



Request for Proposals (RFP)

Technology Support, Managed Services & Strategic IT Planning Services



Bid Issue Date: Monday, October 12, 2026

Bid Deadline Date: Friday, October 30, 2026

01. Summary

01.01 Introduction of Project

The Omaha Municipal Land Bank (OMLB) invites qualified providers to submit proposals for professional information technology ("IT") services beginning January 1, 2027, for an initial 12-month term, with an optional one-year extension upon mutual agreement between OMLB and the selected provider.

In addition to ongoing technology support and managed services, the selected provider will assist OMLB in strengthening its overall technology environment and cybersecurity posture, improving service quality and operational efficiency, managing technology costs, and maximizing the value of OMLB's technology investments.

01.02 Purpose & Objectives

As part of its 2027 budgeting and organizational planning, OMLB is evaluating its technology support model and seeking a managed IT services provider capable of supporting both the organization's day-to-day technology needs and its longer-term technology strategy.

Through this RFP, OMLB seeks to:

- ensure reliable, responsive day-to-day technology support;
- strengthen cybersecurity, technology risk management, and business continuity;
- improve technology administration, documentation, access controls, and asset management;
- establish clear technology service levels, roles, responsibilities, and accountability;
- identify opportunities to improve operational efficiency and responsibly manage technology costs;
- develop a sustainable technology roadmap and budget strategy for 2027 and beyond; and
- establish a trusted advisory relationship to support future technology decisions, initiatives, and investments.

OMLB may also engage the selected provider for authorized special projects and consulting services outside the recurring managed services scope, as described in Section 02.06.

02. Scope of Work

OMLB seeks a qualified managed IT services provider to serve as the organization's primary technology support partner. The selected provider will be responsible for day-to-day technology administration and support, cybersecurity management, technology infrastructure and asset management, and strategic IT planning.

The selected provider should provide the following services as part of its proposed base scope and clearly identify any services that would require additional fees, third-party costs, or separate project authorization.

02.01 Managed IT Operations & User Support

The selected provider will provide ongoing administration and technical support for OMLB's technology environment, including:

- Microsoft 365 administration and support;
- user account creation, modification, and deactivation associated with employee onboarding, role changes, and offboarding;
- administration of email, SharePoint, Teams, Copilot, and other Microsoft 365 services used by OMLB;
- software and licensing administration;
- help desk and troubleshooting support for staff;
- workstation and device setup, configuration, deployment, and replacement;
- remote support for authorized users;
- management of appropriate user permissions and access levels; and
- technical assistance related to OMLB's approved software applications and technology systems.

02.02 Cybersecurity & Technology Risk Management

The selected provider will support the security and integrity of OMLB's technology environment through ongoing cybersecurity administration, monitoring, and recommendations, including:

- endpoint protection and security management;
- implementation and administration of multi-factor authentication;
- security monitoring and incident response support;
- vulnerability identification and management;
- administration and monitoring of email security controls, including SPF, DKIM, and DMARC;
- review and management of user access and security permissions;
- cybersecurity awareness training for OMLB staff;

- identification of cybersecurity risks and recommended corrective actions; and
- consultation regarding technology security policies, practices, and controls.

02.03 Infrastructure, Devices & Asset Management

The selected provider will assist OMLB in maintaining reliable and cost-effective technology infrastructure, including:

- maintaining an accurate inventory of OMLB-managed technology assets;
- assisting with technology procurement and hardware recommendations;
- device configuration, deployment, maintenance, repair coordination, and replacement;
- development and maintenance of a hardware lifecycle and replacement plan;
- monitoring of critical network and infrastructure components;
- DNS and domain administration;
- backup administration and monitoring;
- disaster recovery planning and support;
- business continuity technology planning; and
- recommendations for improving the efficiency, reliability, or cost-effectiveness of OMLB's technology environment.

02.04 Access, Permissions, and Information Governance

The selected provider will assist OMLB in administering technology access and permissions to protect organizational information while enabling appropriate access by employees, board members, contractors, partners, and members of the public, as authorized by OMLB.

Services may include:

- Microsoft 365 user and permission management;
- SharePoint and Teams access administration;
- external/guest user access;
- periodic review of user permissions;
- recommendations regarding access controls and information-sharing practices; and
- technical support for secure public or external document access where required.

02.05 Strategic IT Planning & Advisory Services

The selected provider will serve as a strategic technology advisor to OMLB and assist leadership with evaluating technology needs, risks, investments and priorities.

At a minimum, strategic services will include:

- an initial assessment of OMLB's technology environment;
- identification of technology, cybersecurity, operational, or governance risks and opportunities;
- development and periodic updating of a technology roadmap;
- annual technology budget and investment recommendations;
- hardware and software lifecycle recommendations;
- recommendations regarding IT policies and governance;
- guidance regarding emerging technology needs and opportunities;
- quarterly technology/business reviews with OMLB leadership; and
- consultation regarding significant technology projects or decisions.

02.06 Special Projects & Consulting

OMLB may periodically request assistance with technology projects that fall outside the provider's recurring managed services. The provider should identify its process and pricing structure for such services.

No additional project work should be undertaken without prior authorization from OMLB.

Examples could include:

- major software implementation or migration;
- substantial SharePoint configuration or restructuring;
- technology consulting related to new organizational initiatives;
- significant cybersecurity remediation;
- major infrastructure changes; and
- other technology projects requested by OMLB.

02.07 Required Deliverables

02.07.01 Initial Onboarding Deliverables

1. Technology environment and asset inventory
2. User/account/access inventory
3. Initial cybersecurity and technology risk assessment
4. Documentation of critical systems and administrative access
5. Transition/onboarding plan
6. Initial recommendations and priorities

02.07.02 Recurring Deliverables

1. Help desk and service-level reporting
2. Security monitoring/reporting

3. Asset inventory updates
4. Licensing/account management
5. Cybersecurity awareness training
6. Quarterly technology/business review

02.07.03 Strategic Deliverables

1. Technology roadmap
2. Annual technology budget forecast
3. Hardware/software lifecycle recommendations
4. Cybersecurity improvement recommendations
 - IT policy/governance recommendations

03. Proposal Submittal Instructions & Requirements

03.01 Required Vendor Registration

Companies wishing to submit a proposal must be registered as an OMLB vendor. Vendor registration information is available on OMLB's website.

Link to form: <https://omahalandbank.org/get-involved/vendor-registration/>

03.02 Proposal Contents

Proposals should be organized using the sections below. OMLB may consider the completeness, clarity, and responsiveness of submitted information when evaluating proposals.

03.02.01 Company Overview & Qualification Statement

Please ensure the statements include the following:

- Company name, location, and primary contact
- Brief overview of the company and a portfolio of services offered
- Number of years the firm has been providing IT management services
- Describe relevant experience servicing organizations of similar size and complexity
- Relevant experience serving nonprofit, governmental, or public-sector organizations, if applicable.
- Qualifications and certifications relevant to the services described in this RFP
- Proof of insurance

03.02.02 Proposed Service & Model

Describe in detail the proposed approach to providing the services identified in Section 02, including:

- managed IT operations and user support;
- cybersecurity and technology risk management;
- infrastructure, device, and asset management;
- Microsoft 365 and access administration;
- strategic IT planning and advisory services; and
- special projects and consulting.

Vendors are required to identify any requested services needed through a third party or through subcontracting to perform the scope of services.

03.02.03 Transition & Onboarding Plan

Describe the proposed approach to onboarding OMLB, including discovery, technology assessment, documentation review, transfer of administrative access, user and asset inventory, cybersecurity review, and transition from the incumbent provider.

Vendors must identify the following:

- anticipated onboarding timeline;
- major onboarding activities and milestones;
- information or access required from OMLB;
- OMLB staff responsibilities;
- vendor responsibilities; and
- any one-time onboarding or transition costs.

03.02.04 Cybersecurity & Risk Management

Please describe your plan for providing services that speak to addressing the following needs:

- Cybersecurity tools and services included in the proposed scope;
- security monitoring approach;
- incident response and escalation procedures;
- vulnerability-management approach;
- endpoint-security approach;
- security awareness training;
- email and Microsoft 365 security support; and
- any cybersecurity services or tools requiring additional fees.

Included in your response, Vendors must identify any cybersecurity certifications, standards, frameworks, or third-party assessments relevant to the services proposed.

03.02.05 Service Levels, Help Desk & Response Times

Complete the following table using the service levels included in your proposed base service. If response or resolution targets vary by service plan, clearly explain those differences.

Priority	Example	Response Time	Resolution Target
Critical	<i>System outage, cybersecurity incident</i>		
High	<i>Email failure, major application issue</i>		
Medium	<i>User unable to access a non-critical system</i>		
Low	<i>General support request, software question</i>		

Incorporate in your table the additional items below:

- standard help desk hours;
- methods for requesting service;
- after-hours support availability;
- emergency contact process;
- escalation process; and
- any additional cost for after-hours or emergency service.

03.02.06 Reporting, Communication & Strategic Advisory

Describe how the vendor will communicate with OMLB regarding service performance, technology issues, cybersecurity risks, recommendations, and strategic planning.

Identify your approach for delivering the following items:

- routine reports provided;
- frequency of reporting;
- primary relationship/account management structure;
- escalation communication;
- approach to quarterly business reviews;
- technology planning process; and
- approach to budget and technology roadmap development.

03.02.07 Pricing Proposal

Provide a complete pricing proposal identifying the following:

- monthly recurring managed services fee;
- one-time onboarding/transition fees;
- per-user and/or per-device fees, if applicable;
- software and licensing costs included in the proposal;
- software and licensing costs not included in the proposal;
- cybersecurity tools or services charged separately;
- hourly or project rates for services outside the base scope;
- after-hours/emergency service charges;
- travel or other reimbursable expenses, if applicable;
- optional services; and
- any other anticipated charges.

Clearly identify all assumptions used in developing the proposed pricing and any circumstances that could result in charges beyond the proposed recurring fee.

03.02.08 References & Relevant Experiences

- Provide two to three professional references for projects of similar size, scope, or complexity.
- Including the client's organization; contact name, title, email address, phone number, and year(s) services were provided.
- Include examples of relevant prior work, case studies, or project summaries, as appropriate.

03.02.09 Exceptions, Assumptions & Subcontractors

Identify any exceptions to the requirements of this RFP, assumptions upon which the proposal is based, services the vendor believes are outside the proposed scope, and portions of the proposed services that will be performed by subcontractors or third-party providers.

03.02.10 Insurance & Business Compliance

Vendors shall provide evidence that the company is legally authorized and in good standing to conduct business and shall provide a current Certificate of Insurance evidence of applicable business insurance coverage.

The vendor shall identify any requested coverage that it does not currently maintain and indicate whether such coverage can be obtained prior to contract execution.

The selected vendor will be required to maintain insurance coverage throughout the contract term and provide updated certificates upon request by OMLB.

03.02.11 Proposal Certifications & Authorized Representative

Provide the name, title, contact information, and signature of an individual authorized to submit the proposal and bind the company to the proposed pricing and terms for the period specified in the proposal.

03.03 Submittal Instructions

Proposals should be submitted (PDF preferred) to info@omlb.org by **Friday, October 30, 2026**.

Late or incomplete proposals may not be considered.

03.04 Questions Regarding the RFP

Please contact Karla McGinnis-Taylor, Business Process Manager, 402-800-1242 info@omlb.org with any questions.

All questions regarding the scope of this RFQ must be submitted electronically to info@omlb.org by the October 12th question submittal deadline. All responses to the questions received will be posted on the website on or by October 16th.

Bid Posting Link: www.omahalandbank.org/bidding. (RFP webpage)

03.05 Proposal Evaluation

During the proposal period, OMLB staff and board members will review the contents of the proposal. Only bid packages that satisfy the above-mentioned criteria will be considered for this opportunity.

The following items will be the criteria used to evaluate proposals:

- Proposal requirements satisfied
- Qualifications and relevant experience
- Understanding of OMLB's needs
- Proposed service and support model
- Cybersecurity capabilities
- Transition/onboarding approach
- Service levels and responsiveness
- Strategic IT capabilities
- Cost and overall value
- References

The selected firm will receive an award letter from an OMLB staff member 24 – 48 business hours following the designated Award and Proposal selection date.

05. Timeline & Deadlines

05.01 Bid + Contract Award Schedule

Monday, October 12, 2026	RFP is issued
Wednesday, October 21, 2026	RFP-related Questions Submission Deadline
Friday, October 23, 2026	Response to Submitted Questions Posted Online
Friday, October 30, 2026	Proposal Submission Deadline
Wednesday, November 4, 2026	Proposal Selected and Awarded

05.02 Project Delivery Schedule

December 2026	Contract is signed and firm is formally onboarded
January 2027	Contract for services begins
April 2027	Contract Performance + Evaluation
August 2027	Consideration of Contract Renewal for 2028
December 2027	Scope of Services for 2027 Completed