Microsoft Network Administrator

Work Location: Remote: Honolulu, HI	**Position Type: Full-time**
Reports to: Owner	**FLSA Status: Exempt**
Salary Range: Commensurate with Experience	

Position Summary

The Microsoft Network Administrator supports Microsoft cloud services, Windows endpoints, and client network infrastructure across multiple organizations. This is a hands-on role for someone who can troubleshoot independently, implement approved changes carefully, and communicate with both technical and nontechnical users.

Key Responsibilities

Microsoft 365 and Identity Administration

- **Tenant administration:** Maintain users, groups, licenses, mailboxes, and approved settings across Microsoft 365, Exchange Online, Teams, SharePoint Online, and OneDrive.
- **Identity and access:** Administer Microsoft Entra ID accounts, authentication methods, role assignments, and approved Conditional Access policies using least-privilege practices.
- **User lifecycle:** Complete onboarding, access changes, and offboarding, including approved data handoffs and timely access removal.
- **Environment separation:** Verify the correct client tenant and administrative context before making changes; keep client credentials, data, and records appropriately separated.

Endpoint Management and Security Operations

- **Device administration:** Enroll, configure, monitor, and troubleshoot Windows devices through Microsoft Intune, including device compliance, configuration profiles, applications, and update policies.
- **Endpoint protection:** Maintain approved Microsoft Defender configurations, review endpoint health and alerts, and escalate suspected security incidents promptly.
- **Device safeguards:** Support BitLocker encryption and recovery-key escrow, Windows LAPS, local administrator restrictions, and approved endpoint-hardening standards.

- **Troubleshooting:** Resolve Windows, Microsoft 365 application, authentication, enrollment, printing, and connectivity issues.
- **Lifecycle management:** Maintain hardware and software inventories and support device deployment, replacement, secure retirement, and documented handoff.

Network and Infrastructure Administration

- **Network operations:** Configure and troubleshoot business firewalls, switches, wireless access points, VLANs, VPNs, and related connectivity within approved designs.
- **Core services:** Diagnose TCP/IP, DNS, DHCP, routing, wireless, and internet connectivity issues using a structured troubleshooting process.
- **Windows infrastructure:** Support Windows Server, Active Directory, Group Policy, file permissions, and related services where present in client environments.
- **Resilience:** Monitor assigned backup jobs, investigate failures, and assist with authorized restore tests and recovery documentation.
- **Vendor coordination:** Work with internet providers, software vendors, equipment suppliers, and other IT service providers to resolve issues and complete upgrades.

Cybersecurity and Compliance Support

- **Control implementation:** Apply approved technical baselines and remediation steps supporting client cybersecurity and CMMC readiness efforts.
- **Evidence collection:** Capture accurate configuration exports, screenshots, logs, and other technical evidence from the authoritative client environment.
- **Finding remediation:** Help resolve vulnerabilities, configuration gaps, and assigned corrective actions; verify and document results.
- **Data protection:** Follow client-specific procedures for sensitive information and Controlled Unclassified Information (CUI), using only authorized systems and transfer methods.
- **Scope discipline:** Escalate policy exceptions, high-risk changes, and compliance interpretation questions to the technical delivery lead.

Client Service, Documentation, and Change Management

- **Client support:** Own assigned requests through resolution or a clearly documented handoff, keeping users informed about status and next steps.
- **Technical records:** Maintain network diagrams, inventories, configuration records, procedures, and troubleshooting notes without placing secrets in ordinary documentation.
- **Safe changes:** Record the purpose, authorization, validation steps, and rollback approach for material changes; pilot changes before broad deployment when appropriate.
- **Automation:** Use PowerShell to streamline repeatable administration and reporting, with review and testing before production use.

- **Service accountability:** Record time, work performed, outcomes, and outstanding issues accurately for client reporting and billing.

Required Qualifications

- **Relevant experience:** Approximately 3–5 years in systems administration, network administration, IT support, or a comparable role, or equivalent demonstrated hands-on capability.
- **Microsoft administration:** Practical experience administering Microsoft 365 and Entra ID, including user access, authentication, and common service issues.
- **Endpoint management:** Hands-on Windows administration and experience with Intune or a comparable endpoint-management platform.
- **Networking fundamentals:** Working knowledge of TCP/IP, DNS, DHCP, VLANs, VPNs, firewalls, switching, and wireless networking.
- **Security practices:** Demonstrated understanding of least privilege, multifactor authentication, patching, endpoint protection, encryption, and secure credential handling.
- **PowerShell:** Ability to read, safely modify, and run administrative scripts, interpret output, and recognize when additional review is needed.
- **Troubleshooting and judgment:** Ability to investigate root causes, validate fixes, recognize risk, and escalate issues appropriately.
- **Communication and organization:** Clear written documentation, professional client communication, and the ability to manage competing priorities across multiple environments.

Preferred Qualifications

- **Government cloud:** Experience administering Microsoft 365 GCC environments.
- **Regulated environments:** Familiarity with CMMC, NIST SP 800-171, CUI handling, or support for defense industrial base organizations.
- **Microsoft security:** Experience with Microsoft Defender for Endpoint, Defender for Office 365, and Microsoft Purview capabilities such as sensitivity labels, data loss prevention, and retention.
- **Advanced endpoint administration:** Experience with Windows Autopilot, security baselines, application packaging, BitLocker recovery workflows, and Windows LAPS.
- **Hybrid infrastructure:** Experience with Windows Server, Active Directory, Group Policy, virtualization, and cloud migrations.
- **Consulting or managed services:** Experience supporting multiple clients with separate administrative boundaries, service commitments, and documentation requirements.
- **Professional development:** Relevant Microsoft, networking, or cybersecurity certifications are valued but do not replace demonstrated practical skills.

Work Environment

- Hybrid work environment with duties performed both remotely from a secure home office and on-site at client offices, or other designated work sites as business needs require.
- Remote work requires a reliable high-speed internet connection, a private workspace suitable for handling sensitive information, and the ability to maintain confidentiality during calls, meetings, system administration, and documentation activities.
- On-site client work may include meetings with stakeholders, security assessments, infrastructure reviews, endpoint or network troubleshooting, compliance evidence collection, and support for implementations, audits, or remediation activities.
- Must protect confidential information and use approved administrative accounts, tools, and processes.
- Must be able to follow client site security requirements, access procedures, visitor controls, confidentiality expectations, acceptable use policies, and safety requirements while working at client facilities.
- May require local travel and occasional inter-island, mainland, or other travel for client support, assessments, project work, training, or compliance activities, with schedules determined by business and client needs.
- Work may involve participation in after-hours maintenance windows, urgent security response, system outages, vulnerability remediation, or incident response activities outside normal business hours.
- Must be able to use company-approved devices, security tools, VPN, multifactor authentication, endpoint protection, encrypted storage, and secure communication platforms in accordance with organizational policies.
- Work typically requires prolonged periods of computer use, video conferencing, technical documentation, system monitoring, and collaboration with internal teams, clients, vendors, auditors, and service providers.
- May occasionally need to lift, move, or connect IT equipment such as laptops, desktops, peripherals, small network devices, or related hardware consistent with client support and infrastructure duties.
- Must be eligible to work in the U.S. and undergo a background check; DoD security clearance is preferred but not required.

Equal Opportunity Statement

Alani Group LLC is an Equal Opportunity Employer. We celebrate diversity and are committed to creating an inclusive environment for all employees.