CAMROSA WATER DISTRICT

BUILDING WATER SELF-RELIANCE

Managed IT/OT Service Provider Request for Proposal

Proposals due: November 3, 2021, 4:00 P.M. PST

An informational meeting will be held **October 13, 2021 at 1:00 P.M. PST**
Finalist presentations will be held **November 17, 2021**, times TBD

RFP COORDINATOR:

Joe Willingham
IT Manager, Camrosa Water District
7385 Santa Rosa Road
joew@camrosa.com
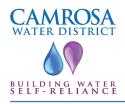(805) 340-4321

Issued Date: October 4, 2021

TABLE OF CONTENTS

1. Introduction

The Camrosa Water District (Camrosa) is pleased to invite you to respond to this Request for Proposal (RFP) for Managed Information Technology (IT) and Operation Technology (OT) Services. The intention of t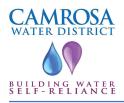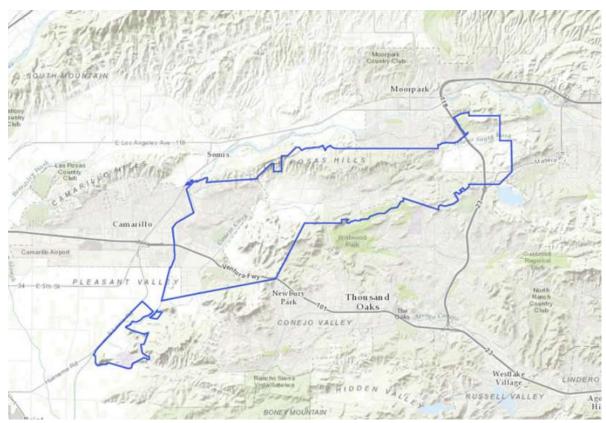his RFP is to solicit responses and formal proposals from qualified Managed IT/OT Services Providers (MSPs) and select a single organization to provide IT/OT services to the district. While the initial contract will be for a three-year period with the option to renew, the District is seeking a long-term relationship with the MSP to assume the bulk of IT/OT management indefinitely.

1.1 About Camrosa

The Camrosa Water District encompasses an area of about 31 square miles in the southern portion of Ventura County, California and services parts of Cities of Camarillo, Simi Valley, Moorpark and Thousand Oaks; and also services unincorporated areas of the County of Ventura including the Santa Rosa Valley. The District serves more than 30,000 people and delivers approximately 15,000 acre-feet of water each year. Camrosa delivers potable water, non-potable surface water, and recycled water produced at its Water Reclamation Facility. Wastewater collection and treatment services are provided in the central portion of the District and to California State University Channel Islands (CSUCI) and the County of Ventura.

Camrosa is a public agency created under the California Water Code. Currently the District has 25 full-time employees under the supervision of the General Manager, who in turn reports to a five-member Board of Directors, elected at large by the ratepayers to alternating four-year terms. The main driver for soliciting managed IT/OT services is to prepare for the imminent retirement of our current IT Manager and to backfill his responsibilities with a contracted firm. It is anticipated the MSP will overlap with the current IT Manager for a period of 2-4 months, after which the MSP will report to the General Manager. Staff management of the MSP will be subject to change as the relationship develops and Camrosa staffing evolves.

1.2 Purpose

With this RFP, Camrosa is requesting information about your company and the IT/OT products and solutions you provide as outlined in the Service Requirements section. This information will be gathered from several different organizations and used to evaluate provider options for Camrosa.

This RFP is issued solely for information and planning purposes. This document does not commit Camrosa to contract for any service, supply, or subscription whatsoever. Camrosa will not reimburse any information or administrative costs incurred as a result of participation in response to the RFP. All costs associated with response will solely reside at the responding party's expense.

1.3 Confidentiality Statement

All information included in this RFP is considered confidential and intended only for use by responders. No information included in this document, or in discussions related to Camrosa Managed Service Provider selection effort, may be disclosed to another party or used for any other purpose without express written consent from Camrosa.

2. Environment Overview

The information below outlines the general demographics of Camrosa and our current technical environment.

Office Locations:

- Main Office – 7385 Santa Rosa Road, Camarillo, CA 93012
- CWRF/RMWTP – 1900 S. Lewis Road, Camarillo, CA 93012
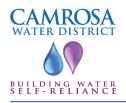
Number of Employees: 25

Remote Employees: 25 VPN capable

Current Technical Environment:

The Camrosa Water District is a small organization that fully leverages on technology when possible. Automation of SCADA tasks that monitor reservoir levels, which in turn, control drinking water wells and booster pump production; a robust high-speed communications infrastructure that supports both voice and data; a Microsoft Windows client/server network utilizing Active Directory for centralized administration; and virtual technology for an array of application servers are but a few examples.

Camrosa is primarily a Microsoft shop with a mix of physical host servers, domain controllers, virtual file and application servers, and workstations. There are no Unix based operating systems at Camrosa (however there could be, and most likely is, some Unix based firmware implementations on proprietary network hardware used at Camrosa).

The current MS Server version baseline is Windows Server 2016 Standard and Data Center with plans this fiscal year to migrate all host server environments to Windows Server 2019 Standard and Data Center. Virtual server machines are a mixture of Windows 2008, 2012, and 2016, depending on the installation date of the application server. Upgrading of these legacy VM server operating systems to MS Server 2019 is also of high-importance to the District. The current domain version is Windows Server 2016.

All client workstations are baselined at Microsoft Windows 2010 and latest patches are applied automatically. Where practical and feasible, Camrosa has steadily migrated its business applications to cloud hosting. A few of these applications include MS Exchange (email), Office365, One Drive, and SharePoint. Camrosa has also migrated it legacy hardware PBX and POTS phone system to Verizon's VOIP virtual PBX environment (Verizon Virtual Communications Express).

Regarding network topology, Camrosa maintains 10 Gbps IT and OT Local Area Networks (LANs) at its physical offices listed above and maintains a high-speed (300 Mbps) wireless backbone which consists of a partial mesh, microwave Wide Area Network (WAN) and provides coverage across the whole of the District. WAN connectivity is mainly used for OT purposes.

Being a retail water purveyor requires water storage at several reservoir sites at elevation. These sites consequently provide the District with excellent locations for wireless line-of-sight communications to pump stations and well sites, sewer lift stations, and other reservoir sites, all of which compose the Supervisory Control and Data Acquisition (SCADA) OT network.

Network switching, routing, and firewalling are a mixture of Fortinet and Cisco products. Separate VLANs are maintained to provide both logical and geographical separation of assets and to provide additional security, through policy-based access control, between IT and OT networks as well as between client and server VLANs.

Primary Internet connectivity is via a 200 Mbps fiber service through our primary Internet Service Provider (ISP) with a low-speed (4 Mbps) backup wireless internet connection provided by our secondary ISP.

Below is an inventory of hardware and software used at the District.

- **Hardware & Infrastructure**
  - 10 Physical Servers
    - 8, Host Servers for VMs/Backup Servers
    - 1, Domain Controller
    - 1, Dedicated Backup Server
    - 1, UHF Emergency Voice Gateway Server
  - 15 Virtual Machine Servers
    - 2, Virtual Domain Controllers
    - 8, IT Application Servers
    - 5, OT Application Servers
  - Workstations
    - MS Windows 10 Workstations
    - ~ 83 total between IT and OT networks

- Printers/Scanners
  - 1, Large Format Plotter
  - 1, Large Format Scanner
  - 1, High speed Scanner
  - 5, Enterprise Multi-Function LaserJet Printers
  - ~6, Desktop Laser Jet Printers
- Transmission Media
  - Cat5e/Cat6 UTP Cabling
  - OM-3, 62.5 Multimode Fiber Cabling
  - ~ 13, High Speed Microwave Backbone Radio Links
  - ~ 40, Low Speed (1.5 Mbps) UHF Radio Links (nodes for OT network)
- Switches
  - 2, 48-port 10GB Managed Switches
  - 2, 24-port 1GB POE Switches for physically separate VOIP distribution
  - ~ 20-30, 10-port managed and Unmanaged Switches at various sites
- Routing/Firewalling/Cyber Security
  - 6, physical router/firewalls
  - 1, Network analyzer providing log, alert, IPS/IDS management
  - Policy based ACL's
  - Client and Server SSL Certificates (TA and Self Signed)
  - Certificate and DDNS based authentication
  - Inter-VLAN routing between client/server and IT/OT networks
  - Cloud-based Endpoint Detection & Response (EDR) Managed Solution
  - Cloud-based Next Generation Anti-Virus (NGAV) Managed Solution
  - On Premise Antivirus & EDR
- Telephony
  - Verizon Communication Express (VCE) VOIP and Virtual PBX
  - ~ 25, VOIP desktop phones
  - 2, VOIP/POTS Gateways
  - 2, 24-port, 1GB POE switches to support VOIP phones
- Mobile Devices
  - ~12, Cell Phones
  - ~10, Tablets
  - ~10, Window 10 Laptops for Remote VPN Access
- Conference/Boardroom
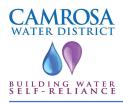 - Short-Throw Projector
  - A/V Equipment Rack

- Emergency Voice Communications
  - POTS/VOIP/SAT – to – UHF Gateway
  - ~ 12, Emergency UHF Voice Radios
  - 2, Fixed Emergency UHF Repeater Sites
  - 2, Satellite Phones
- Incident Command Center
  - 2, Large Screen Displays
  - 1, Short-Throw Projector
  - 1, 4X4 HDMI video switch
  - 2, Spectrum cable-boxes for news feeds
  - 4, Dell laptops
  - Video tie-in for SCADA displays
- SCADA
  - ~ 100-150, PLCs
  - 7, HMIs
  - 3, SQL Historian Servers
  - 1, Data Concentrator
- Automatic Meter Reading (AMR)
  - 1, Network Communication Controller (NCC) Server
  - 16, Data Collection Units (DCUs)
  - ~8,600 Meter Transmission Units (MTUs)
  - 3, Star Programmer Devices
- Corporate/Guest WIFI
  - 3, Corporate APs
  - 5, Guest APs
- **On Premise Application Servers**
  - Automatic Meter Reading (AMR)
  - Backup
  - Billing
  - Document/File Repository
  - Financial
  - Geographical Information System (GIS)
  - Hydraulic Modeling
  - Intranet
  - On Premise End Point Detection and Response (EDR)
  - SCADA MMI and Historian
  - MS SQL

- ➢ Whatsup Network Monitor
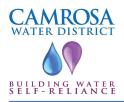- **Hosted (Cloud based) Applications**
  - ➢ External DNS
  - ➢ Cloud Backup
  - ➢ Managed End Point Detection and Response
  - ➢ O365 G3 Subscription
  - ➢ WWW
- **Workstation Applications (common)**
  - ➢ O365 Application Suite
  - ➢ MS OneDrive
  - ➢ Adobe Acrobat
  - ➢ ** Some workstations have additional applications installed depending on job duty*
- **Custom Software Executables, Scripts, Macros and Batch Files**
  - ➢ In-house developed, VBA Active X controls for various Excel functions & reports
  - ➢ In-house developed, ASPX Active Server Pages using VB/Java/C Scripts
  - ➢ Scheduled task (MS Task Scheduler for various routine reports
- **Internet**
  - ➢ Primary
  - ➢ Secondary (failover)
- **Remote Access / VPN**
  - ➢ MFA Team Viewer
  - ➢ MFA VPN
- **Third Party Support Contracts**
  - ➢ AMR
  - ➢ Autocad
  - ➢ Billing, Bill Printing, Customer Portal
  - ➢ EDR
  - ➢ External DNS & DDNS
  - ➢ Financial
  - ➢ GIS
  - ➢ Hosted MS Exchange
  - ➢ Network Analyzer
  - ➢ OpenText
  - ➢ Router/Firewall
  - ➢ Whatsup Gold Network Monitoring

3. Service Requirements

As part of this RFP, Camrosa has requirements for the following services. We realize that not every MSP will be able to provide all the services listed below, but we encourage you to respond regardless.

- **Help Desk Support:** The MSP should offer superior 24x7x365 Help Desk support from Tier One to Three services utilizing by industry best practice processes and procedures.
- **Server & Network System Monitoring:** The MSP must provide 24x7 monitoring of Camrosa's server & network system with proactive communication and escalation protocols based on the severity of any unscheduled outages.
- **Patch Management Services & Preventative Maintenance:** The MSP must provide management of critical security and system patches to all servers and systems on the network to ensure Camrosa's IT/OT systems and resources are properly managed and maintained.
- **Business Continuity and Disaster Recovery:** The MSP must be able to support Camrosa's ability to recover based on the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) agreed upon by organizational constituents. In addition, backup and redundancy should be used to support this need.
- **Remote Backup:** The MSP must execute a nightly backup plan for the critical servers, including a regularly-tested recovery process.
- **Email/Collaboration System Management:** Camrosa requires the management and administration of its cloud-based MS-Exchange email system, MS Office 365, MS Teams, and MS OneDrive environments for all users.
- **Antivirus, AntiSpam & Antispyware Protection:** Maintain Camrosa's existing defenses against security threats including phishing, malware, spam, viruses and to provide recommendations for enhancements to its existing cyber security systems.
- **On-Site Support:** When needed, the MSP should have the ability to deploy onsite resources to assist in issues which cannot be resolved through remote access to in-house systems.
- **Custom Application Support:** Provide technical support as needed for in-house developed software executables, scripts, macros and batch files. This task may include software modifications of source code and scripts to enhance current capabilities, debugging, and/or new software developments as well.
- **Networking Support:** Camrosa requires proactive management and monitoring of our switches, firewalls, routers and Wi-Fi systems, and other networking equipment as identified by Camrosa.
- **Security Systems Monitoring:** MSP must provide proactive monitoring and management of Camrosa's security systems, including firewalls, intrusion prevention, secure remote access, and any implementations of advanced security solutions Camrosa may utilize.
- **Vendor Management:** The MSP should be able to manage other vendors which may be contracted for by Camrosa and serve as the key point of contact unless escalated.

- **Warranty and Asset Inventory Management:** Camrosa expects the MSP to maintain a hardware and asset inventory that includes Desktops, Laptops, Servers, Printers/Scanners, Fax Machines, and notify Camrosa of any potential service or warranty issues. The MSP must also assist with managing the lifecycle of Camrosa devices and maintain an equipment inventory to ensure systems are always current.
- **Software Licensing Control:** Oversight of renewal of software application licensing, third-party support contracts, trusted authority SSL certificates and maintenance of appropriate documentation.
- **Procurement Management:** The MSP must assist with the selection of commercially rated equipment, order placement, order tracking, shipping, equipment returns, and sourcing and ordering of replacement parts.
- **PC Deployment:** Delivery and setup of machines on-site.
- **Desktop and Laptop Support:** MSPs must include their ability to support existing and future desktop and laptop hardware. This includes maintenance and repair, replacement for failed equipment, and the acquisition and provisioning for new equipment as needed.
- **Printers, Copiers and Scanners:** The MSP must be able to support existing printers, copiers and scanner related network-printing issues.
- **Desktop Software Standardization and Software Licensing and Upgrades:** MSP must have a process for identifying standardization and management of desktop images and ensuring that staff are using current products as well as current OS and browser versions.
- **Lifecycle Management of Hardware Units:** The MSP should have processes for end-of-life notification, replacement, and asset decommissioning/disposal.
- **Break Fixes and Installation:** The MSP should offer planned and on-call break/fix services, including emergency response to server issues.
- **Move, Add, Change (MAC):** Camrosa is looking for the MSP to help with any changes to the location, configuration of existing equipment or software, and installation of additional equipment or software as needed.
- **Mobile Device Support:** In addition to laptops and desktops, some staff use mobile phones and tablets. The MSP will need to support secure provisioning (and ongoing support of that provisioning) of any mobile device into the company network. In the event the device is lost, the corporate mail and contact data should be able to be easily wiped from the device while preserving individual's personal information. Camrosa is in the initial stages of implementing a Mobile Device Management (MDM) application. A MDM strategy and additional system recommendations should be considered and included in response to this RFP.
- **Reporting:** The MSP should provide relevant reporting not only based on their performance from a help desk perspective but also regarding system health, uptime, and assist in keeping an accurate hardware inventory to inform ongoing planning of maintenance, warranties, and refresh schedules. Please recommend a level and frequency of reporting, with reference to experience, that has worked well for previous/existing clients.
- **Technology Strategy Planning:** The MSP will work with Camrosa staff to develop a long-term strategic technology plan that specifically defines need and costs. The plan will take

advantage of new and existing technologies to produce a pragmatic and effective future roadmap that enables the organization to fulfill its overall mission plan.

- **Account Management:** The MSP must offer an internal escalation process in tandem with Camrosa to ensure the ability to have multiple points of contact available if needed depending on the items or issue encountered.
- **Project Management:** The MSP should be able to offer project management and technical engineering resources to assist with technical projects as identified by the MSP or Camrosa.
- **Solution Design:** The MSP must provide solution packages (e.g., hardware, software, licensing) and associated consolidation of data.
- **Service Levels:** It is anticipated that Camrosa and the MSP will coordinate on the development of objectives and expected levels of service and that the MSP will report back to Camrosa these levels of service on a regular basis.
- **IT Policy Development:** The MSP will be expected to develop customized policies related to the use of technology.
- **Hosting:** The MSP should offer services relative to hosting or co-location of equipment, either directly or through partners.
- **Onboarding and Offboarding Staff:** The MSP must have process and procedure in place to onboard or offboard Camrosa team members in a timely and efficient manner.
- **Compliance:** The MSP must use systems that comply with published Payment Card Industry Security (PCI) Standards. In addition, the MSP should also support rules and regulations as provided by relevant governing organizations as identified by regulatory or grant based requirements.
- **Scalability:** The MSP must be able to offer a model where scaling up or down from a systems and cost perspective is simple and nimble.
- **Multi-Factor Authentication (MFA):** MSP must be able to provide and manage a Multi-Factor Authentication (MFA) solution to provide an easy-to-use method to verify user identities at login and to protect logins with multi-factor authentication.
- **End-User Security Awareness Training:** The MSP should offer Security Awareness Training to teach Camrosa staff about current threats, terms, standards, and compliance to help them avoid a security incident.
- **Vulnerability Testing:** The MSP should offer vulnerability tests, both internally and externally, to determine what flaws and potential threats exist from the outside, or perimeter, of Camrosa's IT and OT networks.
- **Managed Security Operation Center (SOC):** The MSP should offer Managed SOC-as-a-Service to monitor Camrosa's environment and ensure proactive detection and response to threats, intrusions and attacks.
- **Special Projects:** The MSP should offer support as needed in the planning, development, and execution of special projects related to Informational and Operational Technology.
- **Presentations:** From time-to-time, the MSP may be required to develop and present presentations to Camrosa's Board of Directors for informational purposes related to IT/OT plans and projects.

4. Response Process

4.1 Pre-proposal Meeting/Presentation & Questionnaire

A pre-proposal meeting/walk-through will be provided. Please submit your Corporate Information (Attachment A) and response to Technical Questions (Attachment B) by email to the Primary RFP Contact listed below by the due date outlined in Section 6 below. In addition, please provide the contact details of the individual responsible for coordinating your RFP response. At the same time, we ask that you submit any clarification questions regarding the RFP.

4.2 Primary RFP Contact

Please direct all inquiries regarding this RFP to:

Joe Willingham, IT Manager
Camrosa Water District
joew@camrosa.com
(805) 340-4321

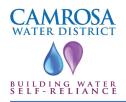## 4.3 Response Delivery Instructions

Camrosa requires responses to this request for proposal to be delivered electronically. You may attach documentation to support your answers, if necessary.

Please review the Key Dates in Section 6 below and submit all responses via electronic delivery no later than dates provided in the table to:

Joe Willingham, IT Manager
Camrosa Water District
joew@camrosa.com

Any response received after the delivery date specified, will not be considered without prior written approval.

Please complete the attached forms (Attachment A and Attachment B), a proposal document, and pricing breakdown.

Please submit a fee proposal, which includes billing rates and labor hours separated by task for key personnel and any subconsultants. Also, for each area of expertise, please provide a brief bio on key personnel that will be supporting Camrosa.

Proposers should carefully review this RFP and the CWD Procurement webpage at https://www.camrosa.com/procurement/. A Vendor Questionnaire, W-9, and insurance certificates will be required prior to signing an agreement. Please consult the "IT Consultant model agreement" (https://www.camrosa.com/wp-content/uploads/2021/10/IT-Consultant-Agreement.pdf) on the Procurement webpage. ***Submitting a proposal will be considered acknowledgment of your agreement with the terms and conditions in the model agreement.*** Comments on or objections to any terms of CWD's agreement must be made in writing and received with the proposal submission; if none, please note that in the proposal as well.

5. Selection Criteria & Process

5.1 Selection Criteria

Camrosa will evaluate the responses based on multiple criteria and will select the best overall solution to fit its needs. Camrosa is not obligated to select the lowest price bidder. All responses will be evaluated in the following areas:

- Completeness of solution
- Pertinent expertise and comparable experience
- Demonstrated customer service quality and support
- Previous relevant experience
- Vendor strength and stability
- Account management
- Reporting capabilities
- Financial considerations

5.2 Selection Process

All responses will be evaluated as received and included in the following process:

- Review and scoring of the responses, including any clarification requested by the evaluation team.
- Identification of 2–3 final candidates to conduct in-depth review of capabilities, including on-site interviews and presentations.

- Conducting of site visits and/or reference calls as deemed appropriate by the evaluation team.

5.3 Finalist Presentations

Our intention is to host presentations/demonstrations from no more than three finalists, in two-hour increments, on November 17, 2021. As soon as Camrosa completes our review and ranking, we will assign presentation times to the finalists. Camrosa will attempt to provide the finalist firms with as much advance notice as possible.
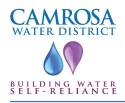
It is expected at this time that finalist presentations will be in person at the District office, 7385 Santa Rosa Road, Camarillo, CA 93012. Should our ability to host in-person meetings change due to public health restrictions regarding the COVID-19 pandemic, we will provide finalists with as much notice as possible as to preferred alternatives.

6. Key Dates

Below is a general timeline outlining the process steps with estimated dates for each step of the process. By participating in the RFP process, MSPs agree that they can adhere to the following general timeline and the meeting times they reserve through this process.

Task	Completion Date
RFP Distributed to MSPs	10/4/2021
Pre-proposal Meeting & Questionnaire	10/13/2021
Proposals Due from MSPs	11/3/2021
Response Analysis / Finalists Selection	11/9/2022
Finalist Presentations	11/17/2021
Award	12/9/2021

The pre-proposal meeting on October 13 at 1:00 P.M. is voluntary however, you are strongly encouraged to attend. It will be in-person and is intended to provide additional context about the District's decision to contract IT services, greater detail about the District's systems, and an opportunity for proposers to ask questions. **The questionnaire will be due by <u>11:59 P.M.</u> the same day**.

Proposals are due to Joe Willingham at JoeW@camrosa.com by 4:00 P.M. on November 3, 2021.

We expect to award the contract to the selected firm at the December 9, 2021 meeting of the Camrosa Board of Directors

Thank You

Camrosa looks forward to reviewing your response and would like to thank you in advance for your participation. The Managed Service Provider selection project is very important to our continued success and represents a major focus of effort for Camrosa. We appreciate and value your input, expertise, and feedback.

Attachment A

[MSP's completing the RFP must fill out this section.]

RFP Response Form: Corporate Information

Please provide the following information about your company.

1.0	Company Profile	
1.1	Company Name	
1.2	Company Address	
1.3	Contact Information (Party responsible for responding to this RFP)	
1.4	Company Webpage	
1.5	Main Products / Services	
1.6	Main Market / Customers	
1.7	Number of years in the Market	
1.8	When did you first start providing similar solutions?	
1.9	Company location(s)	
1.10	Number of Employees	
1.11	Number of Employees in Account Management	
1.12	Number of Employees in Technical Support	
1.13	Notable Acquisitions	
1.14	Key Business Partnerships	

2.0	Financial Information	
2.1	Previous year gross revenue	

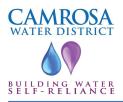|		
2.2	Previous year net income	
2.3	Return on investment	

Attachment B

[MSP's completing the RFP must fill out this section.]
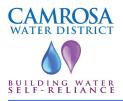
RFP Response Form: Technical Questions

Please provide responses to the questions below to the best of your ability.

1.0 General

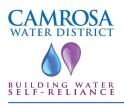|	
1.1	**Q. What are the general types of organizations your clients represent?** A.
1.2	**Q. Why do you believe that you are a good fit with our organization?** A.
1.3	**Q. Describe your onboarding/implementation process and approach if you were selected?** A.
1.4	**Q. Do you conduct Quarterly Business Reviews (QBRs) and what is the nature of those meetings?** A.
1.5	**Q. How do you typically work with IT Management at clients who have staff members?** A.
1.6	**Q. What do you feel your overall strengths and differentiators are?** A.
1.7	**Q. Do you serve clients with 24 X 7 requirements?** A.
1.8	**Q. What services do you offer besides the core services of a Managed Service Provider?** A.
1.9	**Q. What type of training do you offer either during onboarding or ongoing?** A.

| 1.10 | **Q. What do you feel are your biggest hurdles to a successful relationship?** |
| | A. |

| 1.11 | **Q. What training resources are available for team members?** |
| | A. |

| 1.12 | **Q. What type of general expertise can you provide in key technology areas?** |
| | A. |

| 1.13 | **Q. What IT and/or Cyber Security certifications does your staff hold (e.g. MCSE, CCNA, NSE, Security+, etc.)?** |
| | A. |

| 1.14 | **Q. What differentiates your organization from your competitors in the marketplace?** |
| | A. |

2.0 Processes

| 2.1 | **Q. Do you use in-house or contracted resources for services?** |
| | A. |

| 2.2 | **Q. Describe your process for migrating Camrosa to your organization?** |
| | A. |

| 2.3 | **Q. What Camrosa resources would you require (i.e., information, data, staff resources, communication) during initial migration and on an ongoing basis?** |
| | A. |

| 2.4 | **Q. Outline the methods by which clients can access you (i.e. online, by phone, etc.).** |
| | A. |

| 2.5 | **Q. Describe the escalation and account management process.** |
| | A. |

| 2.6 | **Q. Where is/are your support center(s) located?** |
| | A. |

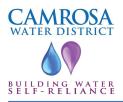| 2.7 | **Q. How involved is your team with creating project plans/testing during technical projects?** |
| | A. |

2.8	**Q. Do you follow Information Technology Infrastructure Library (ITIL) or other processes aligned with industry standard practices?** A.
2.9	**Q. Do you participate in drills or tests i.e. Disaster Recovery, Incident Response, etc.?** A.
2.10	**Q. How do you notify users of maintenance windows or system outages?** A.
2.11	**Q. What types of diagrams would you typically create/maintain?** A.
2.12	**Q. Do you offer knowledge bases for common issues and how are they utilized?** A.
2.13	**Q. What is your willingness or ability to support the security systems, phone systems, audio/visual systems?** A.
2.14	**Q. How often do you conduct Disaster Recover (DR) testing?** A.

3.0	Technology
3.1	**Q. What types of monitoring agents would you use for end user devices?** A.
3.2	**Q. What is the back-end help desk system you use?** A.
3.3	**Q. Do you offer managed firewalls or other managed technology?** A.
3.4	**Q. Do you offer Mobile Device Management (MDM) or other mobile management technology?** A.
3.5	**Q. Do you offer a Security Information and Event Management (SIEM) or other security-based technology?**

	A.
3.6	**Q. Do you have tools to provide system uptime metrics?**
	A.
3.7	**Q. What tools do you use for network monitoring?**
	A.
3.8	**Q. What tools do you use for system monitoring or general health level of end user devices?**
	A.
3.9	**Q. Do you offer or partner for laptop encryption?**
	A.
3.10	**Q. If hosting/co-location is an option please describe details of option i.e. services, vendor partners, etc.**
	A.

4.0	**Support**
4.1	**Q. Describe fully your technical support options including the assistance request process, escalation process, support hours, response times, staffing levels, staff expertise, and physical location of the help desk.**
	A.
4.2	**Q. Please provide details on your standard reporting capabilities.**
	A.
4.3	**Q. Describe any documentation and support (e.g., user manuals, online help, interactive dem[o] web-based seminars, and online knowledge base) that will be available, both from the techni[cal] perspective and the end user perspective.**
	A.
4.4	**Q. What options are available for user training and technical training that may be required by [your] staff?**
	A.

4.5	**Q. How do you monitor customer satisfaction and quality assurance on an ongoing basis and how might we benefit from this process?**
	A.
4.6	**Q. Camrosa's user base varies considerably in its level of technical sophistication. Please describe your experience in successfully supporting users that may be remote and possess limited technical skills.**
	A.

5.0   Pricing & Contracts

5.1	**Please attach cost estimates and worksheets to support estimates. Itemize non-recurring and recurring costs. Recurring costs should be quoted as per user per month costs. Other pricing models may be provided as an option.**

6.0   References

6.1	**Please provide at least three references for customers with similar operations to the proposed solution. Include contact names, phone numbers, email addresses and industry.**

Please provide any other information you feel should be considered in our evaluation.