Term of Agreement

Term of this Agreement is 3-years with a 2-years extension possibility.

Every 12 months, Vendor and Beach Cities Health District (BCHD) retains its right to re-evaluate the size and scope of the environment and propose adjustments to the cost, service levels, and related terms of this contract.

Overview of Requested Scope of Work

BCHD seeks to identify the provider of Information Systems Management to meet current and foreseeable strategic business needs. The primary need at this time is for Vendor to provide a high level of response and resolution time to the user base while maintaining monthly support costs.

Assumptions

- Hybrid-cloud environment with up to 150 users, 110 workstations and 4 servers. Primarily Windows with only a handful of macOS.
- BCHD may provide regular, dedicated workspace for Vendor personnel, and access to telephones, copier, and printing facilities.
- BCHD shall be responsible for the cost of all new hardware, new software licenses, consumable items, desktop/laptop/printer repair parts, server/network equipment repair parts, and 3rd party vendor support contracts for line of business applications and telephone system.
- BCHD shall provide end-user training.
- BCHD shall provide budget for spare equipment repair and replacement. Vendor is not responsible for operating levels that lapse due to unavailable hardware.

Baseline Requirements

- Systems administration (including but not limited to on/off boarding users, user management, group management, emails, SharePoint, Azure, backups, and disaster recovery).
- Monitor and maintain infrastructure (Windows Servers, network, endpoints, and cloud-based assets).
- Event notifications and response.
- Asset, change, and patch management.
- Frontline user support (Windows, MacOS, and any other guidance needs).
- Ticketing system with status, tracking, and management reporting.
- Priority based SLA system.
- Provide up to date recommendations on best practices.
- Minimize security risks and ensure systems uptime.
- Meeting cadence with management.
- HIPAA-covered entities must have a business associate agreement (BAA) in place.

Additional Services for Consideration

- Onsite services: If available on demand, on schedule, or not available.
- Security Operations Center (SOC) or cyber security services.
- New projects that are not in scope.

Operating Level Definitions

Language used to describe services offered by Vendor.

Full Ownership. Whatever actions are required to meet the specific service objectives on a complete and timely basis.

Best Effort. Examine and diagnose the issue identified in the service request. Where staff experience suggests a probable cause and/or appropriate solution are known, the solution will be implemented. May coordinate and drive the resolution; however, the work is a "best effort".

Assessment/recommendation only. Examine and diagnose the issue identified in the service request and advise the requestor of any issues identified as well as available courses of action.

Service for additional fee. Examine the issue identified in the service request and report a possible "out of scope" situation to the Client POC. If mutually determined that the work is out of agreement scope, work will only be completed via a separate agreement and for an additional fee.

Vendor Response:

Please attach any media or URL/website for review.

Propose costs of services:
(Please fill table below and include any other pricing for onsite/SOC/projects/etc…)

Description	Rate $
Example: Help Desk	$5,500/month
Example: Core Services (full stack support)	$100,000/year

References:

Describe fully the last three contracts performed by your firm that demonstrate your ability to provide the services included with the scope of specifications.

- Please include:
- Customer Name
- Contact Individual
- Telephone and e-mail
- Street Address
- Description of services provided including the contract amount, when provided, and project outcomes

Proposer Questionnaire

1. Does the organization fulfill all requirements described in "Baseline Requirements"? If not, what is missing?

FIRM BACKGROUND AND ORGANIZATION
2. Describe the organization, date founded, and ownership of your firm. If your firm experienced a material change in organizational structure, ownership or management during the past three years, describe the change.
3. Describe any other business affiliations. Please disclose current relationships (i.e. relationships with Microsoft, procurement arrangements, etc.).
4. Describe your firm's sources of revenue.
5. Did you, or will you, pay a finder's fee to any third party for business related to this account? Specify the recipients of any fee.

EXPERIENCE
6. Describe your firm's experience in managing IT functions for governmental entities and cyber security practices.
7. What is your firm's experience in developing policies, strategic plans and management guidelines?
8. Provide the number and types of accounts, and composition of IT services currently being managed by your firm.
9. Describe your firm's software support expertise; that is, for what software platforms can your firm provide support?

STAFFING
10. Identify and provide background information on the key person or personnel who take the most active role(s) in the administration and management of the firm.
11. Identify the IT professionals (managers, analysts, techs, etc.) employed by your firm, by classification, and specify the average number of accounts handled.
12. Provide resumes and biographical information on the professionals that will be directly involved in the decision-making process for the district. Include the number of years at your firm, total years of experience, and professional licenses and designation. Include the number of accounts managed and any limits on this.
13. Describe your firm's training and education efforts to keep staff informed of developments relevant to government IT.
14. Has there been any turnover of professional staff in the firm in the last three years assigned to public sector clients?