FAMILY ELDERCARE — REQUEST FOR PROPOSAL

Co-Managed Information Technology Services

Issued By	Key Dates	
Family Eldercare 1700 Rutherford Lane, Austin, TX 78754 www.familyeldercare.org	Issued: Vendor questions due: Proposals due: Anticipated contract start:	September 3, 2026 September 22, 2026 October 23, 2026, 5:00 PM CT February 1, 2027

1. Introduction

Family Eldercare ("the Organization") is soliciting proposals from qualified managed service providers (MSPs) to deliver **co-managed Information Technology services** in partnership with the Organization's internal IT staff. The Organization currently contracts with a vendor under an agreement expiring January 31st, 2027, and is conducting a competitive evaluation to improve operational efficiency, strengthen service delivery, and reduce costs in alignment with its mission-driven goals.

This is a co-managed engagement: the Organization's IT & Data Manager provides Tier 1/Tier 2 end-user support, equipment procurement, asset tracking, and vendor management for business applications. The selected MSP will provide infrastructure management, network and security operations, Tier 3 escalation support, backup and disaster recovery, and supplemental help desk coverage as described in Section 3.

Contract Term: The Organization anticipates an initial contract term of three (3) years commencing February 1st, 2027. The Organization may terminate the agreement for convenience upon ninety (90) days' written notice at any time after the first twelve (12) months of the term, without early-termination fee or penalty; the credential and transition obligations in Section 3.1 apply upon written notice of any expiration or termination. Respondents may amortize one-time onboarding costs into monthly fees but must itemize them in the pricing breakdown (Section 6) so that any unamortized balance can be settled upon early termination. No unamortized onboarding balance is owed on termination for cause or vendor breach.

2. Background

- **Organization:** Community-based nonprofit providing aging, housing, and social support services to seniors and adults with disabilities across Central Texas; over 15,000 clients served annually.

- **Staff:** Approximately 110 employees across a primary office, two residential communities, and eight service coordination and HUD Permanent Supportive Housing sites, with a hybrid remote work structure.
- **Internal IT:** One full-time IT & Data Manager, responsible for Tier 1/Tier 2 help desk support across all sites, endpoint procurement and asset lifecycle management, device provisioning, user onboarding and offboarding, administration of line-of-business applications, and day-to-day management of print, telephony, and internet service vendors. The full division of responsibility between the MSP and the Organization's IT staff is set out in Sections 3.1 and 3.5, respectively.
- **Environment summary:** ~110 users on ~120 Windows 11 Pro Dell workstations, Microsoft 365 Business Premium; one on-premises Dell T360 host running two VMs (domain controller; file server pending decommission upon SharePoint migration); one main office network (UniFi) and two satellite networks (UniFi & Meraki). Full detail in **Appendix A**.
- **Funding:** This procurement is funded in part by federal grant funds; see Section 10.

3. Scope of Services

Appendix B — Responsibility Matrix presents the division of responsibility described in this Section 3 in a one-page summary provided for clarity; Section 3 controls in the event of any conflict.

3.1 MSP Responsibilities (Base Scope)

- **Network & Server Administration**: Monitoring, maintenance, performance tuning, and patching of servers, firewalls, switches, and wireless infrastructure across all named sites listed in Appendix A, §A.1. At Pecan Gardens and Lyons Gardens, MSP responsibility extends to the resident and guest network infrastructure and its segmentation from staff VLANs; individual end-user support for residents, visitors, and volunteers is outside the scope of this engagement.
- **Cybersecurity Operations**: EDR/XDR; email security; firewall management; security monitoring and incident response; and adherence to applicable data protection standards (NIST CSF; HIPAA standards are applied organization-wide). The MSP must verify and maintain BitLocker full-disk encryption on all Organization workstations, with recovery keys escrowed and accessible to the Organization, and must report any non-compliant device in regular service reporting.
- **Backup & Disaster Recovery**: Managed BDR across three data classes:
    - on-premises virtual machines,
    - Microsoft 365 data (Exchange Online, SharePoint, OneDrive, and Teams), and

    - line-of-business snapshot exports from Bonterra Apricot Core and MIP Cloud on a quarterly cadence.

  Each data class is assigned documented retention policies, defined RPO/RTO commitments, and annual restore verification appropriate to the data class (see Appendix A, §A.8). The Organization does not currently hold a third-party Microsoft 365 backup solution; proposals must recommend one, state its RPO and retention, and price it as a discrete line item.

- **Firewall & BDR Provisioning**: The incumbent's main-office firewall (Sophos XGS 126) and the BDR appliance for on-premises VMs are vendor-owned equipment that will be returned at contract end. Proposals must include provisioning of a replacement firewall and BDR solution at cutover, whether as purchased hardware, HaaS, or an equivalent model, with pricing clearly itemized. Because the main-office remote-access VPN (Sophos Connect; see Appendix A, §A.4) is provided by the incumbent firewall, the replacement firewall must include an equivalent remote-access VPN for staff, and the Transition Plan (Section 5) must address migration of VPN clients on all affected workstations.
- **Tier 3 Support & Escalations**: Escalation path for issues beyond internal Tier 1/Tier 2 capability. Proposals must specify a monthly block-hour allotment included in the base fee, whether unused hours roll over, and hourly rates for overage.
- **Group Policy, Identity & VPN Administration**: Including support for planned initiatives (Entra ID maturation, SSPR, Intune evaluation; see Appendix A, §A.8).
- **Strategic IT Guidance**: Technology reviews at least twice annually, budgeting support, and roadmap collaboration with the IT & Data Manager.
- **Credential & Environment Ownership**: The Organization retains sole ownership of its Microsoft 365 tenant, domain registrations, software licenses, and network equipment configurations. All administrative credentials must be documented in a repository accessible to the IT & Data Manager throughout the engagement; no credential may be held exclusively by the MSP. Upon written notice of expiration or termination for any reason, the MSP must deliver complete environment documentation, configuration exports, and all administrative credentials within ten (10) business days, and provide reasonable transition cooperation to a successor provider.

3.2 Supplemental Help Desk Coverage (Priced Separately)

Qualified MSPs must be able to provide on-demand Tier 1/Tier 2 help desk coverage for all Organization users during absences of the IT & Data Manager. This will include approximately 20 planned days (160 hours) per year, activated with 24–48 hours' notice, plus occasional unplanned absences (same-day activation, best effort; proposals must describe how quickly same-day coverage can begin).

During these coverage periods only, supplemental support extends to first-line coordination assistance for the Organization's wireless mobility services, internet services, managed print services, and Nextiva VoIP and virtual fax services, including vendor liaison and ticket escalation. These services are otherwise administered by the IT & Data Manager and are outside MSP base scope under Section 3.1.

Pricing must be quoted as described in Section 6, both as (a) an annual retainer covering a 160-hour pool, billed in twelve equal monthly payments, and (b) a standalone hourly rate.

3.3 Service Levels (Minimums)

For purposes of this section:

- ***Business Hours*** are 8:00 AM to 5:00 PM Central Time, Monday through Friday, excluding Organization holidays.
- ***Discovery*** means the earlier of (a) the Organization's report of an issue to the MSP, or (b) the MSP's own detection of an issue through monitoring, tooling, or staff observation.
- ***Acknowledgment*** means substantive response by a technician to the originator of a ticket, affected users, and/or to the IT & Data Manager, as appropriate; an automated ticket receipt does not constitute Acknowledgment.
- ***Incident Notification*** is a separate obligation owed to the Organization irrespective of Acknowledgment, and is not satisfied by ticket updates, dashboard entries, or portal notifications. An Incident Notification is warranted in the case of Critical Issues, and is owed equally to every recipient on the Incident Notification List—the IT & Data Manager and designated executive recipients—by the method and with the content specified under Critical Issues below.
- ***Resolution*** means the affected service has been restored to normal operation and, for Critical and High-priority Issues, that root cause has been identified and a corrective fix implemented or scheduled to prevent recurrence. Resolution is confirmed by the Organization; closure of a ticket by the MSP does not by itself constitute Resolution.

Critical Issues

An Incident Notification is required within four (4) hours of Discovery, at any hour, including outside business hours, for the following issues:

1. **Security Incident:** Any confirmed or reasonably suspected security incident, including unauthorized access to Organization systems or data, credential compromise, business email compromise, or ransomware or other destructive malware.
2. **PHI Breach:** Any event that may constitute a breach of protected health information or other regulated data.
3. **Outages:** Any network, server, or service outage affecting the Organization as a whole, or affecting any residential community site, expected to exceed four (4) hours.
4. **Data Loss:** Any data loss, corruption, or failed verification of backup data.

It is understood that the details of an Incident Notification are expected to be incomplete, but the MSP must not delay Incident Notification pending confirmation of scope, cause, or attribution.

Critical Issues are expected to be worked continuously until Resolved. For Critical Issues that cannot be resolved remotely, on-site response at the main office (1700 Rutherford Ln.) or designated residential communities (Pecan Gardens and Lyons Gardens) is expected by the end of the next business day.

Recipients. The Organization will maintain and provide a current Incident Notification List identifying the IT & Data Manager and designated executive recipients. The MSP must notify all listed recipients of any Critical Issue and must update the list in its own systems within five (5) business days of written change.

Method. Incident Notification must be delivered by phone call or text message to the numbers on the Incident Notification List, with written confirmation to follow within 24 hours by a channel not dependent on the Organization's Microsoft 365 environment.

Content. Initial notification must state, to the extent known: what was discovered, when and how it was discovered, systems or data potentially affected, actions taken or underway, whether the MSP has taken immediate action required to contain an active security incident, and the name and direct contact of the MSP incident lead.

Written report. A written incident report is due within five (5) business days of Discovery for each Critical Issue, covering timeline, root cause, remediation completed and planned, and recommendations. If root cause is undetermined, an interim report is due on that schedule with a stated date for the final.

Continuity. These obligations apply regardless of whether supplemental help desk coverage under Section 3.2 is active, and regardless of the availability of the IT & Data Manager.

High-priority Issues

An Acknowledgment is required within two (2) Business Hours of Discovery for High-priority Issues.

A High-priority Issue is one that stops work for a workgroup, an entire site, or a business-critical system, or that stops work for an individual user with no available workaround, but that does not meet a Critical threshold above. Examples include loss of internet, wireless, or VPN connectivity at a single site; multiple users unable to reach the file server, Bonterra Apricot Core, or MIP Cloud; mail flow failures or delays affecting more than one mailbox; and an account lockout or unbootable workstation that leaves a user unable to perform their work.

Standard Issues

An Acknowledgment is required within four (4) Business Hours of Discovery for Standard Issues.

A Standard Issue degrades service for one or a few users, or for a non-critical system, where a workaround exists or normal work can otherwise continue. Examples include a workstation

unable to print or reach a mapped drive; docking station, peripheral, or Teams audio and video problems; a single mailbox, calendar, or file permission problem; and a device performing poorly but still usable.

Routine Requests

An Acknowledgment is required within one (1) business day of Discovery for Routine Requests.

A Routine Request is a planned request for service rather than a service failure. Examples include software installation and licensing requests; distribution list, shared mailbox, and permission changes; equipment moves and peripheral setup; and requests for reporting, documentation, or a scheduled maintenance window.

Outside Business Hours, including weekends and Organization holidays, all classes other than Critical Issues are acknowledged on the next business day.

Where the appropriate class is unclear at Discovery, the MSP must apply the more urgent class, subject to reclassification by agreement with the IT & Data Manager. During coverage periods under Section 3.2, the Acknowledgment commitments in this section apply to end-user tickets received directly by the MSP.

Routine on-site work is scheduled as needed; no standing on-site cadence is required.

Vendors must state their standard SLA tiers, target Resolution times by issue class, escalation thresholds, after-hours and on-call coverage arrangements, and any uptime guarantees, and must state whether after-hours coverage is included in the base monthly fee or billed as a surcharge, with rates.

3.4 Project Work

Project work—e.g., SharePoint migration, Intune deployment, hardware refresh—is outside base scope. Project work may be quoted separately by the MSP solely at the Organization's request; proposals must state project hourly rates by engineer level.

3.5 Organization Responsibilities (Retained by Internal IT)

The following functions are performed by the Organization's IT staff and are outside MSP base scope except as expressly provided in Section 3.2. Respondents should assume this division of responsibility when scoping and pricing.

- **Tier 1/Tier 2 End-User Support**: First-line intake, triage, and resolution of end-user issues for all staff and sites, with escalation to the MSP under Section 3.1. First-line assistance for help desk support transfers to the MSP only during coverage periods under Section 3.2.
- **Endpoint Procurement & Asset Lifecycle**: Specification, purchase, warranty administration, and inventory of workstations and mobile devices, including the three-year refresh cycle described in Appendix A, §A.2.

- **Device Provisioning & User Lifecycle**: Imaging and deployment of workstations, account creation, onboarding and offboarding, and Microsoft 365 license assignment. The MSP is expected to support automation of these workflows as part of the Intune evaluation described in Appendix A, §A.8.
- **Line-of-Business Application Administration**: Administration of and vendor liaison for Bonterra Apricot Core, MIP Cloud, Nextiva VoIP and virtual fax, Spectrum internet, GFiber internet, Astound internet, AT&T internet and wireless mobility, and managed print services (Appendix A, §A.1 and §§A.6–A.7). First-line assistance for VoIP/vFax, internet and wireless mobility, and print transfers to the MSP only during coverage periods under Section 3.2.
- **Vendor & Contract Management**: Management of internet service, print, telephony, and business-application vendors, including service escalation and renewal decisions.
- **Change Authorization**: Approval of infrastructure changes, security exceptions, and project scopes prior to MSP execution. The MSP may not implement material configuration changes to the Organization's environment without the IT & Data Manager's authorization, except where immediate action is required to contain an active security incident.
- **Environment & Credential Ownership**: Administration of the Organization's Microsoft 365 tenant, domain registrations, and license inventory, and maintenance of the shared credential repository required under Section 3.1.
- **Coordination & Site Access**: Organization liaison for the MSP; scheduling of physical site access at the locations listed in Appendix A, §A.1; and user communication for maintenance windows.
- **Budget & Cost Allocation**: IT budget development with MSP input under Section 3.1, and cost allocation reporting, including the Lyons Gardens network administration line item required for HUD (see Section 6).

Respondents may propose shifting any function above into MSP scope where doing so would improve service delivery and/or reduce total cost; any such proposal must be priced as a separate, clearly identified line item.

All services must be performed in accordance with applicable local, state, and federal regulations, including cybersecurity and privacy requirements.

4. Minimum Vendor Qualifications

Proposals will not be evaluated unless the respondent affirms and, where indicated, documents:

- **Active SAM.gov Registration:** no current debarment, suspension, or exclusion (2 CFR Part 180).
- **Commercial General Liability Insurance**: at minimums of $1M per occurrence / $2M aggregate (certificate required; final limits subject to confirmation during contracting)

- **Cyber Liability/Errors & Omissions Insurance:** at minimums of $1M per occurrence / $2M aggregate (certificate required; final limits subject to confirmation during contracting)
- **Workers' Compensation:** as required by Texas law
- **Years in Operation:** at minimum three (3) years of continuous operation as a managed service provider.
- **On-site Capability:** Demonstrated capacity to provide on-site support within the Austin metropolitan area within the response times in Section 3.3.
- **HIPAA-Ready:** Willingness to execute a HIPAA Business Associate Agreement in the Organization's form as a condition of award.
- **Criminal Background Screening:** provide proof or permit criminal background screening of all personnel expected to retain administrative access to Organization systems and/or physical access to Organization facilities.

Questions regarding these qualifications should be directed by email to the point of contact outlined in Section 8.

5. Proposal Requirements

Proposals, including all pricing, must remain valid for one hundred twenty (120) days following the submission deadline. Proposals are limited to 15 pages excluding pricing details, appendices, and certifications; 11pt Arial or Times New Roman, standard margins.

Proposals must be submitted as a single PDF and include:

- **Company Overview**: Legal entity name, years in business, size, and experience with nonprofit organizations.
- **Approach to Co-Managed Service Delivery**: Methodology, staffing structure, SLAs offered, escalation procedures, and specific experience working alongside internal IT staff. Proposals must confirm that the Organization's IT & Data Manager will be granted standing access to the MSP's remote-access tooling (and, where applicable, ticketing platforms) consistent with the co-managed model. Proposals must identify which security and management tools (RMM, ticketing, remote access, EDR/XDR, email security, backup, documentation) are included in the base fee, whether licenses are held in the MSP's name or the Organization's, and how each tool is transitioned or terminated at the end of the engagement.
- **Pricing Model**: A complete cost proposal in the form and detail required by Section 6.
- **References**: At least three (3) clients served within the last three years, preferably nonprofits and/or co-managed engagements. References should note one or more of the following categories for which services were provided to clients: help desk support (timely

& proficient), knowledge of M365 administration, proactive security monitoring or tightening, implementation/onboarding process, and overall performance.

- **Compliance & Certifications**: Documented compliance with relevant IT security standards (e.g., SOC 2, HIPAA, NIST CSF); include copies or attestations.
- **Transition Plan**: Detailed onboarding plan, including: approach to credential and administrative-access handoff from the incumbent; provisioning and cutover of replacement firewall and BDR (Section 3.1); timeline; and risk mitigation. **Note:** the Organization's current agreement restricts third-party discovery of its network prior to contract award; vendor evaluation will rely on the documentation in this RFP and Appendix A, with hands-on discovery beginning during the onboarding period following contract execution with the selected vendor.

6. Pricing & Cost Proposal

Pricing must be submitted in the form and detail required by this section. Respondents may add supporting detail but must not omit a required element; an incomplete pricing submission may be found non-responsive.

Pricing forms and tables do not count against the page limit stated in Section 5.

- **Total Three-Year Cost of Ownership**: A single figure covering the full three-year term described in Section 1, itemized by contract year. This figure is the input to the cost scoring formula in Section 7 and must include all recurring fees, tool licensing included in the base fee, Tier 3 block hours, supplemental coverage at the volumes stated in Section 3.2, and any other recurring or one-time costs, whether standalone or amortized into monthly fees, except unplanned same-day coverage activations, which are excluded per the Supplemental Help Desk Coverage bullet below.
- **Monthly Base Fee**: Components of the base fee, the user and device counts assumed, whether pricing is per-user, per-device, or flat, the tools included per Section 5, and what changes to the environment would change the base fee.
- **Rate Card**: Hourly rates by engineer level and time of day, including after-hours and holiday rates, whether after-hours work is included in the base fee or billed as a surcharge as required by Section 3.3, and minimum billing increments.
- **Supplemental Help Desk Coverage**: Pricing for coverage under Section 3.2, stated both as (a) an annual retainer for a planned-coverage volume of 160 hours, billed in equal monthly amounts, and (b) a standalone hourly rate, including the rate applicable to same-day unplanned activation. State whether unused retainer hours roll over, and confirm that hours beyond the pool are billed at the standalone hourly rate. For purposes of the Total Three-Year Cost of Ownership, respondents must price that volume using whichever of the two required pricing bases—retainer or standalone hourly rate—yields the lower annual

cost under the respondent's own proposal. Unplanned same-day activations are excluded from the TCO figure and will be evaluated on the stated rate.

- **Tier 3 Block Hours**: The monthly block-hour allotment included in the base fee, whether unused hours roll over, and hourly rates for overage, as required by Section 3.1.
- **Provisioning, Hardware, and Travel**: Replacement firewall and BDR provisioning under Section 3.1, priced as purchased hardware, HaaS, or an equivalent model; hardware markup stated as a percentage; travel fees; and per-user onboarding or offboarding fees, if any.
- **Escalators and Pass-Throughs**: Annual price increases stated as a fixed percentage or a cap, treatment of pass-through license increases, and the written notice required before any increase takes effect.
- **One-Time and Onboarding Costs**: Separately itemized. Where amortized into monthly fees as permitted by Section 1, state the amortization schedule and the unamortized balance as of each contract anniversary.
- **HUD Cost Allocation**: A separate line item isolating network administration costs attributable to Lyons Gardens, as required by Section 3.5.

7. Evaluation Criteria

Evaluation Factor	Weight
Cost-effectiveness	25%
Technical capabilities and service levels	25%
Cybersecurity, privacy, and compliance safeguards	20%
Nonprofit and co-managed experience	15%
Transition and onboarding plan	10%
Client references and reputation	5%

Each factor is scored by an evaluation panel of no fewer than three Organization staff on a 0–100 point scale, weighted per the table above. The cost factor is scored by formula rather than judgment: the lowest responsive total three-year cost of ownership receives maximum points, and each remaining proposal receives points in proportion to the ratio of that lowest cost to its own.

A proposal scoring below 70/100 on either the *Technical capabilities and service levels* factor or the *Cybersecurity, privacy, and compliance safeguards* factor is non-responsive regardless of total; the final award will be made to the respondent whose proposal is most advantageous, price and other factors considered.

Nonprofit and co-managed experience is assessed on demonstrated experience serving nonprofit organizations, experience partnering with internal IT staff in a co-managed model,

responsiveness during the RFP process, and stated approach to supporting a mission-driven organization.

Transition and onboarding plan is assessed on the credential and administrative-access handoff described in Section 5, the replacement firewall and BDR cutover plan, and the respondent's demonstrated ability to complete onboarding within the window stated in the Section 8 timeline.

Client references and reputation is assessed on the relevance of the references provided, favoring nonprofit and co-managed engagements of comparable size and complexity, and on reference feedback in the categories listed in Section 5: help desk timeliness and proficiency, Microsoft 365 administration, proactive security monitoring, implementation and onboarding execution, and overall performance.

The Organization reserves the right to conduct interviews or request clarifications prior to final scoring.

8. Procurement Timeline & Point of Contact

Date	Milestone
Sep 3, 2026	RFP Issued
Sep 22, 2026	Vendor Questions & Notices of Intent Due
Oct 2, 2026	Consolidated Q&A Responses Posted
Oct 23, 2026	Proposals Due
Nov 4 – Nov 13, 2026	Finalist Vendor Interviews
Nov 20, 2026	Final Selection Notification
Nov 20 – Dec 4, 2026	Contract Negotiation & Execution
Dec 7, 2026 – Jan 31, 2027	Onboarding Period
Feb 1, 2027	Anticipated Contract Start

The Organization reserves the right to amend the timeline or cancel this RFP at any time without obligation.

Point of Contact

Karan Dodia, IT & Data Manager
procurement@familyeldercare.org
(512) 483-3566

Questions must be submitted in writing to the Point of Contact by September 22nd; responses will be posted to www.familyeldercare.org/msp-rfp and distributed by email to all registered respondents on a rolling basis, with a consolidated set of all responses issued no later than October 2nd. Administrative and logistical questions may be raised by phone; substantive

questions about scope, requirements, or evaluation must be submitted by email so that responses can be distributed to all respondents. Vendors contacting other staff or board members during the RFP process may be disqualified.

9. Submission Instructions

- **Registration:** respondents must email a notice of intent to respond to procurement@familyeldercare.org by September 22nd in order to receive Q&A distributions by email. Registration remains open through the submission deadline; respondents who register after September 22nd are responsible for reviewing the responses posted at www.familyeldercare.org/msp-rfp.
- **Submission Deadline:** October 23rd, 2026, 5:00 PM Central Time. Late submissions will not be considered.
- **Submit Final Proposals to:** procurement@familyeldercare.org
- **Format:** Single PDF named `[VendorName]_FEC_MSP_Proposal.pdf`
- **Acknowledgment:** Vendors will receive an acknowledgment email within one business day of submission.

10. Conflict of Interest, Confidentiality & Federal Requirements

Respondents must disclose any existing or prior relationships with Family Eldercare employees, officers, or board members. Proposals will be treated as confidential and shared only with evaluation participants until award.

This procurement is funded in part by federal grant funds; applicable provisions of 2 CFR Part 200, Appendix II apply, including Equal Employment Opportunity; Debarment and Suspension (SAM.gov registration required); Byrd Anti-Lobbying Certification; Records Retention and Access; the prohibition on obligating funds for covered telecommunications equipment or services (2 CFR 200.216); and compliance with applicable cybersecurity and privacy laws. Vendors may be required to complete additional certifications during final contract negotiation.

Family Eldercare reserves the right to accept or reject any proposal, negotiate final terms with one or more respondents, and/or discontinue the solicitation process at its sole discretion.

Appendix A — Environment Summary

Family Eldercare's IT & infrastructure environment is spread across a primary office, two residential communities, and eight scattered service-coordination and HUD Permanent Supportive Housing (PSH) sites. The Organization's staff consists of ~110 users across ~120 workstations.

A.1 Locations

Site	Address	FEC Staff	Internet (ISP)
Main Office (FEC)	1700 Rutherford Ln, 78754	~50 daily	Spectrum (500/25 Mbps)
Pecan Gardens (FEC-owned)	10813 Pecan Park Blvd, 78750	8–10 daily (+~75 residents/visitors, ~4 volunteers)	Spectrum (1 Gbps symmetric)
Lyons Gardens (FEC-owned)	2720 Lyons Rd, 78702	2 daily (+~60 residents/visitors)	Astound (300 Mbps symmetric)
Lakeside Apartments (Svc Coord)	85 Trinity St, 78701	1 daily	Property-provided
Gaston Place (Svc Coord)	1941 Gaston Pl, 78723	1 daily	AT&T FWA
Pathways at North Loop (Svc Coord)	2300 W North Loop Blvd, 78756	1 daily	AT&T FWA
Chalmers Courts (Svc Coord)	1638 E 3rd St, 78702	1 daily	AT&T Fiber
Oak Springs Villas (Svc Coord)	3001 Oak Springs Dr, 78702	1 daily	Property-provided
Wildflower Terrace (Svc Coord)	3801 Berkman Dr, 78723	1 daily	Property-provided
The Veer Apartments (HUD PSH)	7928 Gessner Dr, 78753	1–3 daily	Google Fiber
The Hedge Apartments (HUD PSH)	8300 N Interstate Hwy 35, 78753	1–3 daily	Google Fiber

A.2 Workstation Fleet

- ~120 workstations total: ~25 Dell Pro 16 (PC16255) laptops; ~80 Dell Latitude (predominantly 5540/5550, some 5520/5530); ~15 miscellaneous, shared-use, and spare PCs.
- Operating systems: Windows 11 Pro, all devices
- Average age ~2.5 years, with a long tail of devices at three or more years pending refresh; 3-year Dell ProSupport Plus warranty; 3-year refresh cycle (funding dependent).
- Mobile: 120 iPhone 16e (AT&T Business); count exceeds headcount following a carrier transition, surplus units are held as spares.

A.3 Server & Virtualization

- Dell PowerEdge T360 (installed Feb 2025): Intel Xeon E-2436; 48 GB ECC DDR5; PERC H755; 2×480 GB SSD (RAID 1) + 6×1.2 TB SAS 10K (RAID 5).

- Windows Server 2022 Hyper-V host running two VMs: Domain Controller (Windows Server 2019); File Server (Windows Server 2012 R2, to be decommissioned upon SharePoint migration completion).
- Backup: MSP-managed BDR appliance (incumbent-owned; returned at contract end, see Section 3.1) with daily cloud backups.

A.4 Network Infrastructure (per site)

Site	Firewall	Switches	Wireless	Segmentation
Main Office	Sophos XGS 126 (incumbent-owned)	1× USW-Enterprise-24 (core); 3× USW-Pro-48; 2× Cisco SG300 (EOL, pending removal)	5 Ubiquiti APs (Wi-Fi 5)	2 VLANs (Staff, Guests) VPN: Sophos Connect
Pecan Gardens	SonicWall (FEC-owned)	3× USW-Pro-48; 2× USW-Pro-24	12 Ubiquiti U6 Pro	4 VLANs (Staff, Housing Admin, Residents, Guests)
Lyons Gardens	Cisco MX84 (FEC-owned)	3× Cisco MS225-24P	3× Cisco MR44; 18× Cisco MR20	2 VLANs (Residents/Guests, Admin)
Scattered sites	Property/carrier-provided (see A.1)	—	—	—

A.5 Microsoft 365 & Security

- Microsoft 365 Business Premium: Exchange Online; SharePoint/OneDrive; Microsoft Teams; Entra ID (M365 apps only, no SSO integrations).
- Endpoint protection: SentinelOne. Email security: Avanan. Authentication: MFA enforced via Microsoft Authenticator. Encryption: BitLocker. License ownership: SentinelOne and Avanan are licensed through the incumbent and will not transfer at contract end; proposals must state the replacement EDR/XDR and email security tooling in the base fee (Section 5).
- Compliance: HIPAA standards applied organization-wide for sensitive client data.

A.6 Business Applications and Connectivity

- Bonterra Apricot Core (formerly Social Solutions): web-based social services CRM.
- MIP Cloud (Momentive Software): fund accounting.
- Nextiva: VoIP and virtual fax.
- Video conferencing: Microsoft Teams, Zoom.

A.7 Printer Inventory

- Main Office:
  - Managed print service provider: 3× Ricoh IM C6000 MFP; 3× Kyocera FS-4200DN.

    - FEC-managed: 5× Canon MF200-series MFP.
- Remote:
    - Managed print service provider:
        - Pecan Gardens: 1× Ricoh IM C3500.
        - Lakeside: 1× Ricoh MP C307.
        - North Loop: 1× Ricoh MP C307.
        - Veer: 1× Ricoh MP C307.
        - Hedge: 1× Ricoh IM 430F.
    - Remote workers: 2× Kyocera FS-4200DN.
- Printer inventory at Gaston Place, Chalmers Courts, Oak Springs Villas, and Wildflower Terrace to be confirmed, all FEC-managed.

A.8 Strategic Initiatives & RPO/RTO Targets

Current challenges: hybrid AD environment causing password-reset friction (SSPR desired); incomplete MDM for workstations and mobile devices (Intune desired); semi-manual device provisioning; aging workstation fleet; local server dependencies; incomplete documentation.

Priority projects: SharePoint migration (phased, nearing completion); modern device management (Intune evaluation, automated provisioning); security enhancement (password management solution desired; security awareness training program initiated June 2026).

Business continuity expectations:

- RPO: 24 hours for on-premises VMs (aligned to daily BDR cadence); 24 hours for M365 data once a third-party backup solution is implemented.
- RTO: 1 business day for on-premises workloads (BDR local virtualization); 4 business hours for individual file or mailbox restores.
- SaaS platforms (Apricot, MIP Cloud, Nextiva): vendor-managed availability; recovery commitments to be confirmed against vendor SLAs.
- Line-of-business snapshot exports (Apricot, MIP Cloud): RPO equal to the export/mirror cadence stated in Section 3.1 (quarterly); RTO to be confirmed.
  DR testing: annual restore verification for on-premises VMs, select file or mailbox restores, and validation of the most recent quarterly LOB exports.

Appendix B — Responsibility Matrix

This matrix summarizes the division of responsibility set out in Section 3. It is provided for clarity only; in the event of any conflict, Section 3 controls.

Function	Family Eldercare	MSP	RFP ref.
Network, server, firewall & switch administration — all sites, incl. resident/guest networks and VLAN segmentation at Pecan Gardens and Lyons Gardens	Authorizes changes	Owns	§3.1
Cybersecurity operations — EDR/XDR, email security, monitoring, incident response, BitLocker verification	Holds escrowed keys; approves security exceptions	Owns	§3.1
Backup & disaster recovery — on-prem VMs, M365, LOB exports; firewall and BDR provisioning at cutover	Participates in annual restore verification	Owns	§3.1, §A.8
Tier 3 support & escalations	Escalates	Owns	§3.1
Group Policy, identity & VPN administration	Owns policy decisions	Owns administration	§3.1
Incident Notification & written incident reports	Maintains Incident Notification List	Owns	§3.3
Tier 1/Tier 2 end-user support	Owns	Owns during §3.2 coverage periods only	§3.5, §3.2
Endpoint procurement & asset lifecycle (three-year refresh)	Owns	—	§3.5, §A.2
Device provisioning & user lifecycle — imaging, on/offboarding, licensing	Owns	Supports workflow automation (Intune)	§3.5, §A.8
LOB application administration — Bonterra Apricot Core, MIP Cloud	Owns	Quarterly snapshot exports only	§3.5, §3.1
VoIP & virtual fax, internet & wireless mobility, managed print	Owns	First-line coordination during §3.2 coverage only	§3.5, §3.2
Vendor & contract management — ISP, print, telephony, applications	Owns	—	§3.5
Change authorization & security exceptions	Owns; approval required before execution	Executes; may contain an active security incident first	§3.5
M365 tenant, domains, license inventory & credential repository	Owns and maintains	Administers as directed; documents all admin credentials	§3.1, §3.5
Coordination, site access & maintenance-window communication	Owns	Requests windows and access	§3.5
IT budget & cost allocation, incl. HUD Lyons Gardens line item	Owns	Provides input and pricing detail	§3.5, §6
Strategic technology reviews & roadmap (min. twice annually)	Owns direction	Owns delivery	§3.1, §3.5
Project work — SharePoint migration, Intune, hardware refresh	Authorizes and requests	Quotes and delivers on request; outside base scope	§3.4
Transition-out: documentation, config exports, credentials (10 business days)	Receives and verifies	Owns	§3.1