE APPLICANTS.

JOB SUMMARY:

As a Senior Systems and Network Administrator II, responsible for architecting, administering, and maintaining ICASA's enterprise computing environment, including server, desktop, and laptop systems, as well as the network infrastructure and analytical platforms that support research, development, experimentation, and testing activities across multiple organizations.
This role includes the configuration, installation, testing, monitoring, operation, troubleshooting, and lifecycle maintenance of server hardware and software, endpoint systems, and network infrastructure across both campus and remote sites, including the Playas Research and Training Center (PRTC). Responsible for implementing and maintaining cybersecurity controls in alignment with NIST 800-171, CMMC 2.0, and other customer-specific requirements, ensuring protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), and sustaining NMT's eligibility for Department of War (DoW) programs. Contributes directly to the Institute's overall cybersecurity posture through continuous monitoring, vulnerability management, and risk mitigation. Actively participates in the research, development, and deployment of advanced computing and networking platforms that enable ICASA's technical programs, including support for distributed teams, remote operations, and emerging capabilities in wireless systems and data-driven environments. Collaborates with system administration teams, researchers, and external partners to support multiple concurrent projects, providing technical expertise and operational support to ensure mission success. Receives tasking from team leadership while exercising independent judgment in the execution of complex technical responsibilities.

JOB FUNCTIONS:

Enterprise Infrastructure Management Design, configure, deploy, and maintain enterprise IT infrastructure including user accounts, directory services, network shares, workstations, servers, and network equipment (switches, routers, firewalls). Evaluate and implement secure, robust, and reliable system configurations. Support infrastructure across ICASA and affiliated organizations, including remote environments such as the Playas Research and Training Center (PRTC). Procure, build, install, and lifecycle-manage systems running Windows, Linux (RHEL 7+), and macOS platforms.
Systems Administration, Security & Compliance (CMMC 2.0) Administer and maintain Windows, Linux, and macOS systems ensuring availability, performance, and security. Monitor and remediate vulnerabilities, perform regular patching, and conduct security audits and log analysis. Implement defense-in-depth

strategies and assess system attack surfaces and data exposure risks. Ensure compliance with Cybersecurity Maturity Model Certification (CMMC) 2.0 and Department of War (DoW) requirements, including safeguarding Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Develop, implement, and maintain policies, controls, and technical safeguards necessary to sustain NMT's eligibility for DoW-funded programs.

User Support & Collaboration Provide technical support, training, and guidance to users across multiple organizations (ICASA, Research Compliance, PRTC, MRO-I, and external partners). Troubleshoot hardware/software issues, improve usability, and support deployment of new tools and systems. Collaborate with vendors and technical communities to resolve complex issues.

Backup, Recovery & Continuity Design, implement, test, and maintain backup and disaster recovery strategies using enterprise tools (e.g., Bareos). Ensure data integrity, availability, and recoverability across systems and environments.

Monitoring & Operational Awareness Continuously monitor systems and network performance using tools such as Zabbix. Review logs and audit trails daily, identify anomalies, and take corrective action. Proactively plan and execute administrative improvements based on system performance and security reporting.

Data Systems & DevOps Support Support database development, maintenance, and deployment (primarily PostgreSQL). Assist with containerized environments (Docker/Kubernetes), application updates, and DevOps workflows supporting research and development initiatives.

Research Infrastructure & Remote Operations Support and advance ICASA's research and development activities in areas such as wireless communications, data science, cybersecurity, cloud computing, and emerging technologies. Contribute to the development and operation of research infrastructure at the Playas Research and Training Center and other experimental environments. Collaborate with faculty, researchers, sponsors, and external partners to support technical project execution and innovation initiatives. Research, evaluate, and recommend new technologies, tools, and • Design, deploy, administer, monitor, troubleshoot, and maintain server, workstation, storage, and network infrastructure located in Socorro, Playas, and other ICASA-managed locations. Manage on-premises, cloud, and hybrid computing environments to ensure high availability, reliability, scalability, and performance. Provide remote administration and operational support for ICASA's distributed research and experimentation environments. Support the operation and expansion of ICASA's research testbeds, laboratories, and field experimentation sites, including occasional travel as required. Develop and maintain system architecture, operational standards, and infrastructure lifecycle management processes. Support events being executed in the Cyber Kinetic Environment maintained jointly by ICASA and PRTC Cloud Engineering, Infrastructure Automation Design, build, and maintain secure and scalable cloud infrastructure using Infrastructure as Code (IaC), automation, and orchestration technologies. Develop and maintain automated provisioning, configuration management, deployment, monitoring, and operational workflows. Implement and maintain authentication architectures that provide for various security requirements at ICASA (i.e. CMMC, CJIS, etc.) for desktop and cloud services across macOS, Windows and Linux Collaborate with software developers, system administrators, and researchers to implement modern cloud-native and hybrid computing solutions. Evaluate and integrate emerging technologies that improve infrastructure performance, scalability, and maintainability. Participate in technical planning, architecture reviews, and technology roadmap development

Systems Administration, Security & Compliance (CMMC 2.0) Administer and maintain Windows, Linux, and macOS systems ensuring availability, performance, and security. Monitor and remediate vulnerabilities, perform regular patching, and conduct security audits and log analysis. Implement defense-in-depth strategies and assess system attack surfaces and data exposure risks. Ensure compliance with Cybersecurity Maturity Model Certification (CMMC) 2.0 and Department of War (DoW) requirements, including safeguarding Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Develop, implement, and maintain policies, controls, and technical safeguards necessary to sustain NMT's eligibility for DoW-funded programs.methodologies that enhance ICASA's capabilities and mission impact.

Documentation, Training, and Professional Development Develop and maintain technical documentation, diagrams, standard operating procedures, and knowledge management resources. Provide technical training, mentorship, and guidance to staff, researchers, students, and stakeholders. Maintain professional knowledge of current and emerging technologies, industry standards, cybersecurity practices, and applicable regulations. Perform other duties as assigned in support of ICASA's mission and strategic objectives.

REQUIRED QUALIFICATIONS:

Bachelor's Degree in Computer Science or Information Technology. Experience administering and troubleshooting Windows, Linux (RHEL preferred), and macOS systems in enterprise environments. Knowledge of switches, routers, firewalls, VPNs, network segmentation, and enterprise networking principles. Experience supporting on-premises, cloud, and hybrid computing environments with a focus on availability, scalability, and performance. Working knowledge of CMMC 2.0, NIST 800-171, vulnerability management, identity and access management, encryption, and security monitoring. Experience with Infrastructure as Code (IaC), automation tools, configuration management, and deployment workflows. Experience implementing and maintaining monitoring, backup, recovery, and business continuity solutions. Ability to diagnose and resolve complex hardware, software, systems, and network issues while providing excellent customer support. Ability to create technical documentation, standard operating procedures, diagrams, and communicate effectively with technical and non-technical stakeholders. Experience with AWS, Azure, Google Cloud, Kubernetes, Docker, and containerized application environments. Experience supporting research laboratories, experimentation environments, testbeds, or high-performance computing infrastructure. Experience implementing enterprise identity solutions, SSO, MFA, Active Directory, LDAP, Entra ID, or similar technologies. Experience with PostgreSQL administration, database maintenance, backup, and performance tuning. R Proficiency with PowerShell, Bash, Python, or similar scripting languages for automation and systems management. Familiarity with CJIS, NIST Cybersecurity Framework, RMF, FedRAMP, or other government security standards. Exposure to wireless communications, cybersecurity ranges, data science environments, or experimental technology platforms. Experience participating in technology roadmaps, architecture reviews, infrastructure planning, and technical project execution. Must be a US Citizen and eligible to obtain up to a TS/SCI Security Clearance.

LIFTING REQUIREMENTS:

(f)requently, (o)ccasionally, or (s)eldom

0 - 15 pounds	F
15 - 30 pounds	F
30 - 50 pounds	S
50 - 100 pounds	O
100 + pounds	N

PHYSICAL DEMANDS:

Standing 20%	Sitting 50%	Walking 10%	Pulling
Pushing	Lifting 5%	Stooping	Kneeling
Crawling	Climbing	Reaching 5%	Other 10%

Apply to: nmtjobapps@npe.nmt.edu