IT Systems Analyst

AngelEye Health · Information Technology

Location	Little Rock, AR (In-Office), Occasional travel to Nashville, TN
Department	Information Technology
Reports To	Jay Maples, CISO
Experience	3-5+ years in IT Systems, Security, or Compliance Administration
Employment	Full-Time

Role Overview

AngelEye Health is a healthcare technology company building neonatal care solutions trusted by hospitals across the country. As IT Systems Analyst, you will serve as a critical part of the IT Systems and Security team, helping to secure, manage, and continuously improve the internal systems and tools that keep our team and compliance posture operating at the highest standard.

This is a hands-on, cross-functional role at the intersection of IT administration, networking, security operations, and compliance. You will own day-to-day user and system management and support while supporting the CISO on security and regulatory compliance activities. The ideal candidate is equal parts detail-oriented problem-solver and proactive communicator, someone who thrives in a fast-moving healthcare technology environment and takes ownership of the infrastructure they manage.

Key Responsibilities

User Lifecycle & Identity Management

- **Systems Management Employee Onboarding & Offboarding:** Execute secure, timely provisioning and deprovisioning of user accounts, devices, and application access across all internal systems.
- **IAM Administration:** Manage user accounts, roles, groups, and permissions in JumpCloud and Google Workspace, ensuring least-privilege access principles are enforced.
- **SSO & Application Integrations:** Maintain and configure Single Sign-On (SSO), SAML, and OAuth integrations between the directory and third-party SaaS applications.
- **Access Reviews:** Conduct and document regular user access reviews and privilege audits to support SOC 2 compliance and internal security policies.

Security Operations & Compliance Support

- **CISO Support:** Serve as the CISO's primary operational partner for day-to-day security tasks helping to implement policies, gather compliance evidence, and respond to internal security tasks and incidents.
- **Compliance Administration:** Maintain and manage the organization's compliance monitoring platform, including evidence collection, control monitoring, and remediation tracking to support continuous SOC 2 readiness.
- **Endpoint Security:** Deploy, monitor, and maintain enterprise antivirus and endpoint security tooling. Enforce endpoint hardening standards including full-disk encryption and screen lock policies.

- **Security Reviews:** Evaluation of both Internal and External systems and software against security and compliance standards. Maintain the vendor risk register and assist in completing or reviewing security questionnaires.
- **Security Incident Response:** Assist in the detection, investigation, and documentation of internal security incidents, including unauthorized access events, phishing reports, and anomalous endpoint behavior.
- **SSL & Certificate Management:** Track and manage the full lifecycle of SSL/TLS certificates across internal and customer-facing systems to prevent lapses and service disruptions.

Internal Systems & Infrastructure Management

- **Device Lifecycle:** Provision, configure, maintain, and troubleshoot end-user computing devices — desktops, laptops, and mobile devices across Windows, Linux, and macOS.
- **MDM & Directory Administration:** Administer cloud directory and MDM platforms as the primary tools for device enrollment, policy deployment, configuration management, and patch management.
- **Hardware Support:** Act as the primary escalation point for complex hardware and OS-level issues, minimizing employee downtime and resolving issues efficiently.
- **Network Maintenance:** Manage and maintain internal network infrastructure ensuring high availability and optimal performance.
- **Physical Access & Surveillance:** Administer office door access control and IP camera systems to maintain a safe, secure workplace.
- **Telecommunications:** Support and manage corporate phone systems to ensure reliable internal communication channels.
- **Documentation:** Create and maintain IT documentation including network diagrams, SOPs, system configuration records, and end-user guides.
- **Continuous Improvement:** Proactively identify and recommend improvements to tooling, processes, and security posture across both physical and digital infrastructure.

Required Qualifications

- 3-5+ years of experience in IT Systems Administration, Security Administration, or a closely related role
- Deep, hands-on experience administering cloud directory and MDM platforms in a corporate environment
- Proven expertise in IAM protocols (SAML, OIDC, SSO, LDAP) and integrating MDM platforms with cloud directories
- Experience with compliance monitoring and trust management platforms supporting SOC 2 or similar frameworks
- Solid understanding of IT security principles including role-based access controls, endpoint hardening, least-privilege access, and certificate management
- Familiarity with enterprise antivirus and endpoint protection platforms
- Working knowledge of core networking concepts: DNS, DHCP, TCP/IP, VLANs, VPNs, and firewall management.
- Experience managing physical security technologies including door access control and camera surveillance systems
- Exceptional analytical and troubleshooting skills with a methodical approach to complex technical problems
- Strong verbal and written communication skills and ability to explain technical concepts clearly to non-technical stakeholders
- Willingness to occasionally travel to remote office location for on-site systems or infrastructure work.

Preferred Qualifications

- Relevant certifications: CompTIA Security+, CompTIA Network+, Google Workspace Administrator, or equivalent
- Experience supporting SOC 2 Type II audits including evidence collection, control documentation, and remediation tracking
- Familiarity with compliance frameworks such as SOC 2, HIPAA, or ISO 27001
- Experience with automation and scripting (PowerShell, Bash, or Python) to streamline IT and security operations
- Prior experience in a healthcare technology or regulated industry environment is a plus
- Comfort working in a fast-paced startup or growth-stage environment where processes are still being built
- Experience with JumpCloud, Google Workspace, Vanta, AWS

Why AngelEye Health

At AngelEye Health, our technology is directly connected to the care of the most vulnerable patients in the hospital. The work you do to secure and maintain our internal systems has a real impact on our ability to serve families and clinicians who depend on us. We offer a collaborative, mission-driven environment where you'll have direct access to senior technical leadership, ownership over your domain, and the opportunity to help shape our security and IT practices as the company scales. We offer competitive salary and healthcare benefits package.

AngelEye Health · Little Rock, AR · jmaples@angeleyehealth.com