

REQUEST FOR PROPOSALS

ADVANCED NETWORK ADMINISTRATION & INFRASTRUCTURE

WORKING DRAFT — Procurement dates, service targets, and contract terms require Logos approval.

RFP detail	Information
Issuing organization	Logos Public Charter School • Medford, Oregon
Issue date	October 29th, 2026
Questions deadline	November 20th, 2026
Proposal deadline	November 27th, 2026
Anticipated service start	January 1st, 2027
Submission contact	accounting@logoscharter.com
Initial term	Up to 12 months; renewal only by written agreement

1. Purpose and award structure

Logos Public Charter School seeks proposals for advanced network administration and physical network infrastructure support (this RFP). This is a standalone procurement. Logos is separately soliciting the complementary technology services scope and may award the two contracts to different providers. A bidder may respond to either or both solicitations, but must submit a distinct proposal and pricing for each. The selected provider must cooperate with the separately selected technology contractor, school personnel, and Medford School District (MSD). Logos prioritizes competent and timely troubleshooting, clear ownership of work, measurable service commitments, transparent pricing, and independence from vendor-controlled hardware.

2. Operating environment

- Approximately 100 employees with staff laptops; approximately 600 student Chromebooks. Many routine issues are resolved internally before a service ticket is opened.
- Two physical sites with a wireless air bridge connecting the primary and secondary buildings.
- Internet is supplied and managed by Medford School District; Logos' selected vendor does not independently control the upstream connection.
- Recently refreshed UniFi networking equipment; Logos intends to retain its equipment and purchase hardware independently when desired.
- Approximately 100 surveillance cameras; existing UniFi Protect NVR surveillance system.
- MSD manages the telephone service, while phone connectivity depends on switches supported by Logos' IT provider.
- Google Workspace is used for email and documents; Logos does not operate a conventional Active Directory environment.
- Technically capable school employees may provide on-site observation, basic diagnostics, and hands-on coordination with remote network engineers.

Additional sensitive system details may be provided to shortlisted bidders as appropriate. State any assumptions or discovery work needed for accurate pricing.

3. Mandatory requirements

- Hardware independence: Services may not be conditioned on purchasing or leasing hardware through the provider. Provider must support compatible existing equipment and equipment obtained from third parties, subject to clearly disclosed, reasonable technical or manufacturer-support limitations.
- Ownership and access: Logos retains ownership of school-purchased hardware, configurations, credentials, licenses purchased in its name, and school data. Provider shall not withhold administrative access or documentation because Logos changes vendors.
- No forced replacement of recently purchased equipment as a condition of award. Recommended replacements may be offered separately with supporting reasons and optional pricing.
- Initial contract may not exceed 12 months. Renewal or a longer later term requires a new written agreement. Proposed terms must include termination for material or repeated service-level failures with a reasonable opportunity to cure, and transition assistance.
- Provide all recurring fees, hourly rates, travel charges, minimums, emergency premiums, software/license charges, project exclusions, price-increase rules, and offboarding charges. No undisclosed charges.
- Provider must disclose use of subcontractors, including local dispatch partners, and remain responsible for their performance, confidentiality, and applicable school access requirements.
- Maintain appropriate security, confidentiality, least-privilege access, and personnel screening suitable for a K–12 environment. All vendor employees and subcontractors who will be sent on-site to Logos facilities must successfully complete a background check before performing on-site work. Disclose cybersecurity incident response and data handling practices.
- Coordinate promptly and in good faith with the separately contracted technology provider and Medford School District (MSD), where applicable. Share relevant diagnostic findings, identify responsible systems, and participate in joint troubleshooting without unreasonable barriers or blame-shifting. Each provider remains accountable for its own scope and commitments.

4. Scope of services

network infrastructure provider owns the network and physical network infrastructure, including approved on-site equipment work directly or through qualified subcontractors. It does not own staff laptop repairs, endpoint security agents, or routine end-user device support.

4.1 Scope

- Administer, monitor, troubleshoot, and document the existing UniFi network environment, including switches, wireless access points, VLANs, subnets, routing, firewall/security settings, and related connectivity.
- Troubleshoot the two-building wireless bridge, network performance, intermittent outages, and dependencies between the two sites.
- Work effectively in an environment where MSD supplies upstream internet and manages telephone service; identify fault domains and coordinate escalation without assuming control over MSD systems.
- Support network connectivity for approximately 100 surveillance cameras and associated UniFi Protect NVR surveillance system; clearly distinguish network responsibilities from camera repair and vendor-specific software support.

- Support secure remote connectivity and network access methods appropriate to the existing architecture, including applicable VPN technologies.
- Plan and execute approved configuration changes, firmware/security updates, monitoring, backup of network configurations, and recovery procedures; obtain approval for material changes.
- Provide incident response for network outages and major degradation, with access to qualified senior engineers and an identified local field-service option for physical intervention. network infrastructure provider is responsible, directly or through qualified subcontractors, for installation, replacement, repositioning, and physical troubleshooting of network infrastructure, including UniFi access points, switches, cameras, surveillance monitors, and related equipment; equipment swaps, labeling, testing, and documentation. Licensed cabling/electrical work may be separately subcontracted as required.
- Document network topology, critical dependencies, device inventory, configuration backup location, credentials/access procedures, and known risks.

4.2 Required evidence of advanced expertise

Offerors must explain their real-world experience with multi-VLAN/multi-subnet networks, Layer 2/Layer 3 switching, wireless bridges, UniFi management, network segmentation, troubleshooting across third-party-managed internet connections, and surveillance traffic. Provide examples of comparable environments and describe the actual troubleshooting approach. Certifications are helpful but are not substitutes for demonstrated ability.

4.3 Named engineers and depth of coverage

Identify the primary network engineer, at least one independently qualified backup engineer, and the escalation lead who would support Logos. For each, provide role, relevant experience, specific technology competencies, normal coverage hours, and whether the person is an employee or subcontractor. State how many additional senior network engineers could assist if these individuals are unavailable. Do not substitute the name of an account manager for the required technical personnel.

Explain the process when the primary engineer is sick, on vacation, assigned to another client, or unable to resolve a problem. Confirm that backup personnel will have secure access to current network documentation and can begin independent troubleshooting without waiting for the primary engineer.

4.4 Local physical intervention

Remote-first network support is acceptable. Offerors must describe a realistic process for obtaining qualified local hands-on support, including named partner or coverage method, typical dispatch window, additional costs, and how remote engineers direct on-site personnel.

4.5 Deliverables

- Current network topology and critical systems documentation, updated after material changes.
- Configuration backup and recovery plan, including periodic verification.
- Monthly reporting of incidents, priority, response time, troubleshooting-start time, restoration time, final resolution time, and outstanding issues.
- Written root-cause analysis for major incidents, including preventive recommendations.
- Quarterly review of network health, recurring issues, risks, and proposed improvements.

5. Division of responsibility and joint incident handling

Responsibility	This contractor	Other separately awarded contractor
Staff laptops, peripherals, OS updates, endpoint protection	Coordinate / refer	Primary
UniFi network, bridge, switches, access points, network security	Primary	Coordinate / refer
Cameras, UniFi Protect NVR, physical network equipment work	Primary	Coordinate / refer
Upstream internet and telephone service	MSD-managed; coordinate as needed	MSD-managed; coordinate as needed
Unclear fault affecting both devices and network	Prompt joint diagnosis and documented handoff	Prompt joint diagnosis and documented handoff

When the cause is unclear, neither provider may close or decline a ticket solely because the issue may belong to the other scope. The receiving provider must document initial findings, notify the appropriate party, and support a coordinated handoff. No contractor is required to perform out-of-scope project work without authorization.

6. Service levels, escalation, and reporting

The RFP intentionally separates acknowledgment, qualified investigation, restoration, and permanent resolution. A ticket is not considered actively investigated merely because an automated reply or account manager acknowledges it. Offerors must either accept the proposed targets below or clearly state alternate commitments and their rationale. All times below are PROPOSED and must be approved by Logos before publication.

Priority	Example	Meaningful response	Qualified troubleshooting begins	Restoration target / updates
P1 Critical	Site-wide outage, bridge failure, major security incident	15 minutes	30 minutes	Restore as soon as feasible; updates every 30 minutes
P2 High	Major degradation affecting multiple users or key system	1 business hour	2 business hours	Target workaround/restoration within 1 business day; updates every 2 business hours
P3 Normal	Localized or intermittent problem	4 business hours	1 business day	Target resolution plan within 2 business days; daily updates while active
P4 Routine	Minor issue, planned request	1 business day	3 business days or scheduled date	Agreed completion date; updates on milestone changes

Definitions: Response = a human acknowledgment that confirms priority, ownership, and next step. Troubleshooting start = qualified technician actively diagnosing. Restoration = core service available again, including an accepted workaround. Resolution = underlying issue corrected and confirmed with Logos. Report all four timestamps separately.

For P1/P2, bidders must state hours of coverage, after-hours contact procedures, and whether the proposed target is clock time or business time. Resolution targets may depend on MSD, manufacturers, replacement parts, or physical access; bidders must still document escalation, continued effort, and communication. Ticket clocks should not be paused without a documented reason and notice to Logos.

Proposed accountability: monthly service-level scorecard; repeated material failures trigger a written corrective-action plan; continued failures after cure allow termination without early-termination penalties. Bidders must describe service credits, remedies, and exclusions they propose. Final contract definitions and thresholds are subject to negotiation.

7. Security and software pricing

Logos wants necessary and effective security measures, not an automatically bundled managed-services stack. Clearly identify included security work and optional products; distinguish your responsibilities from those of the separately contracted provider.

- Describe network segmentation, secure administrative access, UniFi firmware/configuration patching, monitoring, configuration backups, logging, and network security incident response.
- List each proposed network security/management product with function, covered systems, recurring cost, implementation, ownership, and transfer/cancellation terms.
- Identify required versus optional products and explain how existing UniFi systems and MSD-managed internet affect recommendations.
- Describe transfer of network configuration, credentials, monitoring, and administrative tools at contract end.

8. Required proposal format and questions

Use the numbered checklist as your response outline. Answer each question directly with specific personnel, examples, and commitments; short tables or bullets are welcome. Do not submit generic marketing narratives in place of answers.

#	Required response	Include in your answer
01	Support model	Describe how staff request help, ticket ownership, escalation, business hours, and emergency procedures.
02	Assigned personnel and backup	Name primary staff, qualified backup, escalation contact, relevant experience, and absence coverage.
03	Service-level commitments	Respond to Section 6: human acknowledgment, qualified troubleshooting start, restoration, progress updates, and resolution reporting.
03A	Qualified engineering depth	Identify at least two independently qualified engineers, total senior network capacity, escalation leadership, and coverage during simultaneous client emergencies.

04	On-site service	Explain how visits are requested, normal dispatch windows, staffing, subcontractors, and any fees.
05	Scope and experience	Explain your experience with the services in this RFP, including a comparable example.
06A	Relevant network expertise	Explain hands-on UniFi, VLAN/L2/L3, multi-subnet, wireless bridge, UniFi Protect NVR, and third-party internet troubleshooting; include two concrete incidents or projects.
06B	Physical intervention	Identify local technician/partner, network equipment work arrangements, dispatch expectations, and charges.
06	Security and background checks	Describe controls within your scope, handling of school data, account access, and completed background checks for all on-site staff/subcontractors.
07	Vendor independence	Confirm hardware-purchase independence, continued use of compatible school-owned equipment, school-held access, and transfer at exit.
08	Coordination with other provider and MSD	Describe handoff procedures, incident coordination, and how you will prevent support gaps when causes are initially uncertain.
09	Pricing	Complete the standardized pricing schedule; disclose exclusions, minimums, premiums, software, rate increases, and offboarding.
10	Onboarding and offboarding	Provide a transition plan, documentation approach, and exit process.
11	Business references	Provide 2–3 business references from organizations of similar size and/or structure, with contacts and services provided.
12	Contract exceptions	Confirm a term of no more than 12 months and performance-based termination; list requested exceptions.

9. Standardized pricing response

Cost component	Proposed amount / terms
Base monthly/annual service fee	[Bidder completes]
Included hours, tickets, or visits	[Bidder completes]
Additional remote hourly rate	[Bidder completes]

Additional on-site hourly rate / minimum	[Bidder completes]
After-hours emergency rate	[Bidder completes]
Travel / dispatch charges	[Bidder completes]
Onboarding / discovery fee	[Bidder completes]
Required software / licenses	[Bidder completes]
Optional software / licenses	[Bidder completes]
Project work / exclusions	[Bidder completes]
Transition / offboarding fees	[Bidder completes]
Estimated year-one total	[Bidder completes]

Provide a realistic first-year total, separating fixed, variable, and optional costs. State assumptions about users, devices, sites, incident volume, and any additional charges.

10. Evaluation methodology

Logos will screen mandatory conditions before scoring. The school may request written clarification and verify qualifications and service quality through references. No technical interview or live exercise is required.

Evaluation criterion	Points
Relevant network technical capability	25
Qualified engineering depth and backup	25
Response and escalation commitments	25
Coordination and local intervention	10
Transparent cost and value	10
References and transition readiness	5
TOTAL	100

Reviewer guide: 0 = absent; 1 = weak or unsupported; 3 = credible but incomplete; 5 = specific, well evidenced, and supported by personnel, references, or enforceable commitments. Scale ratings to the points shown.

11. Proposed contract principles

- Initial term no longer than 12 months; no automatic multi-year commitment. Extensions and later 2–3-year agreements only by mutual written agreement.
- Define severity levels, clocks, reporting, escalation, and material/repeated failures in the final service-level agreement.
- Termination for cause, including repeated service-level failures after notice and cure; consider a separate termination-for-convenience right with a defined notice period.
- School ownership/control of purchased assets, school data, network configurations, administrative credentials, and transferable school-held licenses.
- Reasonable documented exit assistance, predictable fees, and timely credential/documentation transfer; no withholding of access or forced equipment buyout.
- Written approval before billable projects or changes outside scope; clear change-order process and restrictions on unilateral price increases.
- Clear division of responsibility where MSD, staff device support provider, and network infrastructure provider intersect.

12. Submission and procurement administration

Submit one PDF proposal for this standalone RFP to accounting@logoscharter.com by Friday, **November 27th, 2026**. Questions should be sent to accounting@logoscharter.com by Friday, **November 20th, 2026**. Logos may issue written clarifications to all participating bidders, request written clarifications, check references, negotiate terms, reject proposals, or award this scope separately from the complementary technology services RFP as permitted by applicable procurement rules and school policy. Final dates and procedures must be checked against Logos' governing procurement requirements before publication. Logos reserves the right to disqualify submissions where there is clear evidence of undisclosed or inappropriate AI-generated questions or answers, particularly where AI is used to misrepresent qualifications, personnel, experience, or technical understanding. Any permitted AI assistance must be reviewed and verified by the bidder; bidders remain responsible for the accuracy and originality of their responses.

For avoidance of doubt, vendors responding to both technology RFPs must submit separate scope-specific proposals and pricing; Logos may select different firms for each.