Arizona Alliance
FOR COMMUNITY HEALTH CENTERS

Primary Healthcare for All

IT Support

Request for Proposal

October 31, 2023

REQUEST FOR PROPOSAL: TABLE OF CONTENTS

1 INTRODUCTION

INTRODUCTION

The Arizona Alliance for Community Health Centers ("AACHC") is issuing this Request for Proposal ("RFP") to solicit proposals for recurring IT Support ("IT Support") Services that will be used to provide direct IT support for its employees.

AACHC would like to better understand the IT support services you provide and the services / functionalities available. They have provided detailed business requirements in Section 5.

All costs that you incur in connection with the preparation and submission of your response to this RFP and with any subsequent discussions or negotiations of a formal contract will be at the vendor's own discretion and expense. This document shall not be construed as a request or authorization to perform work at AACHC's expense. This RFP does not represent a commitment to purchase. Submission of a response constitutes acknowledgment that the vendor has read and agrees to be bound by such terms.

OVERVIEW

The Arizona Alliance for Community Health Centers (AACHC) is a non-profit organization whose mission is to advance Community Health Centers (CHCs) 's vital work in serving our communities' unique needs. AACHC has served as Arizona's Primary Care Association (PCA) since 1985 and comprises the state's largest network of primary care providers, serving over 817,000 patients across 175 sites and providing health services at over 3,200,000 office visits. AACHC houses Arizona's current –Health Center Controlled Network (HCCN), which supports health centers in addressing their challenges in leveraging Health IT for value-based care, requiring HIPPA compliance controls in our IT environment. AACHC also has an administrative services agreement with The Arizona Partnership for Immunization (TAPI), an Arizona nonprofit corporation. AACHC's partnership with TAPI includes access to the IT infrastructure and support from any contracted vendor.

This document is being used to solicit proposals from prospective vendors and to identify a vendor that can best fulfill the objectives and other criteria outlined in this Request for Proposal.

AACHC's primary objectives in implementing the IT SUPPORT solution includes the following:

- Providing direct technical support to approximately 50 employees and third-party contractors.
- Help to manage SaaS systems to ensure proper configuration and security standards.
- Ensure standardized equipment is properly patched and security standards are in place.
- Provide escalation for IT Problems and Service Requests.
- Monitoring of critical systems to ensure uptime, security, and reliability.
- Provide oversight of business continuity for IT systems and services.
- Reporting showing performance and opportunities for improvements.
- Conducting internal and external audits to ensure compliance and proper access rights.
- Ensuring proper documentation of IT systems, configurations, and processes.

To learn more about AACHC, please visit the public website at https://aachc.org

2 CONTACT / RESPONSE GUIDELINES

RESPONSE TIMING:

The schedule of major activities for this vendor selection process and their tentative completion dates includes the following:

Activity	Target Completion
Distribute RFP to Vendors	10/31/2023
Confirmation vendor intent to respond	11/17/2023
Vendor submit questions	12/1/2023
AACHC response to vendor questions	12/8/2023
RFP responses due	12/15/2023
Vendor Demonstrations	Week of 12/18/2023
Vendor Client Reference Site / Visits or Calls	Week of 1/8/2024
Vendor Recommendation	On or before 1/19/2024
Contract Finalized	On or before 1/31/2024

CONTACT INFORMATION

2.1.1 All communication with AACHC must be directed at the Points of Contact for this project, as follows:

Jeffrey Rosenthal
Project Manager
Direct: (602) 492-4090
Email: jeff@ciogenius.com

Copy: rfp@aachc.org

INTENT TO RESPOND

2.1.2 **Vendors must notify AACHC of their intent to respond by 11:59 PM MST on Friday, November 17, 2023**. This notification should be sent via email to the contact information noted in Appendix I.

PROPOSAL SUBMISSION

2.1.3 AACHC reserves the right to reject any and all proposals after the submission deadline.

2.1.4 All responses must include the following:

a) Completed electronic copy of this document.

b) Pricing.

c) Copy of your Annual Report.

d) Copy of the most recent Dunn and Bradstreet report or other recognized third-party credit agency report for your company.

e) Sample of your company's proposed Terms and Conditions.

f) Sample Service Level Agreements.

g) Signed Terms & Conditions Related to the RFP Response (Appendix 1).

h) Attachments and Additional Information (product brochures, specifications, etc. as appropriate).

i) All responses related to deadline times should be indicated in Arizona Time (MST).

REVIEW PROCESS

2.1.5 The review process for IT SUPPORT will be based on a variety of factors, at the sole discretion of AACHC, including but not limited to the following:

(a) The ability of the selected vendor to successfully support the current and future business needs of AACHC.

(b) Compliance with any regulations, and guidance from regulatory authorities.

(c) The total price, taking into account one-time vendor and AACHC costs, as well as the cost of ongoing service and support.

CONFIDENTIALITY / DISCLAIMER

2.1.6 This notice is a reminder to all recipients of this Request for Proposal that the RFP is the confidential and proprietary information of AACHC. As such, this RFP, and all such other information, is to be treated confidentially and used only to prepare a response for submission. Any other use is strictly prohibited.

2.1.7 All material submitted to AACHC in response to this RFP shall become the property of AACHC.

2.1.8 The submission of this RFP in no way obligates AACHC to award the project to you or anyone else.

2.1.9 AACHC reserves the right to accept or reject your response at its complete discretion. AACHC is not bound to explain its selection decision.

2.1.10 AACHC reserves the right to determine whether your response to the mandatory requirements subjects the bid to disqualification.

2.1.11 AACHC may withdraw and/or revise this RFP at any time and for any reason whatsoever. Nothing in this RFP or its submission to you or others obligates AACHC to purchase any products or services from you or anyone else.

2.1.12 No binding contract relating to the RFP shall be deemed to exist unless and until AACHC, in its sole discretion, executes a written contract with the party or parties of its choosing.

2.2 COST OF RESPONSE/DISCLAIMER

2.2.1 Your response to this RFP shall be prepared and submitted by you at your sole cost, risk, and expense.

3 EVALUATION CRITERIA

OVERVIEW

3.1.1 AACHC is looking for a reliable, financially stable supplier who has the ability to meet or exceed AACHC's stringent cost, quality, and service requirements. All elements of each response, including value-added and intangible factors will be evaluated. General areas of focus are as follows:

a) Competitive pricing.

b) Supplier's experience, qualifications, and capabilities.

c) Supplier's compliance with regulatory requirements as it relates to AACHC's customer list and compliance with any other applicable regulatory and client data protection requirements.

d) Strong program leadership and delivery experience. AACHC is looking for vendors who are supporting other small-to-midsized companies, preferably at a growing non-profit organization with healthcare focus.

e) Strategic point of view – need a partner to identify and raise the proposed roadmap's longer-term implications and impacts.

f) Knowledge and understanding of AACHC's operating business model.

g) Strength of the vendor's IT Support services in terms of services provided, knowledge of key systems, focus, references, implementation intensity/cost, and solution's best fit and effectiveness within AACHC's business and IT environment.

3.1.2 AACHC does not represent that these are the sole selection criteria and reserves the right to adjust its selection criteria at any time.

4 SUPPLIER BACKGROUND

Please Note: Answers should not be limited to yes or no. Provide detail wherever possible.

COMPANY BACKGROUND

4.1.1 Provide detailed background information about your company, including:

i. Year company was founded.

ii. Name of parent organization and any affiliates/subsidiaries.

iii. Ownership structure (major shareholders and share of ownership).

iv. Name of the principal(s) of the firm.

v. Name, telephone number and email address of a representative of the firm authorized to discuss your submission.

vi. Business focus.

vii. Number of employees.

viii. Company Type (Corporation, LLC, S-Corp)

ix. Address of all offices of the firm.

x. Description and history of the firm.

xi. Description of the firm's IT Support solution and any related implementation, hosting, support, or other services your firm provides; length of time the firm's solution has been on the market.

xii. Description of the organization's position within the industry; description of the IT solution's source of competitive advantage.

xiii. Provide three references, including a contact name and telephone number for a similar organization that has used your firm's solution and/or to which your firm has provided IT support services. Briefly describe the products and/or services provided to each customer.

xiv. Identify key members of your management team and provide their biographies.

xv. Are there any mergers or acquisitions that your company is currently committed to executing? What if any impact would those business events have on the products and services outlined in this RFP?

FINANCIAL BACKGROUND

4.1.2 Provide audited financial statements, annual reports if available, for the three most recent fiscal years.

4.1.3 List your top five customers: a) in total; b) in healthcare; and c) in services industry, and year in which customer relationship began.

4.1.4 Provide the name and phone number of a senior finance person within your company that may be contacted to discuss financial matters and assist AACHC with a financial due diligence evaluation of your company.

4.1.5 What insurance do you have in force that will extend to AACHC in the vendor relationship proposed?

STRATEGIC INITIATIVES

4.1.6 What new services or products will you bring to market within the next 18 months that could benefit AACHC?

VALUE PROPOSITION TO AACHC

4.1.7 Articulate how the strategic initiatives outlined in Section 4.1.6 above will benefit AACHC's IT Support Service efforts.

4.1.8 What differentiates your solution from your competitors?

4.1.9 How will you help AACHC differentiate itself from other providers of IT Support services?

4.1.10 Do all of your clients have the same functional capabilities? Please identify what you have done to customize solutions for current customers.

LAWSUITS AND LEGAL ACTIONS

4.1.11 Describe any potential liability related to material litigation.

5 FUNCTIONAL REQUIREMENTS

FUNCTIONAL REQUIREMENTS MATRIX

The table below includes the detailed business requirements. The detailed business requirements identify requirements that are "must haves". In your response, you must explain how you will meet each of the requirements listed in the table. **If you choose not to provide this detail in the vendor response column of the table, please ensure that a clear explanation is provided and identifiable in the RFP response.**

ID#	IT Support Requirements	Vendor Response
1.00	**Systems Infrastructure**	
1.01	Can you maintain physical and virtual servers?	
1.02	Can you maintain workstations and mobile devices?	
1.03	Can you support server software, including but not limited to Microsoft Windows Server and Active Directory?	
2.00	**Network Administration Management**	
2.01	Can you maintain Firewall, Switches, and Wireless Access Points, including configuration, monitoring, and upgrades?	
2.02	Do you have experience in managing Ubiquiti and Cisco Meraki gear?	
2.03	Will you help to provide support services for circuits with telecommunications providers?	
3.00	**SaaS Management**	
3.01	Can you maintain 3rd party SaaS tools (e.g. Cloud PBX, EDR, etc.)?	
3.02	Can you support Microsoft M365, Azure Active Directory, Endpoint Manager (formerly Intune), and Security/Compliance tools?	
4.00	**Helpdesk Support**	
4.01	What ticket system do you use to manage and track issues / service requests?	
4.02	How is the ticket system configured to segment company data from other customers?	
4.03	Is there a self-service portal our users will be able to access to see status updates?	
4.04	If yes to 4.03, will you be creating and posting KBs to help users receive self-help articles to resolve their issues?	
4.05	If yes to 4.03, can we set up Service Requests for specific software/hardware requests, and is there capacity for management approval of some items?	
4.06	Are there SLAs/OLAs put in place and if so, what are your standard policies?	

ID#	IT Support Requirements	Vendor Response
4.07	If SLAs/OLAs are in place, how do you escalate items that fail and how are these reported to the customer?	
4.08	How do you measure Help Desk staff performance and are those metrics provided to AACHC for review?	
4.09	What technology do you use to remote into managed systems?	
4.10	Is your team able to communicate technical jargon to non-technical users?	
5.00	**Consulting and Project Management**	
	For specific projects and upgrades, will you assign a Project Manager depending on the scope of the engagement to ensure the project's success?	
	If a project is required to help upgrade or improve a system, software, or service, will you be taking away from general Helpdesk hours to complete the project properly?	
6.00	**Basic Services, Office Hours, and Staffing**	
6.01	How many people operate in your Helpdesk environment?	
6.02	What are your normal business hours?	
6.03	Does your team provide any training, especially for gaps identified within the helpdesk?	
6.04	Will your organization help track and maintain inventory of assets, and keep track of licensing (including SaaS subscriptions)?	
6.05	Will you provide QBRs to review IT performance, bring up concerns, and provide recommendations for improvements?	
6.06	Can you provide documentation on how items will be escalated to AACHC's leadership? (e.g. employee requests, SLA/OLA violations, breaches, etc.)	
6.07	What technologies or staffing do you outsource and does any of those products or staff come from off-shore (outside the United States)?	
7.00	**Certifications / Memberships**	
7.01	Please provide any certifications you or your team has completed and maintains.	
7.02	Please provide any memberships or associations your company belongs to.	
8.00	**Security**	
8.01	Does your organization maintain a SOC?	
8.02	If yes to 8.01, can you manage an existing SIEM, or do you require the use of your own SIEM?	
8.03	If requiring own SIEM, what are specifications around specific software and/or collectors used?	
8.04	What is your company's ability to handle Cyber Security attacks?	

ID#	IT Support Requirements	Vendor Response
8.05	How do you work with companies with HIPAA/HITECH and PCI requirements?	
8.06	Can you provide guidance to AACHC for NIST, HIPAA/HITECH and PCI-DSS?	
8.07	Are you able to conduct external penetration tests and/or vulnerability scanning?	

6 TECHNICAL & INFORMATION OUTSOURCING REQUIREMENTS

GENERAL

6.1.1 Please find below AACHC's Information Security Third- Party Requirements. Could you please answer indicating either

(1) Not Applicable based on services to be provided under this RFP,
(2) Yes,
(3) Partially or
(4) No.
Please provide comments where you feel you need to explain answers.

ID#	Technical & Information Security Requirements	Vendor Response
1.00	**Vendor Information**	
1.01	Can you accommodate an onsite visit for a security audit within 72 hours notice?	
1.02	Can you store all AACHC confidential data within Contiguous United States - incl. backups?	
1.03	Do you maintain an audit log for the location of all AACHC confidential data and their backups, to identify where it is located at any point in time, in order to address privacy laws for storage within Contiguous United States?	
1.04	Can you confirm you will not access AACHC confidential data from outside of Contiguous United States?	
2.00	**Policies, Standards and Procedures**	
2.01	Do you have formal written Information Security Policies?	
2.02	Can you provide copies of the Information Security Policies?	
2.03	Can you provide results of a third-party external Information Security assessment conducted within the past 2 years (SOC-2, pen. test, vulnerability assess., etc.)?	
2.04	Do you maintain incident response procedures?	
2.05	Do you have a policy to protect client information against unauthorized access; whether stored, printed, spoken or transmitted?	
2.06	Has a policy that prohibits sharing of individual accounts and passwords been created?	
2.07	Do you have a policy that implements the following Information Security concepts: need to know, least privilege and checks and balances been created?	
2.08	Do you provide training to your System Administrators?	
2.09	Do you implement AAA (Authentication, Authorization, Accounting) for all users?	

ID#	Technical & Information Security Requirements	Vendor Response
2.10	Do you perform background checks for individuals handling confidential information?	
2.11	Do you have termination or job transfer procedures that immediately protect unauthorized access to information?	
2.12	Do you provide customer support with escalation contacts?	
2.13	Do you have documented change control processes? Can we view them?	
2.14	Do you require contractors, subcontractors, vendors, outsourcing ventures, or other external third-party contracts to comply with policies and customer agreements? What sort of subcontractor/vendor documentation is required?	
2.15	Do you maintain a routine user Information Security awareness program?	
2.16	Do you have a formal routine Information Security risk management program for risk assessments and risk management?	
4.00	**Architecture**	
4.01	Can you provide a network topology diagram/design of your solution?	
4.02	Will the services being provided to AACHC be running on shared hardware of standalone servers dedicated to AACHC?	
4.03	Have you implemented a network firewall protection system?	
4.04	Have you implemented a web application firewall protection system?	
4.05	Have you implemented a host firewall protection system?	
4.06	Do you maintain routers and ACLs?	
4.07	Can you provide network redundancy?	
4.08	Do you have IDS/IPS technology implemented?	
4.09	Do you use DMZ architecture for Internet systems?	
4.10	Do you adhere to the practice that web applications, which 'face' the Internet, are on a server different from the one that contains the database?	
4.11	Do you use enterprise virus protection on all systems?	
4.12	Do you follow a program of enterprise patch management?	
4.13	Do you provide dedicated customer servers to segregate AACHC data from other customer data? If not, then how is this accomplished in a secure virtual or segmented configuration?	
4.14	Do you implement controls to restrict access to AACHC data from other customers?	
4.15	Can you ensure that remote access is only possible over secure connections?	

ID#	Technical & Information Security Requirements	Vendor Response
4.16	Do you use separate physical and logical development, test and production environments and databases?	
4.17	Do you secure development and test environments using, at a minimum, equivalent security controls as the production environment?	
4.18	Do you provide the architectural software solution design with security controls?	
5.00	**Configuration**	
5.01	Do you implement encryption for confidential information being transmitted on external or Internet connections with a strength of at least AES 256 bit or uses TLS 1.2, preferably TLS 1.3?	
5.02	Do you implement encryption for confidential information at rest with a strength of at least AES 256 bit?	
5.03	Do you have password-protected screen savers that activate automatically to prevent unauthorized access when idle, for computers used by system's support users?	
5.04	Can you remove all unnecessary services from computers?	
5.05	Do you use file integrity monitoring software on servers (such as tripwire, etc.)?	
5.06	How quickly do you change or disable all vendor-supplied default passwords or similar “published” access codes for all installed operating systems, database management systems, network devices, application packages, and any other commercially produced IT products?	
5.07	Do you use password conventions that are a minimum of 8 characters, expire at least annually and have complexity requirements?	
5.08	Do you ensure that passwords are never stored in clear text or are easily decipherable?	
5.09	Do you Check all systems and software to determine whether appropriate security settings are enabled?	
5.10	Do you manage file and directory permissions following least privilege and need-to-know practices?	
5.11	Do you implement redundancy or high availability for critical function?	
5.12	Do you authenticate all user access with either password, token or biometrics?	
5.13	Do you formally approve all tests and log all system changes?	
5.14	Can you confirm you not use production data for both development and testing, unless it has been declassified by the customer?	

ID#	Technical & Information Security Requirements	Vendor Response
5.15	Can you confirm you use artificial data in both development and test environments?	
5.16	Do you limit access to development and test environments to personnel with a need to know?	
5.17	Do you set the account lockout feature for successive failed logon attempts on all system's support computers?	
5.18	Do you prohibit split tunneling when connecting to customer networks?	
6.00	**Compliance**	
6.01	Will you provide relevant certificates of applicable ISO 27001 certification?	
6.02	Can you provide documentation that your product is HITECH compliant for any PHI on behalf of AACHC?	
6.03	Can you provide documentation of your PCI-DSS compliance for any payment card information, on behalf of AACHC?	
6.04	Do you use industry standard best practices for application security (e.g. OWASP)?	
7.00	**Access Controls**	
7.01	Do you immediately remove, or modify access, when personnel terminate, transfer, or change job functions?	
7.02	Do you achieve individual accountability by assigning unique IDs and prohibiting password sharing?	
7.03	Do you ensure that critical data, or systems, are accessible by at least two trusted and authorized individuals, in order to limit having a single point of service failure?	
7.04	Do you ensure that users have the authority to only read or modify those programs, or data, which are needed to perform their duties?	
7.05	Have you had any security breaches in the last three years? If yes, describe the incident, solution deployed, time to remedy and post implementation monitoring and feedback results.	
8.00	**Monitoring, Maintenance and Support**	
8.01	Do you review access permissions monthly for all server files, databases, application, etc.?	
8.02	Do you implement system event logging on all servers and records at a minimum who, what, and when for all transactions?	
8.03	Do you conduct reviews and analyses of after-hour system accesses, at least monthly?	
8.04	Do you review system logs for failed logins, or failed access attempts monthly?	
8.05	Do you review and remove dormant accounts on systems at least monthly?	

ID#	Technical & Information Security Requirements	Vendor Response
8.06	Do you review web server logs weekly for possible intrusion attempts and daily for significant changes in log file size as an indicator of compromise?	
8.07	Do you review network and firewall logs at least monthly?	
8.08	Do you review wireless access logs at least monthly?	
8.09	Do you perform scanning for rogue access points at least quarterly?	
8.10	Do you actively manage IDS/IPS systems and ensure alert notifications have been implemented?	
8.11	Do you perform vulnerability scanning at least quarterly? This is a mandatory requirement for all AACHC IT SUPPORTs.	
8.12	Do you perform penetration testing at least annually, if the vendor manages any PHI on behalf of AACHC? This is a mandatory requirement for all AACHC IT SUPPORTs.	
8.13	Do you check routinely that password complexity is adhered to?	
8.14	Do you have 24x7x365 system, operations and network administrators onsite to support AACHC's application? If not, indicate how these individuals respond to non-work-hour issues.	
8.15	Please detail the maintenance activities that will be performed to maintain the production health of all the platform(s) that will support AACHC processing (examples include Database Reorganization, Preventative Hardware Maintenance, Firmware Upgrades, System Configuration Reviews, etc.).	
8.16	What products/tools are used to monitor servers, networks, applications, databases and transmissions of data onsite/offsite and between platforms on a 24x7x365 basis? What metrics are used for monitoring, including thresholds. How does this impact capacity planning?	
8.17	Do you have change control procedures for applications, hardware and operating system modifications (including frequency, how changes get migrated through various environments and whether any are customizable by client). How do you notify clients of planned changes?	
8.18	Do you have a problem tracking and resolution process? How do you report client problems?	
9.00	**Physical Security**	
9.01	Do you control access to secured areas. E.g. key distribution management (both physical and electronic), paper/electronic logs, monitoring of facility doors, etc.?	

ID#	Technical & Information Security Requirements	Vendor Response
9.02	Do you control access to server rooms and follow least privilege and need-to-know practices for those facilities?	
9.03	Do you have special safeguards in place for any computer rooms. e.g. cipher locks, restricted access, room access log, card swipe access control, etc.?	
9.04	Do you shred or incinerate printed confidential information?	
9.05	Do you prohibit or encrypts confidential information on laptops & mobile devices?	
9.06	Do you position desktops, which display confidential information, in order to protect from unauthorized viewing?	
9.07	Do you escort all visitors in computer rooms or server areas?	
9.08	Do you implements appropriate environmental controls, where possible, to manage equipment risk. E.g. fire safety, temperature, humidity, battery backup, etc.?	
9.09	Do you have any external signage indicating the content or value of the server room or any room containing confidential customer information?	
9.10	Do you provide an export copy of all the customer's data in a mutually agreed upon format at the end of the contract?	
9.11	Do you follow forensically secure data destruction processes for confidential data on hard drives, tapes & removable media when it's no longer needed and at the end of the contract term?	
9.12	Can you provide continued power for the computer facility to allow normal operation in the event of loss of the normal power supply? If yes, for what duration?	
10.00	**Contingency**	
10.01	Do you have a written contingency plan for mission critical computing operations?	
10.02	Do you have emergency procedures and responsibilities documented and stored securely at all sites?	
10.03	Do you review and update the contingency plans at least annually?	
10.04	Have you identified computing services that must be provided within specified critical timeframes, in case of a disaster?	
10.05	Have you identified cross-functional dependencies, to determine how the failure in one system may negatively impact another one?	
10.06	Have you written backup procedures and processes?	

ID#	Technical & Information Security Requirements	Vendor Response
10.07	Do you test the integrity of backup media quarterly?	
10.08	Do you store backup media in a secure manner and controls access?	
10.09	What is your backup frequency (daily, weekly, monthly, etc.), what is the format (full or incremental), media (tape, disk, electronic vaulting, etc.), and retention period for the various types of data that would be used to support?	
10.10	What is the retention period that would apply to AACHC Rehab.	
10.11	Do you maintain a documented and tested disaster recovery plan?	
10.12	Do you use off-site storage and do you have documented retrieval procedures for those backups?	
10.13	Do passwords protect and encrypt all backups?	
10.14	Do you provide rapid access to backup data?	
10.15	Do you label backup media appropriately, to avoid errors or data exposure?	
10.16	Do you have hardware and network redundancy that you deploy to avoid extended outages and minimize client risk?	
11.00	**Vendor's Business Associates**	
11.01	Have confidentiality agreements been signed before proprietary and/or confidential information is disclosed to the vendor's business associates?	
11.02	Are your business associate contracts, or agreements, in place and contain appropriate risk coverage for customer requirements?	
11.03	Are your business associates aware of customer security policies and what is required of them?	
11.04	Have vendor business associate agreements documented the agreed transfer of customer's data when the relationship terminates?	

7 RELATIONSHIP MANAGEMENT / CLIENT SERVICE

7.1.1 AACHC requires a centralized relationship model for product and operational support. The centralized relationship model must serve as a single point of contact, supporting all of our users, and must meet all ongoing requests for new issues and services, client requests and resolution for all production and operational issues/concerns.

7.1.2 Outline your vision of the centralized relationship model with AACHC. Describe how it would be developed, implemented and staffed.

7.1.3 Outline the approach you use to provide management level reviews of your company's performance, resolve disputes, track progress of projects and provide updates on overall relationship tracking.

7.1.4 Does your company create individual service level agreements to track performance to SLA goals, for example; System Uptime, Response time to queries, Error Resolution, etc. How often do you report on your performance and in what format? How are actions items tracked and communicated? Provide a sample client 'report card'.

7.1.5 How does your company handle system, software and/or functionality upgrades for the hardware and software components? How are your upgrade plans determined?

8 PRICING

Price flexibility will be a fundamental requirement for AACHC in determining our future services provider.

Based on the AACHC's requirements, please provide a high-level estimate of costs associated with the purchase and implementation of your firm's solution, including any necessary assumptions. Responses to this section are understood to be for informational purposes. Similarly, it is understood that your firm's estimates may change depending on the scope of work presented in the future. Your firm's estimate of the cost of implementing IT Support services to assist AACHC in determining a reasonable budget. Please include the following:

8.1.1 Break out all applicable hardware, software, licensing, subscription, hosting, support, and required third party costs;

8.1.2 Describe your pricing model, including how the estimated costs were established and what factors affect the cost;

8.1.3 Indicate whether service pricing is based on named users, service/ticket time, and/or other;

8.1.4 Discuss the cost effect of expanding service usage based on company growth and/or extension to other business areas of the AACHC;

8.1.5 Discuss any potential future costs and identify what services are included in the pricing proposed;

8.1.6 Outline any third-party components that your solution relies upon and their associated costs over one, three, and five years, respectively.

8.1.7 Identify any additional service components you charge beyond those listed above. Include any other pricing categories that would be charged by your company.

APPENDIX 1: RFP INTENT TO RESPOND FORM

Please complete and e-mail this form to the designated AACHC Representative on or before **Friday, November 17, 2023**

To:		From:	*[Vendor to complete]* (the "**Vendor**")
Name of the Entity:	AACHC	Legal Name:	
E-mail:		E-mail:	
Phone Number:		Phone Number:	
Date:	September 19, 2023	Date:	

Re: IT Support Services RFP

Please indicate your intent to respond to this RFP by placing an "X" in the appropriate boxes:

	We understand the scheduled dates as specified in this RFP and intend to respond accordingly by December 15, 2023.
	We will not be responding to this RFP and will delete and destroy all materials sent to us.

Name	**Signature**
Title Account Executive	**Date 10/31/2023**

I have the authority to bind to corporation.

APPENDIX 2: RFP QUESTION SUBMISSION FORM

Any and all questions or comments regarding the RFP must be submitted to the designated AACHC Representative using the enclosed **Appendix 2** "**Question Submission Form**". Questions must be submitted by e-mail and will be accepted up until **11:59 pm, December 1, 2023**.

To: Designated Representative
Date: <<Date>>
Subject: **IT Support Services RFP**
Company Name:
Contact Person:
Telephone Number:
E-mail Address:

QUESTION #1

SECTION:		SUBSECTION:	
Q.			

QUESTION #2

SECTION:		SUBSECTION:	
Q.			

QUESTION #3

SECTION:		SUBSECTION:	
Q.			

QUESTION #4

SECTION:	General	SUBSECTION:	
Q.			

QUESTION #5

SECTION:	General	SUBSECTION:	
Q.			

APPENDIX 3: TERMS AND CONDITIONS RELATED TO THE RFP RESPONSE

1. Right to Select

AACHC reserves the right to select and negotiate with those suppliers it deems qualified and to terminate negotiations without incurring any liability. AACHC reserves the right to reject any or all responses received.

2. Response Submission

In order for responses to qualify, they should conform to the prescribed format of the RFP. If you believe there is additional information that is both absent from the RFP and relevant to your proposal, include this additional information in attachments to this RFP. Be sure to clearly mark each additional sheet with the exact topic and RFP part/section to which the additional sheet refers. Expenses related to the development and submission of this, or any information, are the sole responsibility of the supplier.

If AACHC awards you a contract, at its option, AACHC may choose to incorporate any or all parts of your response in the contract. All RFP responses submitted will become the property of AACHC. Responses received after the prescribed day and time may not be considered, or penalties may be assessed.

3. Confidentiality

Either the Vendor and/or AACHC requested, or may request, certain information from the other in connection with this RFP for an IT Support Services solution (the "Proposed Transaction"). In consideration thereof and as a condition to being furnished such information by the other, each party in its capacity as a recipient of information (in such capacity, the "Receiving Party") agrees as follows with the other party in its capacity as a provider of information (in such capacity, the "Disclosing Party"):

A. Definition of and Ownership of Information

(i) All disclosures embodying business affairs and activities, including but not limited to, the identification of customers and suppliers, customer information, financial information pertaining to the Disclosing Party, its affiliates or its customers, business plans, all documents and things related to the Disclosing Party's business and activities, and the fact that the parties are contemplating the Proposed Transaction (hereinafter referred to collectively as "Confidential Information") are and remain the sole and exclusive property of the Disclosing Party.

(ii) All disclosures embodying and/or relating to any computer software, systems and related documentation of Disclosing Party (hereinafter referred to collectively as "Proprietary Information") are the proprietary property of the Disclosing Party, either by way of

ownership or license agreements with third parties, and that said Proprietary Information is not publicly known or available from other sources and is presently being maintained and disclosed by the Disclosing Party in the strictest of confidence. Proprietary Information is a subset of Confidential Information.

(iii) Nothing in this Agreement shall give the Receiving Party or its Affiliates any right, title, license or interest whatsoever in or to the Confidential Information or any other intellectual property of the Disclosing Party or its Affiliates.

(iv) As used herein, Confidential Information does not include any information: (a) which was or becomes generally available to the public or is in the public domain at the time of its disclosure, other than as a result of the disclosure by Receiving Party or its Representatives; (b) already in Receiving Party's possession on a non-confidential basis at the time of disclosure pursuant to this Agreement; (c) was or becomes available to Receiving Party from a source other than Disclosing Party or Disclosing Party's directors, officers, employees or agents provided that such source is not known to Receiving Party to be bound by a confidentiality agreement with Disclosing Party; (d) developed independently by Receiving Party or Receiving Party's Representatives, without violating any of Receiving Party's obligations hereunder; or (e) is approved for disclosure or release by written authorization from Disclosing Party.

B. Use of Information

(i) Except as expressly provided below or with Disclosing Party's written consent, Receiving Party agrees (a) that it will hold all Confidential Information in confidence, (b) that it will not disclose any Confidential Information to any third party, other than its affiliates and its and their directors, officers, employees, agents, consultants, or representatives who have a need to know such information in connection with the Proposed Transaction (collectively, the "Representatives"), and (c) that Receiving Party will not use or permit its Representatives to use any such Confidential Information for purposes other than in connection with the Proposed Transaction or to disclose any such Confidential Information except as permitted hereunder.

(ii) Receiving Party agrees to inform its Representatives of the confidential and valuable nature of the Confidential Information and of its obligations under this Agreement.

(iii) Receiving Party agrees to be responsible for any breach of this Agreement by any of its representatives.

C. Protection of Information

(i) Receiving Party will protect all Confidential Information by establishing appropriate safeguards and controls which Receiving Party shall validate periodically. The results of the validations will be made available to Disclosing Party upon request.

(ii) The disclosure or release of Confidential Information by Receiving Party requires the prior express written consent of Disclosing Party, at any time before, during or subsequent to the engagement and rendering of services, regardless of Receiving Party's participation in the design and development thereof.

(iii) No copying or duplication of any documentation, electronic storage media (such as tapes and disks) or other material relating either in whole or in part to Disclosing Party's Confidential Information, unless specifically required as part of providing services to Disclosing Party, will be performed by Receiving Party.

D. Compelled Disclosure

(i) If Receiving Party becomes legally compelled by law, regulation, self-regulatory organization requirement, government or regulator request, disclosure obligation, deposition, subpoena, or other legal process to disclose any of the Confidential Information, Receiving Party will, unless otherwise prohibited by applicable law, give Disclosing Party prior notice of such disclosure. If a protective order or other remedy is not obtained by Disclosing Party, Receiving Party may disclose such Confidential Information. In the event of such compelled disclosure, Receiving Party agrees to use reasonable efforts to obtain assurances that confidential treatment will be afforded to such Confidential Information. Any effort by Receiving Party to cooperate with Disclosing Party, if Disclosing Party seeks to obtain a protective order concerning the Confidential Information, will be at Disclosing Party's sole expense. Receiving Party shall not be required to take any action unless expenses or costs thereof are prepaid by Disclosing Party.

E. Return of Information

(i) Upon notification that the Proposed Transaction will not proceed or termination of one party's services for the other party for any reason, whichever occurs first, Receiving Party shall immediately return or destroy, at the Receiving Party's option, all copies and originals of material containing Confidential Information to Disclosing Party, subject to the Disclosing Party's direction, within thirty (30) days of notification of termination of services. Receiving Party may retain copies of Disclosing Party's Confidential Information only if required by law or regulation.

F. Notification and Relief of Security Breach

(i) Receiving Party will notify Disclosing Party within twenty-four (24) hours of its initial discovery of any suspected or known security breach related to any of the following:

(a) Unauthorized access to or use of Disclosing Party's Confidential Information

(b) Unauthorized disclosure, misuse, alteration, destruction or other compromise of Disclosing Party's Confidential Information

(ii) Receiving Party agrees that notification of breach to Disclosing Party must be made through private and secure means, and that Receiving Party will maintain confidentiality of the breach by not communicating with or notifying the media, affiliates, other third parties, or Disclosing Party's customers without prior written consent from Disclosing Party.

(iii) Receiving Party acknowledges the significant risks to Disclosing Party associated with a security breach related Confidential Information and agrees that knowledge of and information related to any Breach will be controlled and limited by Receiving Party to only those Receiving Party employees who have a "need to know."

(iv) Unauthorized disclosure by Receiving Party, its agents or employees, of Disclosing Party's Confidential Information may cause irreparable injury to Disclosing Party and Disclosing Party may be entitled to injunctive relief in addition to any other remedies that may be available at law or in equity, in the event Receiving Party breaches any of its duties and/or obligations under this agreement. Receiving Party further agrees to pay all Disclosing Party's attorney's fees and related legal costs arising out of any breach of this Agreement.

G. Changes and Governance

(i) This Agreement may not be modified, amended, or waived in any manner except in writing, executed by both parties. Failure of either party to enforce rights hereunder shall not be deemed a waiver. Should any provision(s) be ruled invalid by applicable legal authority, such provisions shall be deemed omitted and the remaining terms of the Agreement remain in full force and effect.

(ii) This Agreement may not be assigned by either party without the prior written consent of the other and shall be binding on, and inure to the benefit of, the respective successors of the parties hereto.

(iii) This Agreement shall be governed by and construed in accordance of the laws of the State of Texas.

(iv) This Agreement shall expire on the date which is the earlier of eighteen (18) months from the Effective Date of this Agreement or the consummation of any transaction contemplated by this Agreement.

4. Signature

I, _____, an authorized representative of the company,

_____, agree to the terms outlined in this RFP and to the prices quoted herein. I further understand that AACHC's issuance and subsequent receipt of this RFP does not obligate AACHC in any way. AACHC will not be bound to purchase any services or products until such time as legal provisions are determined, contracts or agreements are negotiated in detail, and purchase orders are issued. AACHC reserves the right to reject any and all offers at its sole discretion.

Name (PRINT): _____

Signature: _____

Title: _____

Date: _____

APPENDIX 4: VENDOR ENGAGEMENT GUIDELINES FOR AACHC RFP

1. Representatives of AACHC will disclose any information provided by the vendor to a third party without the expressed consent of the vendor.
2. Representatives of the AACHC will uphold the values, policies, and procedures established by the AACHC.
3. Vendors and representatives of the AACHC will conduct business in an atmosphere of honesty and good faith, without intentional misrepresentation, and with equal objectivity and fairness.
4. No vendor shall cause or influence or attempt to cause or influence any AACHC officer or employee in their official capacity in any manner that might tend to impair the objectivity or independence of judgment of that AACHC officer or employee.
5. No vendor shall offer or provide any interest, financial or otherwise, direct or indirect, in the business of the vendor or professional activity in which the vendor is involved with the AACHC officer or employee.
6. No vendor shall offer any AACHC officer or employee any gift, favor, service or other thing of value under circumstances from which it might be reasonably inferred that such gift, service, or other thing of value was given or offered for the purpose of influencing the recipient in the discharge of his or her official duties.
7. These guidelines do not replace, supersede, or circumvent the Employee Code of Business Conduct and Ethics as established by the AACHC.