

REQUEST FOR PROPOSAL

Information Technology Managed Services

Arkansas Development Finance Authority

1 Commerce Way, Suite 602 • Little Rock, AR 72202

adfa.arkansas.gov

RFP Reference Number	ADFA-MSP-2026-001
Issue Date	April 1, 2026
Proposals Due	April 30, 2026
RFP Contact	Jake Bleed, General Counsel jake.bleed@arkansas.gov (501) 682-5927

Section 1: Introduction & Agency Overview

1.1 Purpose

The Arkansas Development Finance Authority (hereinafter "ADFA" or the "Authority"), a public body and instrumentality of the State of Arkansas, is soliciting competitive proposals from qualified Information Technology Managed Services Providers (MSPs) to deliver comprehensive IT support and management services.

This Request for Proposal (RFP) is issued pursuant to ADFA's procurement policies, applicable provisions of the Arkansas Procurement Law (Ark. Code Ann. § 19-11-201 et seq.), and ADFA's enabling statutes. ADFA seeks a single, experienced MSP to serve as its primary technology partner, responsible for the day-to-day management, support, security, and strategic direction of its information technology environment.

1.2 About ADFA

The Arkansas Development Finance Authority was established in 1985 to promote economic growth and community development across Arkansas. ADFA provides affordable financing options for business expansion, affordable housing, infrastructure, public health initiatives, and higher education funding. ADFA operates under the oversight of a Board of Directors composed of the State Treasurer, the Director of the Department of Finance and Administration, and eleven public members appointed by the Governor of Arkansas.

ADFA administers programs across several divisions:

- Housing Development – Low-Income Housing Tax Credits (LIHTC), HOME Investment Partnerships, National Housing Trust Fund, CDBG-Disaster Recovery, Emergency Solutions Grants, and homelessness solutions programs
- First-Time Homeownership and Mortgage Originations, including administration of federally administered programs providing mortgages to home buyers statewide
- Student Loan Administration, including provision of lending opportunities of Arkansas based and related students at institutions of higher education.
- Development Finance – Small Business Guaranty Program, Industrial Development Bond Guaranty, Capital Access Program, Venture Capital and Venture Development Funds
- Finance and Administration – Public Finance (state agency and conduit bond issuance), Private Student Loan programs (through the Arkansas Student Loan Authority), and internal operations

ADFA employs over forty (40) full-time staff at its principal office in Little Rock and administers programs impacting affordable housing, small business growth, and public finance throughout the state. The nature of ADFA's mission — including the management of federally funded programs, bond issuances, and financial data for borrowers and lenders statewide — requires a technology partner with a deep understanding of data security, compliance obligations, and reliable, responsive service delivery.

1.3 Current IT Environment Overview

The following information is provided to assist respondents in scoping their proposals. ADFA will provide additional technical detail during the pre-proposal site visit and to selected finalists under a Non-Disclosure Agreement.

Agency Full Name	Arkansas Development Finance Authority (ADFA)
Principal Office	1 Commerce Way, Suite 602, Little Rock, AR 72202
Website	adfa.arkansas.gov
Parent Organization	The State of Arkansas
Number of Staff	Approximately 40+ full-time employees
Primary OS / Environment	Microsoft Windows 10/11 (enterprise environment)
Productivity Suite	Microsoft 365 (Exchange Online, Teams, SharePoint, OneDrive)
Directory Services	Microsoft Active Directory / Azure AD
Work Model	Primarily on-site; some hybrid/remote capability
Network Infrastructure	On-premises switches, firewall, wireless access points (inventory provided at pre-proposal meeting)
Regulated Data Handled	Federally funded program data (HUD, Treasury), financial/borrower PII, bond transaction records, tax credit program records
Current MSP Status	To be disclosed; transition support from incumbent MSP will be required

1.4 Compliance & Regulatory Context

Due to ADFA’s role as an administrator of federal housing and economic development programs, the selected MSP must demonstrate awareness of and ability to support compliance with applicable regulatory requirements, including but not limited to:

- HUD information security requirements applicable to federally funded housing programs
- IRS requirements related to Low-Income Housing Tax Credit program data and reporting
- Arkansas Department of Finance and Administration IT policies as applicable to state instrumentalities
- NIST Cybersecurity Framework (CSF) or equivalent standards
- Arkansas Freedom of Information Act (Ark. Code Ann. § 25-19-101 et seq.) as it pertains to records maintained on behalf of ADFA
- Generally Accepted Privacy Principles (GAPP) for handling personally identifiable information (PII) of borrowers and program participants
- Banking and servicing of loans, mortgages and student lending as applicable

Respondents with prior experience supporting government agencies, housing finance agencies (HFAs), Community Development Financial Institutions (CDFIs), or similarly regulated entities are strongly preferred.

1.5 Procurement Objectives

ADFA's primary objectives in selecting an MSP are to:

- Ensure reliable, responsive, and professional IT support for all ADFA staff
- Streamline new user provisioning and hardware deployment to support staff onboarding
- Strengthen ADFA's cybersecurity posture, particularly given the sensitivity of program participant data and bond/financial records
- Optimize and administer the Microsoft 365 and cloud environment
- Maintain network infrastructure performance and reliability at ADFA's Little Rock office
- Establish a robust, tested backup and disaster recovery capability
- Engage a long-term, responsive technology partner aligned with ADFA's public mission

Section 2: Eligibility & Local Presence Requirement

2.1 Local Presence Requirement (MANDATORY – Pass/Fail Threshold)

IMPORTANT: This is a mandatory pass/fail threshold requirement. Proposals that do not affirmatively demonstrate compliance with this requirement will be deemed non-responsive and will not be evaluated further, regardless of other qualifications.

ADFA requires that the selected MSP maintain a staffed, physical office or operations center within a one (1) hour normal driving distance of ADFA's principal office at 1 Commerce Way, Suite 602, Little Rock, AR 72202. This geographic requirement is established to ensure the MSP's ability to deploy qualified, on-site technical personnel promptly when remote remediation is insufficient — a capability that is essential to ADFA's operational continuity.

To demonstrate compliance, respondents must include all of the following in their proposal:

1. The full street address of the respondent's nearest staffed office or dispatch location;
2. The estimated normal driving time from that location to 1 Commerce Way, Suite 602, Little Rock, AR 72202 (must not exceed sixty (60) minutes under normal driving conditions);
3. A declaration that qualified technical personnel are based at or regularly dispatched from that location; and
4. Confirmation that the respondent can deploy a qualified technician on-site at ADFA's office within two (2) hours of an on-site support request during normal business hours (8:00 AM – 5:00 PM CST, Monday–Friday, excluding Arkansas state holidays).

Use of subcontractors or third-party field technicians to satisfy this requirement may be considered on a case-by-case basis, provided the primary respondent: (a) discloses the arrangement fully in the proposal;

(b) retains management accountability; and (c) demonstrates that all subcontracted personnel meet the qualifications stated in this RFP. Undisclosed subcontracting arrangements are grounds for disqualification.

2.2 Minimum Organizational Qualifications

2.2.1 Experience

- Minimum five (5) continuous years of operation as a Managed Services Provider as of the RFP issue date
- Demonstrated experience serving government agencies, quasi-governmental or public authority entities, housing finance agencies, CDFIs, or similarly regulated organizations
- At least three (3) active client engagements of comparable size (50–250 users) in Arkansas or an adjacent state (Missouri, Tennessee, Mississippi, Louisiana, Oklahoma, or Texas)

2.2.2 Technical Certifications

Certification / Designation	Status	Notes
Microsoft Solutions Partner (Cloud / Modern Work)	REQUIRED	Proof must be submitted
CompTIA Managed Services (MSPVerify or equivalent)	Preferred	
SOC 2 Type II (MSP’s own infrastructure)	Preferred	Or willingness to undergo
Microsoft Certified: Modern Desktop Administrator	Required (key staff)	At least one named technician
Microsoft Certified: Azure Administrator (AZ-104)	Preferred (key staff)	
NIST 800-171 / CMMC Level 1 Familiarity	Preferred	Relevant to federal program data

2.2.3 Insurance Requirements

The selected MSP shall maintain the following minimum insurance coverage throughout the contract term and provide certificates of insurance prior to contract execution:

- Commercial General Liability: \$1,000,000 per occurrence / \$2,000,000 aggregate
- Technology Errors & Omissions: \$1,000,000 per claim
- Cyber Liability / Data Breach Response: \$1,000,000 per occurrence
- Workers’ Compensation: As required by Arkansas law (Ark. Code Ann. § 11-9-101 et seq.)
- Automobile Liability (if applicable): \$500,000 combined single limit

ADFA shall be named as an additional insured on all applicable policies.

Section 3: Scope of Work & Service Requirements

ADFA requires the services described below. Respondents must clearly indicate in their Technical Proposal (Tab C) whether each service is: (1) included in the base monthly price, (2) available as an optional add-on at additional cost, or (3) not offered. Services are organized into six functional areas.

3.1 IT Help Desk & End-User Support [PRIMARY REQUIREMENT]

The MSP shall serve as the single point of contact for all IT-related issues experienced by ADFA staff. Responsive, courteous, and expert support is critical to ADFA’s daily operations, particularly given time-sensitive program deadlines and loan closing activities.

3.1.1 Help Desk Operations

- 24x7x365 Tier 1 and Tier 2 remote help desk support via phone, email, and web portal
- Formal ticketing system with portal access for ADFA staff and management-level reporting
- Tier 3 escalation path for complex infrastructure and server-level issues
- Dedicated primary account contact(s) familiar with the ADFA environment and programs
- Monthly and quarterly service review meetings with ADFA’s designated IT/administrative contact

3.1.2 Service Level Objectives (SLOs) – Minimum Requirements

Priority	Definition	Response Time	Resolution Target
P1 – Critical	System-wide outage; complete loss of business function	15 minutes	4 hours
P2 – High	Significant impairment; multiple users affected	30 minutes	8 business hours
P3 – Medium	Single-user issue; workaround available	2 business hours	3 business days
P4 – Low	Informational or non-urgent request	4 business hours	5 business days

3.1.3 On-Site Support

- Deploy a qualified technician on-site at 1 Commerce Way, Suite 602, Little Rock, AR within two (2) hours of an on-site support request during normal business hours
- Provide scheduled quarterly preventive maintenance visits at ADFA’s office at no additional charge
- Maintain a documented after-hours escalation path for emergencies requiring on-site presence

3.2 New User Provisioning & Hardware Deployment [PRIMARY REQUIREMENT]

ADFA regularly onboards new employees and periodically deploys or upgrades hardware. The MSP shall manage the full lifecycle of user provisioning and hardware deployment.

3.2.1 New User Onboarding

- Provision Microsoft Active Directory / Azure AD accounts, M365 licenses, and email within one (1) business day of receiving an approved, completed request form
- Configure and deliver a fully imaged, domain-joined, and security-hardened workstation ready for use on the user's first day of employment
- Enroll new users in MFA, configure VPN access, and deploy all ADFA-standard applications
- Provide a brief onboarding IT orientation guide for new staff
- Maintain a documented, ADFA-approved onboarding checklist updated throughout the contract term

3.2.2 Hardware Procurement & Deployment

- Source and procure ADFA-approved hardware (laptops, desktops, monitors, peripherals, printers) at competitive market pricing, leveraging volume licensing or purchasing agreements where available
- Maintain and update a standard ADFA hardware image aligned with current security policies and software standards
- Deliver and configure new workstations on-site at ADFA's Little Rock office
- Maintain an accurate, up-to-date hardware asset inventory register accessible to ADFA management
- Manage manufacturer warranties, hardware lifecycle planning, and end-of-life replacement scheduling; provide written refresh recommendations annually

3.2.3 User Offboarding

- Disable user accounts, revoke all system access, and coordinate hardware recovery within four (4) hours of receiving an approved, completed offboarding request
- Ensure secure data handling, account de-provisioning, and device wiping in compliance with ADFA's data security policies
- Maintain a documented, ADFA-approved offboarding checklist updated throughout the contract term

3.3 Cybersecurity & Endpoint Protection

Given ADFA’s management of federally funded programs, financial records, borrower PII, and bond transaction data, cybersecurity is a top-tier requirement. The MSP must demonstrate mature, proactive security capabilities.

3.3.1 Endpoint Security

- Deploy and manage enterprise-grade Endpoint Detection and Response (EDR) on all ADFA-managed devices
- Maintain real-time antivirus, anti-malware, and anti-ransomware protection
- Manage automated patch deployment for operating systems and third-party applications (critical patches within 24–48 hours of release; routine patches per defined monthly schedule)
- Configure and enforce host-based firewall and device compliance policies via Microsoft Intune

3.3.2 Identity & Access Management

- Deploy and manage Multi-Factor Authentication (MFA) across all ADFA accounts and systems
- Administer Azure AD Conditional Access policies appropriate for ADFA’s hybrid environment
- Manage privileged access, Role-Based Access Control (RBAC), and least-privilege enforcement
- Implement and maintain Single Sign-On (SSO) where feasible

3.3.3 Security Monitoring & Incident Response

- Provide 24x7x365 security event monitoring (SIEM/SOC or equivalent managed detection and response)
- Deliver a documented, ADFA-tailored Incident Response Plan within 90 days of contract commencement
- Conduct semi-annual internal and external vulnerability assessments; provide written reports with prioritized remediation recommendations to ADFA leadership
- Administer a security awareness training platform (KnowBe4 or equivalent) for all ADFA staff, including annual phishing simulation campaigns

3.3.4 Regulatory Compliance Support

- Assist ADFA in aligning IT practices with NIST CSF, CIS Controls, and applicable HUD/federal program information security requirements
- Support ADFA during audits by HUD, IRS, state oversight agencies, or ADFA’s Board of Directors; provide documentation as required
- Advise ADFA on emerging compliance obligations relevant to housing finance agencies and bond-issuing public authorities
- Respond to and accommodate requests for information from internal and external auditors.

3.4 Microsoft 365 & Cloud Services Management

- Administer and optimize ADFA’s Microsoft 365 tenant (Exchange Online, SharePoint Online, Teams, OneDrive, Intune, Defender for Business)
- Manage M365 licensing, user assignments, and license compliance to prevent overprovisioning
- Configure and maintain Microsoft Teams for ADFA staff collaboration and external partner communication
- Administer SharePoint Online site collections and OneDrive storage policies
- Manage Microsoft Intune for Mobile Device Management (MDM) and enforcing device compliance policies
- Provide ongoing M365 optimization recommendations as Microsoft releases new features
- Assist with any future cloud migrations or Azure workload transitions as ADFA’s needs evolve

3.5 Network Infrastructure Management

- Provide 24x7x365 proactive monitoring of all network components at ADFA’s Little Rock office: switches, routers, firewall, wireless access points, and internet circuits
- Manage firewall rule sets, security policy updates, and firmware/software patches for network hardware
- Administer and maintain VPN for remote staff access
- Monitor internet circuit performance and coordinate with ISP on outages or performance degradation
- Respond to network outages per SLOs defined in Section 3.1.2
- Provide network capacity planning guidance and infrastructure refresh recommendations
- Produce and maintain network topology documentation (initial documentation due within 60 days of contract start; updated annually or upon material changes)

3.6 Backup & Disaster Recovery

- Implement and manage a cloud-hosted or hybrid backup solution for all critical ADFA data, systems, and servers
- Define and commit to Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) approved by ADFA; proposed targets must be included in the respondent’s proposal
- Execute automated nightly backups with off-site or cloud redundancy; no single point of failure in backup chain
- Perform and document quarterly backup restoration tests; deliver written test results to ADFA management
- Deliver a documented Business Continuity and Disaster Recovery (BCDR) Plan tailored to ADFA’s operations within 90 days of contract commencement
- Facilitate an annual BCDR tabletop exercise with ADFA leadership

3.7 Strategic IT Planning & Advisory (vCIO Services)

- Assign a named Virtual CIO (vCIO) or senior strategic account manager as ADFA's primary technology advisor
- Conduct semi-annual strategic IT reviews with ADFA's Executive Director or designee to assess the technology roadmap and budget planning
- Deliver a written IT Technology Roadmap within 120 days of contract commencement, updated annually
- Advise ADFA on technology relevant to housing finance, public bond administration, and state agency environments
- Assist ADFA in developing and maintaining IT policies, acceptable use policies, and data governance procedures

Section 4: Contract Terms & Conditions

4.1 Contract Term

The initial contract term shall be three (3) years commencing upon execution of the agreement, with ADFA retaining the option to renew for up to two (2) additional one-year periods (total potential term: five years), subject to satisfactory MSP performance and ADFA Board of Directors budget approval. Annual price increases, if any, shall be capped at the lesser of three percent (3%) or the annual change in the U.S. Bureau of Labor Statistics Consumer Price Index (CPI-U) for the South Region.

4.2 Pricing Structure

ADFA expects a per-user, per-month (PUPM) or flat monthly all-inclusive pricing model that provides cost predictability and eliminates surprise billing. All pricing must be comprehensive for the services proposed. Any services not included in the base price must be explicitly itemized in Attachment A with their applicable rate.

4.3 Performance Standards & Remedies

The MSP shall meet all SLOs defined in Section 3.1.2. ADFA reserves the right to require written root cause analysis for recurring P1 or P2 failures. Chronic failure to meet SLOs (defined as three or more monthly SLO failures of the same priority level in any rolling 90-day period) shall constitute a material breach subject to the remedies in Section 4.4.

4.4 Termination

ADFA reserves the right to terminate the contract for cause upon thirty (30) days written notice if the MSP materially breaches its obligations and fails to cure such breach within the notice period. ADFA may terminate for convenience upon sixty (60) days written notice. Upon any termination, the MSP shall cooperate fully with transition to a successor provider, including delivering all ADFA data, credentials,

network documentation, and administrative access within fifteen (15) business days at no additional charge.

4.5 Data Ownership, Confidentiality & Security

All ADFA data, configurations, credentials, documentation, system access, and intellectual property created or managed under this contract remain the exclusive property of ADFA. The MSP shall execute a Data Processing Agreement (DPA) and, if applicable, a Business Associate Agreement (BAA) satisfactory to ADFA prior to contract commencement. The MSP shall not use, disclose, sell, or retain ADFA data for any purpose other than contracted service delivery. Any breach of this provision shall be deemed a material breach.

4.6 Applicable Law & Venue

This contract shall be governed exclusively by the laws of the State of Arkansas. All disputes shall be resolved in Pulaski County, Arkansas. The MSP shall comply with all applicable federal and state law, including the Arkansas Freedom of Information Act (Ark. Code Ann. § 25-19-101 et seq.) as it applies to records maintained on behalf of ADFA, a public body of the State of Arkansas.

4.7 Background Screening

All MSP personnel assigned to ADFA accounts or granted access to ADFA systems, facilities, or sensitive data shall undergo criminal background screening consistent with Arkansas state standards prior to assignment. ADFA reserves the right, in its sole discretion, to deny access to any individual. The MSP shall certify annually that all assigned personnel have passed background screening.

4.8 Subcontracting

Any subcontracting arrangements must be disclosed in the proposal and approved by ADFA in writing prior to commencement. The prime MSP remains solely responsible for all subcontractor performance and compliance with this contract. ADFA shall have the right to require removal and replacement of any subcontractor.

Section 5: Proposal Submission Requirements

5.1 Proposal Format & Delivery

Proposals must be submitted electronically in PDF format to the RFP Contact identified on the cover page by the deadline. The email subject line must read exactly: "ADFA-MSP-2026-001 Proposal – [Respondent Company Name]". Proposals received after the deadline will not be considered under any circumstances. No faxed, mailed, or hand-delivered proposals will be accepted.

Proposals must be organized in the following order with clearly labeled tabs:

Tab	Section	Required Contents
Cover	Cover Letter	One-page letter on company letterhead, signed by an authorized representative. Must affirm compliance with all eligibility requirements, including local presence.
A	Company Profile	Legal entity name, years in operation, ownership structure, all office addresses, total staff count, organizational chart, and local presence documentation (per Section 2.1).
B	Qualifications & Certifications	All certifications and Microsoft partnership documentation; key personnel résumés (including named vCIO and lead technician); current certificates of insurance.
C	Technical Approach	Detailed response to each service area in Section 3. Identify tools, platforms, monitoring systems, ticketing system, and methodologies for each area. State whether each service is included in base price or is an add-on.
D	Client References	Three (3) completed reference forms per Section 6.7. Government, quasi-governmental, or regulated entity references strongly preferred.
E	Transition Plan	Proposed onboarding timeline and methodology; approach to data migration, documentation capture, and coordination with incumbent MSP; staff communication plan.
F	Fee Schedule	Complete Attachment A with all-inclusive base pricing, optional service rates, hardware markup policy, and project/professional services hourly rates.
G	Vendor Questionnaire	Written responses to all questions in Section 6. Incomplete responses will be deemed non-responsive.
H	Exceptions	Any requested exceptions to RFP terms, scope, or contract language. Proposals with material exceptions may be disqualified at ADFA's discretion.

5.2 Procurement Timeline

Milestone	Target Date
RFP Issue Date	April 1, 2026
Optional Pre-Proposal Site Visit at ADFA’s Office	Week of April 13, 2026
Deadline for Written Questions from Respondents	April 30, 2026 at 5:00 PM CST
ADFA Issues Written Responses / Addendum	May 7, 2026
Proposal Submission Deadline	April 30, 2026
Anticipated Award Notification	May 22, 2026
Anticipated Contract Execution	May 27, 2026
Anticipated Service Commencement	June 1, 2026

5.3 Questions & Communications

All questions must be submitted in writing by email to the RFP Contact by the deadline above. Verbal inquiries will not be addressed. Responses to all written questions will be issued simultaneously to all known respondents by addendum and posted to ADFA’s website at adfa.arkansas.gov/resources/requests-for-proposals/. No other ADFA personnel may be contacted regarding this RFP; unsolicited contact may result in disqualification.

5.4 Pre-Proposal Site Visit

A non-mandatory but strongly encouraged pre-proposal site visit will be held at ADFA’s office, 1 Commerce Way, Suite 602, Little Rock, AR 72202. Attendees will have an opportunity to inspect the physical office environment, review network infrastructure, and ask questions of ADFA staff.

Section 6: Vendor Questionnaire

Respondents must provide complete, specific written responses to all questions below. Responses of "to be determined," "available upon request," or equivalent will not be accepted and will render the proposal non-responsive. Responses must be organized by section number in Tab G of the proposal.

6.1 Company & Local Presence

5. Provide the full legal name, entity type (LLC, Inc., S-Corp, etc.), year founded, and headquarters address of your organization.
6. Identify the specific office address from which you would dispatch technicians to ADFA. Provide the estimated driving time to 1 Commerce Way, Suite 602, Little Rock, AR 72202 under normal conditions. Confirm this location is staffed with qualified technical personnel.

7. How many full-time employees does your organization employ total, and how many are dedicated to service delivery roles (technicians, engineers, vCIOs, account managers)?
8. Have you served any Arkansas state agencies, quasi-governmental entities, housing finance agencies, or similarly regulated organizations? If so, please describe (without identifying confidential client information).
9. Has your organization undergone any ownership changes, mergers, acquisitions, or restructuring in the past three (3) years? If yes, explain.

6.2 Help Desk & On-Site Support

10. Describe your help desk platform, ticketing system, and escalation procedures in detail. What is the name of your ticketing system and does ADFA staff get portal access?
11. What are your standard help desk hours? How do you handle after-hours P1 and P2 incidents?
12. Specifically, how do you guarantee on-site response within two (2) hours from your local dispatch location for emergency on-site requests at ADFA's Little Rock office?
13. What is your current average ticket resolution time by priority level across clients of similar size?
14. What client-facing reports does ADFA receive, at what frequency, and through what mechanism?

6.3 New User Provisioning & Hardware Deployment

15. Walk through your end-to-end new user onboarding process step by step, from receipt of a completed request to the user's first day.
16. How do you manage standard workstation imaging, software deployment, and hardware provisioning?
17. What hardware procurement relationships (e.g., Dell, HP, Lenovo) or state contract vehicles (e.g., APSCO, AR state contracts) do you leverage that could benefit ADFA?
18. Describe your asset inventory management system. How does ADFA leadership access current inventory data?
19. What is your standard turnaround time for deploying a new workstation from receipt of an approved request?

6.4 Cybersecurity

20. What EDR/XDR platform do you deploy and manage? Do you maintain an in-house Security Operations Center (SOC) or use a third-party SOC? Describe your 24x7 monitoring capability.
21. Describe your patch management process including timelines for critical, high, and routine patches.
22. What security awareness training platform do you use? How do you measure effectiveness and report results to clients?
23. Has any client of your organization experienced a ransomware attack or significant data breach? Without identifying the client, describe how the incident was handled and what the outcome was.
24. What experience do you have supporting organizations that handle federally funded program data, borrower PII, or financial records subject to federal oversight (e.g., HUD, IRS, Treasury)?

6.5 Microsoft 365 & Cloud

- 25. Describe your Microsoft Solutions Partner designation and your team’s specific M365 administration experience.
- 26. How do you manage Microsoft Intune for device compliance in a hybrid (on-premises AD + Azure AD) environment?
- 27. How do you approach M365 license optimization to ensure ADFA is not paying for unused licenses?

6.6 Backup & Disaster Recovery

- 28. What backup platform do you recommend and why? Is it cloud-hosted? What cloud provider does it use?
- 29. What RTO and RPO targets do you propose for an organization of ADFA’s size and profile? What factors drive those targets?
- 30. Describe your backup testing process. How are results documented and communicated to ADFA leadership?

6.7 Client References

Provide three (3) client references. Government agencies, quasi-governmental entities, housing finance authorities, CDFIs, or Arkansas-based organizations are strongly preferred. ADFA will contact references during the evaluation process.

Field	Reference 1	Reference 2	Reference 3
Organization Name			
Contact Name & Title			
Phone & Email			
Approx. User Count			
Services Provided			
Contract Start Date			
Government / Regulated?	Yes / No	Yes / No	Yes / No

Section 7: Evaluation Criteria & Selection Process

7.1 Evaluation Process

Proposals will be evaluated by an Evaluation Committee appointed by ADFA’s Executive Director. The process will proceed through the following phases:

- 31. Phase 1 – Threshold Review: Verify local presence requirement (Section 2.1) and minimum qualifications (Section 2.2). Pass/fail. Non-compliant proposals are eliminated without further review.
- 32. Phase 2 – Technical Scoring: Proposals passing Phase 1 are scored against the weighted criteria below by the Evaluation Committee.
- 33. Phase 3 – Reference Verification: ADFA will contact references for top-scoring respondents.
- 34. Phase 5 – Best and Final Offer (BAFO): ADFA may invite finalists to submit revised pricing.
- 35. Phase 6 – Award & Contract Negotiation: ADFA reserves the right to negotiate with the top-ranked respondent prior to contract execution and Board approval.

7.2 Weighted Scoring Criteria

Evaluation Category	Key Factors	Weight
Local Presence & On-Site Availability	Office location, confirmed drive time, on-site staffing commitment, 2-hour response guarantee	Pass/Fail + 15%
Technical Approach & Service Capability	Scope comprehensiveness, toolset quality, SLO commitments, BCDR approach, M365 depth	30%
Relevant Experience & Qualifications	Years in operation, government/regulated sector experience, certifications, key staff credentials	20%
Cybersecurity Capabilities	EDR/SOC maturity, identity management, federal compliance awareness, incident response history	15%
Pricing & Total Cost of Ownership	Competitiveness, transparency, all-in pricing vs. hidden fees, hardware markup disclosure	15%
Client References	Satisfaction levels, similarity of engagements, government/regulated entity references	5%
TOTAL		100%

ADFA reserves the right to award to the respondent offering the best overall value to ADFA and the State of Arkansas, which may not be the lowest-priced proposal. ADFA further reserves the right to reject any or all proposals, waive minor informalities, or reissue the RFP in its sole discretion.

Section 8: General Conditions & Disclaimers

- This RFP does not constitute a contract, a commitment to contract, or authorization to proceed with any work.
- ADFA reserves the right to modify, suspend, or cancel this RFP at any time without liability to any respondent.
- All proposals become property of ADFA upon submission and may be subject to public disclosure under the Arkansas Freedom of Information Act (Ark. Code Ann. § 25-19-101 et seq.) following contract award.
- Respondents bear all costs of proposal preparation; ADFA will not reimburse any costs regardless of outcome.
- Any material misrepresentation in a proposal shall be grounds for immediate disqualification and may be referred to appropriate authorities.
- ADFA may conduct independent investigations of any respondent’s background, financial stability, litigation history, or reputation.
- Proposals must remain valid and irrevocable for ninety (90) days from the submission deadline.
- Contract award is subject to approval by the ADFA Board of Directors.
- Issuance of this RFP does not guarantee that a contract will be awarded or that any particular MSP will be selected.

Attachment A: Fee Schedule

Complete all applicable fields. All pricing must be in U.S. dollars and reflect the three-year initial contract term. For per-user pricing, state the assumed user count clearly. ADFA’s estimated current user base is approximately 40–60 users; respondents should price for 50 users and provide a per-user rate for scaling above or below that baseline.

Respondent assumes _____ users for the purposes of per-user pricing above.

Part 1: Base Managed Services (Monthly)

Service Component	Per User / Month	Flat Monthly	Annual Total
Help Desk (24x7x365, Tiers 1–3)	\$	\$	\$
On-Site Support (scheduled & reactive)	\$	\$	\$
New User Provisioning & Hardware Deployment	\$	\$	\$
Endpoint Protection (EDR / AV / Patch Mgmt)	\$	\$	\$
M365 / Azure AD Administration	\$	\$	\$
Network Infrastructure Monitoring & Management	\$	\$	\$

Service Component	Per User / Month	Flat Monthly	Annual Total
Backup & Disaster Recovery (cloud-hosted)	\$	\$	\$
Security Awareness Training Platform	\$	\$	\$
vCIO / Strategic Advisory Services	\$	\$	\$
TOTAL BASE MONTHLY FEE		\$	\$

Part 2: Optional & Additional Services

Service	Rate	Unit
After-Hours / Emergency On-Site (unscheduled)	\$	per hour
Project / Professional Services (standard rate)	\$	per hour
Additional Vulnerability Assessment	\$	per assessment
Hardware Markup Above Actual Cost		%
M365 Licensing Pass-Through Markup		% or \$0
Additional User (above baseline)	\$	per user / month
Other (specify):	\$	

Proposed RTO: _____ Proposed RPO: _____

Annual price escalation cap (confirm): _____ % or CPI-U South Region, whichever is less.

END OF REQUEST FOR PROPOSAL

Arkansas Development Finance Authority • 1 Commerce Way, Suite 602 • Little Rock, AR 72202 • adfa.arkansas.gov