



Managed Information Technology Services

Issue Date

10/1/2026

Proposal Due

10/22/2026

Introduction and Overview

Decide DeKalb Development Authority ("Decide DeKalb" or the "Authority") invites qualified managed service providers to submit proposals for secure, reliable, responsive, and cost-effective information technology services. The selected firm will serve as the primary point of accountability for end-user support, Microsoft 365 administration, cybersecurity, infrastructure oversight, backup and recovery, and strategic technology planning.

Decide DeKalb is a public economic development organization serving DeKalb County, Georgia. The Authority operates from one primary office location and supports approximately 15 to 25 employees, contractors, and authorized users, including remote and offsite work needs.

Key Dates and Communications

Milestone	Date / Time
RFP issued	10/1/2026
Written questions due	10/8/2016 by 5:00pm
Responses or addendum issued	10/15/2026 by 5:00pm
Proposals due	10/22/2026 by 5:00pm
Interviews, if needed	10/26/2026-11/25/2026
Board or final approval	1/14/2027
Anticipated service start	February 2027

Decide DeKalb may adjust the schedule as necessary. Questions must be submitted in writing to the procurement contact. Responses, clarifications, or changes may be issued by written addendum. Vendors shall not contact other Authority employees, board members, consultants, or representatives regarding this RFP unless authorized in writing.

Current Technology Environment

The following summary is provided for proposal development. Quantities and configurations may change. Vendors must clearly identify assumptions used in pricing, and the selected finalist may be asked to validate the environment before contract execution.

- Microsoft 365 Business Premium and Office 365 enterprise licensing, including Exchange Online, SharePoint Online, OneDrive, Teams, Defender, Teams Rooms, Copilot, Power BI, mailbox archiving, and cloud backup.
- Remote help desk and onsite support; endpoint monitoring and maintenance; managed detection and response; security awareness and phishing simulation.
- User onboarding and offboarding; identity, permissions, mailbox, license, and multifactor authentication administration.
- Firewall, wireless network, internet service coordination, device inventory, conference room technology, backup monitoring, testing, and restoration.

Scope of Work

The selected firm will provide the following services. Proposals may include disclosed subcontractors where needed to meet the scope.

1. Help Desk, Users, and Devices

- Provide telephone, email, and online ticket support for desktops, laptops, mobile devices, printers, peripherals, approved applications, connectivity, and conference room technology.
- Provide remote support and onsite support when remote resolution is not appropriate or successful; maintain ticket ownership, escalation, status, and resolution records.
- Provision and deprovision users; administer passwords, multifactor authentication, groups, permissions, shared mailboxes, distribution lists, licenses, and authorized data transfers.
- Maintain device inventory, endpoint monitoring, operating system and third-party patching, encryption support, warranty status, and secure device retirement.

2. Microsoft 365 Administration

- Administer Exchange Online, Teams, SharePoint Online, OneDrive, Entra ID, Microsoft Defender, Teams Rooms, Copilot, and Power BI within the awarded scope.
- Manage service health, configuration, security policies, retention, permissions, licensing, renewals, adoption, cost optimization, and user troubleshooting.

3. Cybersecurity

- Provide continuous security monitoring, endpoint detection and response, threat containment, investigation, remediation, vulnerability scanning, and incident escalation.
- Support multifactor authentication, conditional access, least privilege, Zero Trust, secure remote access, security awareness training, phishing simulations, and incident response planning.
- Promptly notify the Authority of suspected or confirmed incidents affecting Authority systems or data and provide after-action reporting.

4. Backup, Recovery, and Continuity

- Back up covered Microsoft 365 email, OneDrive, SharePoint, and Teams data; state frequency, encryption, storage, immutability, retention, and data ownership.
- Provide item-level restoration, routine backup and restoration testing, proposed recovery objectives, continuity support, and an orderly process for returning Authority data.

5. Network and Infrastructure

- Manage or support firewalls, switches, wireless access, connectivity monitoring, provider escalation, configuration backups, hardware replacement, warranty coordination, and critical updates.
- Maintain current network and infrastructure documentation and use documented change control for material updates.

6. Strategic Services, Reporting, and Optional Work

- Conduct quarterly business reviews and maintain a prioritized technology roadmap covering services, security, assets, licensing, projects, lifecycle planning, and budget recommendations.
- Provide monthly reports on ticket activity, response and resolution performance, unresolved issues, security events, patching, backups, assets, licensing, and recommendations.

- Maintain Authority-accessible documentation, including network diagrams, asset and licensing records, administrative procedures, configurations, contacts, and vendor dependencies.
- Provide separate pricing for after-hours support, onsite projects, board meeting support, procurement, AI consulting & opportunities, penetration testing, security assessments, migrations, office moves, cabling, and other project work.
- Other scenarios that changing times dictate

Service Levels and Transition

- Propose business hours, after-hours procedures, priority definitions, response and restoration or resolution targets, escalation paths, measurement rules, and remedies for repeated service-level failure.
- Provide named service management and escalation contacts and use auditable ticket and monitoring data.
- Provide a transition plan addressing discovery, roles, milestones, risks, incumbent coordination, secure transfer of access and documentation, deployment of tools, user communications, testing, acceptance, and steady-state support.
- Identify Authority dependencies, one-time fees, third-party costs, licensing changes, travel, hardware, and exclusions.

Required Deliverables

- Transition and implementation plan; current asset, licensing, network, and administrative documentation.
- Monthly service and security reports; quarterly business reviews; prioritized technology roadmap, budget recommendations and annual IT & cybersecurity questionnaire completion for audit.
- Security awareness training and phishing reporting; incident reports when applicable; backup and restoration test results.
- Contract-end transition assistance and return of Authority data, accounts, configurations, and documentation.

Vendor Qualifications and Submission Requirements

Vendor Qualifications

- Experience serving public-sector, government, authority, nonprofit, or similarly sized organizations.
- Demonstrated experience with Microsoft 365, cybersecurity, cloud backup, networking, and hybrid or remote users.

- Qualified staffing, service desk and escalation model, account management, relevant certifications, and disclosed subcontractors.
- Appropriate cyber liability, technology errors and omissions, commercial general liability, and workers compensation insurance.
- Three references for comparable clients and disclosure of conflicts, relevant litigation, regulatory action, data breaches, or major service disruptions.

Proposal Content

Proposals should be no more than 10 single-spaced pages, excluding resumes, references, insurance documentation, and sample agreements, and should include the following in order:

- Cover letter signed by an authorized representative and executive summary.
- Company profile, qualifications, certifications, project team, and subcontractors.
- Understanding of the Authority's needs and proposed technical and service delivery approach.
- Cybersecurity, Microsoft 365, service-level, escalation, reporting, and strategic planning approach.
- Transition and implementation plan, including assumptions and Authority responsibilities.
- Complete cost proposal identifying recurring, one-time, optional, licensing, labor, travel, pass-through costs, price adjustments, and three-year pricing.
- Three comparable references, proof of insurance, W-9, sample service agreement, proposed terms, exceptions, assumptions, exclusions, and acknowledgment of addenda.

Submission Process

- Submit one searchable PDF proposal by the deadline listed under Key Dates.
- Email proposals to jwilliams@decidedekalb.com with the subject line "Proposal: Managed Information Technology Services."
- Cloud-storage links or email attachments are acceptable. Include the proposer's contact name, email address, and telephone number in the submission email.
- Late or incomplete submissions may be rejected. Clearly identify material claimed as confidential or proprietary and state the legal basis for the designation.

Selection Process

- Qualified submissions will be reviewed and ranked by a selection committee using the published criteria.
- Decide DeKalb may request clarifications, conduct reference checks, invite firms to interviews or demonstrations, or request a best-and-final offer.

- Final scope, service levels, pricing, and contract terms will be negotiated with the selected proposer and remain subject to required approvals.

Administrative Requirements and Reservation of Rights

- The selected vendor must enter into a written agreement acceptable to the Authority, protect Authority information, comply with applicable laws, maintain required insurance, and disclose and manage subcontractors.
- The Authority retains ownership of its data, accounts, configurations, documentation, and paid deliverables. The vendor must provide reasonable transition assistance at contract commencement and termination.
- Decide DeKalb may reject any or all proposals; cancel, modify, or reissue the RFP; waive minor irregularities; request additional information; verify qualifications and references; negotiate scope, price, and terms; accept all or part of a proposal; or make no award.
- Any award is subject to funding, successful negotiations, and required approvals. This RFP may be cancelled at any time before execution of a written agreement.
- Decide DeKalb encourages participation by diverse vendors, including DBE, FBE, and MBE firms.