

NEOMIN INFORMATION TECHNOLOGY SERVICES

District Technology Designated Contact Authorization Form

1. Purpose, Governance & Policy Scope

This form officially designates the primary technical authority for the district. The designated contact is authorized to make operational and technical decisions on behalf of the district for identity management, system access, configuration approvals, and joint technical troubleshooting across all current and future NEOMIN-managed platforms.

- **Policy & Directive Hierarchy:** All decision-making authority and system configurations granted under this agreement remain subject to NEOMIN's security policies, acceptable use procedures, and directives from NEOMIN's Director and Governing Board. Access levels may be scoped or administratively restricted to ensure compliance with these standards.
- **System-Specific Addendums:** Specific platforms or services (e.g., VoIP/Telephony, Managed Security) may be subject to individual Service Level Agreements (SLAs), Addendums, or Detailed Responsibility Matrices that outline granular duties (such as local network maintenance, power, and physical security). Where specific service addendums exist, their explicit terms take precedence over the general terms of this form.

2. Designated Technical Contact Information

District Name:	
Designated Contact Name:	
Title / Role:	
Contact Type:	☐ Internal District Staff ☐ Third-Party Technology Vendor
Vendor Name if Applicable	
District Email & Direct Phone:	Email: _____ Phone: _____
Vendor Email & Direct Phone:	Email: _____ Phone: _____

3. Scope of Technical Expectations & Shared Responsibilities

By signing below, District Administration authorizes NEOMIN to interface directly with the designated contact. The contact is expected to manage, coordinate, or assist with the following operational areas within NEOMIN's administrative guidelines:

- **Identity, Directory & SSO Integration:** Authority to request and approve user authentication, single sign-on (SSO), and access permissions across identity platforms (e.g., miniOrange, Frontline Platform). Responsible for assisting with local district environments (e.g., Google Workspace) to maintain integration health.
- **Infrastructure & Hosted Virtual Servers:** For district environments hosted on NEOMIN's VMware cloud, NEOMIN maintains the physical hardware, hypervisor layer, and local cloud redundancy. The designated

contact is responsible for operating system health, application management, and data integrity within the virtual machines.

- **Backups & Data Retention:** For districts utilizing NEOMIN's MSP360 backup solution or hosted server infrastructure, the designated contact holds sole responsibility for configuring, monitoring, and reviewing backup jobs for success or failure, as well as establishing independent data retention procedures if NEOMIN backup services are declined.
- **Network, Wireless & Telephony:** Administrative access and visibility to monitor network bandwidth (e.g., Arista edge dashboards), manage wireless platforms (e.g., Arista Cloud, Extreme WiFi, Cisco Meraki), and oversee telephony systems (e.g., 3CX), subject to service-specific support addendums.
- **Security & Threat Management:** Oversight of district security tools within defined policy limits, including URL filtering policies, firewall log reviews via NEOMIN Panorama, and security awareness tools (e.g., Tech Guard phishing simulations).
- **Future Services & Platform Expansion:** Authority to grant operational approvals, configure settings, and assist in onboarding for any new software, platform, or security control deployed by NEOMIN during the term of this agreement.

4. District Administrative Approval

I certify that the individual or entity listed in Section 2 is authorized to act as the district's technical decision-maker within the framework of NEOMIN's policies, procedures, governing directives, and specific service addendums.

Superintendent / Executive Signature

Date

Printed Name & Title