MINNEHAHA CREEK WATERSHED DISTRICT
QUALITY OF WATER QUALITY OF LIFE

IT Managed Services

January 17, 2025
Questions and Responses

1. **Can you elaborate on any specific or special projects that you envision requiring the services of an MSP?**
   The District values a proactive Managed Services Provider (MSP) partner who can provide strategic guidance and hands-on support for projects to ensure long-term operational efficiency and security. These projects may include IT Infrastructure upgrades, cybersecurity enhancements, disaster recovery and business continuity planning, technology procurement support.

2. **Would you require Full-Time Equivalent (FTE) staff, remote support, or a combination of both?**
   The District primarily requires remote support for day-to-day IT operations, system monitoring, and troubleshooting. However, there are instances where on-site support is necessary for tasks such as hardware installations, network maintenance, and critical issue resolution. Therefore, we seek a MSP that can offer a flexible support model—delivering reliable remote support while also providing on-demand on-site assistance as needed.

   At this time, we do not require dedicated Full-Time Equivalent (FTE) staff on-site but value the ability to scale support based on project demands or unforeseen technical issues.

3. **What monitoring tools are currently being used within your IT infrastructure?**
   We are committed to ensuring effective system performance, security, and network reliability. Monitoring is managed by our current MSP but we are open to evaluating and implementing industry-standard monitoring solutions recommended to strengthen our infrastructure monitoring and management capabilities.

4. **Regarding equipment management, maintenance, and replacement, would you prefer the MSP to procure replacement products on your behalf or simply recommend the necessary replacements for you to purchase?**
   The District prefers the MSP to procure replacement products on our behalf. This approach streamlines the procurement process, ensures compatibility with our existing infrastructure, and leverages the MSP’s expertise in selecting cost-effective, high-quality solutions.

We value an MSP that can manage the entire lifecycle of equipment—handling sourcing, purchasing, installation, and configuration—while maintaining transparency in pricing and adhering to our procurement policies and requirements that apply to the District as a public agency. Collaboration on product recommendations and budget considerations is also important to ensure that all purchases align with the District's operational needs and fiscal responsibility.

5. **You mentioned that the current antivirus solution is provided by your existing MSP. Could you clarify its validity period? Would you like the new MSP to provide a fresh antivirus solution, or do you plan to continue with the existing one?**
   The District is open to evaluating its current antivirus solution and would rely on the expert recommendation of the selected MSP to determine the best path forward. This may include continuing with the existing solution if it meets our security needs or transitioning to a more effective, up-to-date solution based on the MSP's assessment.

6. **How many resources are currently provided by your MSP, including both FTE and remote support staff?**
   The District currently receives as-needed support from our existing MSP and does not have any designated Full-Time Equivalent (FTE) staff assigned to our account. Support is provided through a combination of remote assistance and on-site visits, when necessary, based on the nature and urgency of the issue.

   We value a flexible support model that can scale to meet our operational needs and are open to discussing the most effective resource allocation with the selected MSP.

7. **What is the Budget of the Project?**
   This request is for ongoing IT support and managed services, not a one-time project. As such, there is no fixed project budget. The District is seeking a cost-effective, scalable service model that aligns with our operational needs and fiscal responsibility.

   We welcome detailed pricing proposals that reflect transparent, competitive rates for ongoing support, with clear breakdowns of any one-time, recurring, or variable costs.

8. **How many hours per week do you require the services of an IT professional, 20 hours or 40 hours? Additionally, what is the weekly hour requirement for an account manager?**
   The District does not have a set hourly requirement for IT professional services or account management. The level of support needed will depend on the volume and complexity of tickets and service requests. Our primary expectation is for the MSP to deliver timely, responsive, and effective support as issues arise.

   For account management, we expect proactive communication, regular updates, and availability to discuss ongoing needs or project planning, but we do not have a predefined number of hours allocated. We value a flexible service model that can scale support based on our operational demands.

9. **What are the storage policies for these sectors in terms of the frequency of backup?**
   We would welcome the selected MSP’s recommendations on establishing or improving backup strategies to ensure data integrity, security, and quick recovery in the event of data loss or system failure. Further details can be provided or discussed during the onboarding process.

10. **On average, how many tickets and changes are made per week on the network and VM infrastructure?**
    The District makes infrequent changes to our network and VM infrastructure. Most of our IT support needs are related to routine maintenance, troubleshooting, and user support rather than frequent infrastructure modifications.

    However, we expect the MSP to be prepared to handle infrastructure changes as needed, particularly during system upgrades, security enhancements, or project implementations.

11. **Who will manage the service provider?**
    Tessa Vacek, Administrative Services Manager will be the point of contact and managing the service provider.

12. **Who is the existing IT vendor company, and has there been any dissatisfaction with their performance? If so, what specific issues have been encountered?**
    Our current provider is Solution Builders. This request for proposals is not prompted by dissatisfaction with the current vendor.

13. **What is the monthly/annual amount of the existing IT support contract (public information)?**
    Monthly Fee is $3,770.00

14. **Could you provide insights into how accountability will be upheld, and what metrics will be used to measure success?**
    Accountability will be upheld through regular monthly meetings with the MSP to review:
    - Closed Tickets: Evaluation of resolved issues, including the nature of the problems and how they were addressed.
    - Resolution Times: Assessment of how quickly and effectively support requests are resolved, ensuring alignment with agreed-upon service level agreements (SLAs).
    - Outstanding Open Tickets: Discussion of ongoing issues, their status, and plans for resolution.

A key performance metric will be the tickets per endpoint per month, with a target ratio of 0.3 or below to ensure proactive system management and minimize recurring issues. Additional success metrics may include:

- Average response and resolution times
- System uptime and availability
- User satisfaction feedback

15. **What would you consider problems/failures in communication?**

Clear, consistent, and proactive communication is essential to maintaining an effective partnership and ensuring timely issue resolution. Problems or failures in communication would be:

- Lack of timely follow-up
- Inability to reach support staff or account representatives, especially during urgent or high-priority situations
- Slow acknowledgement or response to service requests that impact operations
- Providing unclear or incomplete information
- Failure to properly escalate critical issues

16. **Who will be the primary point of contact for the service provider?**

Tessa Vacek, Administrative Services Manager will be the point of contact and managing the service provider.

17. **Are there any upcoming IT projects or system enhancements planned outside of the replacement timelines listed?**

Yes, the District is currently exploring the implementation of Microsoft Teams Phones to enhance communication and collaboration across the organization. Additionally, there will be a need to upgrade certain systems to Windows 11 to ensure compatibility, security, and optimal performance.

We anticipate that the selected Managed Services Provider (MSP) will play a key role in supporting these initiatives by providing technical guidance, managing deployment, and ensuring a smooth transition with minimal disruption to operations.

18. **Are there any plans to adopt cloud-based solutions or hybrid systems for specific applications or workloads?**

We are open to exploring cloud or hybrid solutions if they align with our operational needs, security requirements, and budget considerations. We welcome recommendations from the selected MSP on how cloud-based technologies could enhance efficiency, scalability, and data security for the District.

19. **Is there a strategy for transitioning all devices to Windows 11 in the future?**

The District is aware of the need to transition all devices to Windows 11 and plans to collaborate with the selected MSP to develop and implement a comprehensive migration strategy.

20. **Are there plans to include iPads under a management contract for better oversight and control?**
There are currently no formal plans to include iPads under a management contract; however, the District is open to exploring this option. We recognize that managing mobile devices through a structured solution could enhance security, oversight, and operational efficiency.

21. **How is the integration between the databases (e.g., GIS, Laserfiche, and ElementsXS) managed?**
The integration between the District's databases—such as GIS, Laserfiche, and ElementsXS—is currently managed by their respective separate vendors. The MSP is not responsible for directly managing these databases but is expected to provide technical support and assistance when needed. This support may include:
    - Coordinating with database vendors to troubleshoot integration issues or system performance concerns.
    - Assisting with network connectivity, system compatibility, and infrastructure support related to these platforms.
    - Offering guidance on security measures and best practices to ensure smooth operation between systems.

    The MSP's role will be to ensure that the overall IT environment supports the optimal functioning of these systems without assuming direct database management responsibilities.

22. **Are there any challenges or limitations with the SonicWall Global VPN Client (GVC) for remote users?**
At this time, the District is not aware of any challenges or limitations with the SonicWall Global VPN Client (GVC) for remote users. It has been functioning as expected in supporting secure remote access.

23. **Have there been any issues with managing the switches under different vendor contracts?**
At this time, the District is not aware of any issues with managing switches under different vendor contracts. The current setup has been functioning effectively without any reported challenges.

    However, we welcome the selected MSP to review our network infrastructure and provide recommendations to ensure continued efficiency, seamless management, and proactive issue prevention.

24. **Are there plans to upgrade the Comcast fiber internet connection if higher bandwidth is required?**
The District's current Comcast fiber internet connection is performing sufficiently for our operational needs. However, if future demands require higher bandwidth, we are open to upgrading the internet connection to ensure continued performance and reliability.

We would rely on the selected MSP to monitor network performance, identify any capacity limitations, and provide recommendations for scaling bandwidth to support growth and evolving technology requirements.

25. **Are legacy systems like Windows Server 2012 R2 and associated VMs presenting any security or compatibility concerns?**
    At this time, the District is not aware of any security or compatibility concerns related to legacy systems such as Windows Server 2012 R2 and associated virtual machines (VMs).

26. **Are there additional cybersecurity measures in place to complement endpoint antivirus?**
    In addition to endpoint antivirus protection, the District has implemented multi-factor authentication (MFA) to enhance account security and protect against unauthorized access. While these measures provide a solid foundation, we are committed to continuously improving our cybersecurity posture. We are open to exploring additional security solutions and welcome recommendations from the selected MSP to further strengthen our overall security framework.

27. **Referring to the equipment list within the RFP under the Systems Overview: are respondents expected to price the listed planned replacements into our bids? Or is that procurement already planned and separate from this RFP and only mentioned for respondents to consider labor effort required to tackle those projects?**
    Respondents are not expected to include pricing for the listed planned replacements in their proposals. These items were provided solely for transparency to give insight into the anticipated workload and upcoming projects.

    The procurement of those planned replacements has not yet begun. We expect the selected MSP to actively support the District in this procurement process by offering technical guidance, product recommendations, purchasing agreed upon products on our behalf and assistance with implementation planning.

28. **Under System security: What if any vulnerability scanning solution is currently used? Is this leased via the current MSP or do you possess the licensing information yourselves?**
    The District currently does not possess its own licensing for a vulnerability scanning solution. We would expect the selected MSP to implement and manage a comprehensive vulnerability scanning solution as part of their security services.

29. **Same question set, for Anti-malware solutions?**
    The District currently does not possess its own licensing for an anti-malware solution. We would expect the selected MSP to implement and manage a robust anti-malware solution to protect our systems from viruses, ransomware, and other malicious threats.

30. **Who is your current MSP? Can you share the last month's or year's performance metrics against things such as availability, or response time, or mean time to resolve, or any other performance metrics you might have recorded to track satisfaction with their services?**
Our current provider is Solution Builders. This request for proposals is not prompted by dissatisfaction with the current vendor. At this time, we do not have formal performance metrics readily available to share. However, we monitor service quality through factors such as issue resolution times, system availability, and responsiveness to support requests.

31. **Can you share the last month's or year's expenses on the MSP?**
Our monthly fee is $3,770.00.

32. **What kind of patching products do you currently use? MECM(formerly SCCM)? Puppet? Terraform? Something else? Nothing?**
Currently, the District is not aware of any specific patching products being used for system updates and maintenance. We expect the selected MSP to manage and implement a comprehensive patch management solution to ensure all systems remain secure, up-to-date, and compliant.

33. **Ticketing – What ticketing system is currently in use? Does that system go away with the current MSP or is it on-site?**
The District's current ticketing system is provided and managed by our existing MSP. We expect the selected MSP to provide a comparable ticketing system that allows for:
    - Efficient submission and tracking of support requests.
    - Prioritization and escalation of issues based on urgency.
    - Transparency and reporting on ticket status, resolution times, and support trends.
    - User-friendly access for staff.

    The system should support timely and effective communication, ensuring that IT issues are managed and resolved promptly.

34. **Average # of monthly tickets and their severity?**
The District averages approximately 30 support tickets per month. The severity of these tickets can vary; however, the majority are typically low to moderate in severity and are easily resolved within a short time frame.

    While most tickets are minor, we expect the MSP to have the capability to prioritize and escalate critical issues when necessary to ensure minimal disruption to operations.

35. **The RFP called attention to the Data Practices Act – is MCWD currently in compliance with this and other data regulations you are aware of governing your organization? Does MCWD have a compliance officer, or program?**

Yes, the District is currently in full compliance with the Minnesota Government Data Practices Act and all other applicable data regulations governing our organization. We have a designated responsible authority and the District maintains internal processes and protocols to ensure ongoing compliance and to safeguard sensitive information.

The selected MSP will be required to maintain Data Practices Act compliance, support District compliance, and otherwise follow best practices for data security, privacy, and regulatory standards.

36. **Current SLAs or SLOs in place with your existing MSP? Are they meeting? Exceeding? Underperforming?**
This request for proposals is not prompted by dissatisfaction with the current vendor. They are meeting the standards in the SLA/SLO.

37. **Current IT Challenges: What specific challenges or pain points is the District currently facing with its IT infrastructure and services?**
At this time, the District is not experiencing any specific challenges or pain points with its IT infrastructure and services.

However, we are committed to continuously improving our IT operations to ensure efficiency, security, and scalability. We welcome the selected MSP to proactively assess our systems and provide recommendations for enhancements, emerging technology adoption, and best practices to support the District's long-term goals.

38. **Success Metrics: How will the success of the IT managed services provider be measured over the contract period?**
The success of the MSP will be measured through a combination of performance metrics, project execution, and service quality throughout the contract period. Key success indicators include:

- Tickets Per Endpoint Per Month: Maintaining a ratio of 0.3 or below to ensure proactive issue management and minimize recurring problems.
- Project Delivery: Successful completion of projects, delivered on schedule and within budget while meeting project objectives and quality standards.
- Ticket Response and Resolution Times
- System Uptime and Reliability
- Proactive Communication and Reporting
- Regular updates through monthly performance reviews, covering ticket resolution, system health, and any outstanding issues.
- User Satisfaction: Positive feedback from District staff on the MSP's responsiveness, professionalism, and overall service quality.
- Compliance and Security: Ongoing support in maintaining compliance with data security regulations and implementing best practices for cybersecurity.

39. **Integration with Existing Vendors: Can you provide more details on how the IT managed services provider will be expected to collaborate with other vendors, particularly those involved in the IT systems update?**
We would expect the MSP to collaborate closely with all vendors involved in the IT systems update to ensure seamless integration and minimal disruption. Providing system integration support, security and compliance oversight, technical support and issue resolution.

40. **Data Security and Compliance: Are there any specific compliance requirements or data security standards that the provider must adhere to, beyond those mentioned in the RFP?**
The District prioritizes adherence to industry best practices for data security, privacy, and regulatory compliance. Providers should be prepared to follow applicable federal, state, and local regulations related to data protection, cybersecurity, and public sector IT operations. If there are any additional requirements beyond those specified in the RFP, we would look to the MSP to provide guidance, recommendations and implementation.

41. **Preferred Communication Channels: What are the preferred channels and frequency for communication and reporting between the IT managed services provider and the District?**
The district values clear, consistent and transparent communication.
<u>Communication Channels</u>:
    - Email: for routine updates, non-urgent requests, formal documentation
    - Phone: for urgent matters or detailed discussions requiring immediate attention
    - Ticketing system/Service Portal: for logging, tracking and managing IT Support requests and incidents

    <u>Reporting Frequency</u>:
    - Monthly Meetings to review closed tickets, resolution times, and discuss any outstanding open tickets. This space would also be used to discuss strategic IT planning and continuous improvement opportunities.

42. **Budget Constraints: Are there any budget constraints or considerations that the provider should be aware of when proposing fees and expenses?**
As a public entity, the District has a responsibility to manage taxpayer dollars with transparency, accountability and fiscal responsibility. Therefore the MSP should be mindful to be cost-effective (competitive and reasonable pricing that balances quality service with cost-efficiency), have a transparent pricing structure (avoid hidden fees or ambiguity), and offer solutions that are scalable and flexible to adapt to the District’s evolving needs without incurring significant additional costs.

43. **Special Projects: Can you provide examples of potential special projects that the IT managed services provider might be asked to consult on?**
    Potential examples include:
    - Server Infrastructure Upgrade
    - Microsoft Teams Phone System Implementation:
    - Windows 11 Migration
    - Assessing and upgrading network components (switches, firewalls, wireless access points) to enhance speed, security, and reliability.
    - Cybersecurity Enhancements and training
    - Disaster Recovery and Business Continuity Planning
    - Assisting with the creation and enforcement of IT policies and procedures.

44. **Transition Process: What is the expected timeline and process for transitioning from the current IT managed services provider to the new one?**
    The District will rely on the selected MSP to develop and present a comprehensive transition timeline and plan. This plan should ensure a smooth, efficient, and secure transfer of services from the current provider with minimal disruption to daily operations.

45. **Feedback and Improvement: How does the District handle feedback and continuous improvement with its service providers?**
    The District values open communication and collaboration with its service providers to ensure high-quality service and continuous improvement. Our approach to handling feedback and fostering improvement includes:
    - Monthly meetings to review service performance, ticket resolution times, system health, and any outstanding issues.
    - Discussion of metrics such as tickets per endpoint per month (target ratio of 0.3 or below) to track service effectiveness.
    - Open Communication Channels
    - Issue escalation and resolution
    - Post-project debriefing

46. **Long-term Vision: How does the District envision its IT infrastructure evolving over the next few years, and how can the provider support this vision?**
    The District envisions its IT infrastructure evolving to become more secure, scalable, and efficient over the next few years, with a focus on supporting operational growth, enhancing cybersecurity, and leveraging modern technology.

47. **How many user/mailboxes do you have? Would you like having a back up of those?**
    We would look to the selected MSP to:

    - Assess the current email environment and confirm the number of mailboxes.

- Recommend and manage a reliable and scalable email backup solution that protects against data loss, accidental deletion, and security threats.
- Ensure that the backup strategy complies with industry best practices and relevant data retention policies.

48. **Is there a move forward plan with your department to address outdated and unsupported technology, or would that be a series of projects that you would like us to assist with?**
The District recognizes the importance of addressing outdated and unsupported technology to maintain security, efficiency, and operational effectiveness. While there is currently no formal, comprehensive plan in place, we anticipate that this will be addressed through a series of targeted projects in collaboration with the selected MSP.

49. **Do you require a SQL DBA or do just need server maintenance of the SQL server?**
The District primarily requires SQL Server maintenance rather than a dedicated SQL Database Administrator (DBA). The selected MSP will be expected to:
    - Perform routine maintenance tasks such as backups, updates, and patch management.
    - Monitor SQL Server performance and optimize configurations for reliability and efficiency.
    - Ensure security best practices are followed
    - Troubleshoot and resolve SQL-related issues as they arise.

    While advanced database development or complex query optimization is not currently needed, we would rely on the MSP to provide guidance or escalate to a DBA resource if specialized support becomes necessary.

50. **For the vulnerability scanning, at what level/scale are you expecting? We offer everything from PC scanning through our antivirus tool to network pin testing.**
The District expects a comprehensive approach to vulnerability scanning to ensure the security and integrity of our IT infrastructure. The selected MSP should provide a solution that balances thorough security coverage with cost-effectiveness and operational efficiency.

51. **What do you need as far as incident management is concerned? We have a few different offerings, and want to make sure we are getting you what you would like/need.**
In terms of incident management, the District is seeking a structured and proactive approach from the MSP to effectively identify, respond to, and resolve IT incidents with minimal disruption to operations. Key expectations include:
    - Clear Incident Classification and Prioritization:

    - A system for categorizing incidents by severity and impact (e.g., critical, high, medium, low).
    - Prioritizing incidents to ensure timely response to urgent or business-critical issues.
- Timely Response and Resolution
- Comprehensive Tracking and Documentation: Use of a ticketing system to log, track, and manage incidents from reporting to resolution.
- Post-incident reviews for major issues to evaluate the response, identify lessons learned, and improve future incident handling.
- 24/7 Monitoring for detection of system issues, security threats and performance disruptions

52. **For Asset Management of your environment, how often/how many assets do you normally deploy at a time? Is there an image that is already created, or would you need us to create one for you?**
    The District typically deploys a small number of assets at a time, with deployments occurring as needed rather than on a fixed schedule. The volume of deployments is generally limited to routine replacements, new hires, or project-specific needs.

    We currently have a standardized system image in place for device deployments. This image includes the approved operating system, essential software, and security configurations to ensure consistency, security, and efficiency across all devices.

53. **For your Vulnerability Scanning , How many IP's do you have within your current network.**
    We have 14.

54. **For antivirus, how many Operating Systems or endpoints are currently within your network.**
    We currently have approximately 35 endpoints.

55. **What in more detail are you looking for with security policy guidance including password protection**
    The District is seeking comprehensive security policy guidance to strengthen its overall cybersecurity posture, with a particular focus on areas such as password protection, access control, and data security. The selected Managed Services Provider (MSP) will play a key role in developing, reviewing, and implementing these policies to ensure alignment with industry best practices and compliance requirements.

56. **When you talk about incident management, can you elaborate what you are looking for in this?**
    SEE QUESTION 51.