Request for Proposals (RFP)

Managed IT Services

Village of Ossining

ISSUE DATE:

Monday, January 24, 2022

SUBMISSION DATES:

Intent to Respond and Questions Due: **January 28, 2022**
Responses Due: **February 11, 2022**

Office of the Village Manager, 16 Croton Avenue, Ossining, NY 10562

OR kdattore@villageofossining.org

Mayor Rika Levin

Deputy Mayor Manuel R. Quezada

Trustee Robert M. Fritsche

Trustee Omar Lopez

Trustee Dana White

www.villageofossining.org

The Village of Ossining
RFP for Managed IT Services
Village of Ossining

The Village of Ossining (VOO) is inviting responses to this Request for Proposal (RFP) for Managed IT Services. VOO will review responses and formal proposals from qualified Managed IT Service Providers (MSPs) and select a single organization to provide IT services to VOO.

The Village of Ossining

The Village of Ossining is looking for IT services to manage five Village owned sites (Ossining Police Department, Justice Court – Town of Ossining; Village Hall, The Joseph G. Caputo Community Center, the John Paul Rodrigues Operations Center and the Indian Brook Water Treatment Plant) and one Town of Ossining owned site (the Town of Ossining Highway Department). For purposes of this RFP, VOO shall refer to IT services provided to the Village of Ossining (VOO); the Ossining Police Department (OPD); and the Town of Ossining (TOO).

Under the supervision of the Village Manager, the selected MSP will provide IT services to the VOO. It is anticipated that, subject to approval by the Board of Trustees, the selected MSP will begin providing IT services on or about March 1, 2022.

In-House IT Support

The VOO and the OPD each employ a full-time IT Technical Support Specialist who is responsible for providing all areas of computer related technical support including installation, maintenance and troubleshooting of personal computers, peripherals, applications software and telecommunications equipment and services. The Technical Support Specialists also manage local area network projects and provide training on basic computer usage, applications software and telephone systems for internal staff. The Technical Support Specialists will work closely with and will coordinate with the MSP to ensure comprehensive IT support services. The Technical Support Specialists will serve as Tier 1 support and be the single point of contact with the IT MSP for any issues that require escalation or assistance of the MSP. Users will not be authorized to contact the MSP directly for service.

Purpose

The VOO is requesting information about companies and IT products and solutions that meet needs outlined in the Service Requirements section.

This RFP is issued solely for information and planning purposes. This document does not commit the VOO to contract for any service, supply or subscription whatsoever. VOO will not reimburse any information or administrative costs incurred as a result of

participation in responding to the RFP. All costs associated with response will solely reside at the responding party's expense.

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 the VOO Managed Service Provider selection effort, may be disclosed to another party or used for any other purpose without the express written consent of the VOO.

Minimum Qualifications

1. Vendor is to have been in operation for at least five years.
2. Vendor is to have a local presence with the ability to provide an onsite support person in two hours if needed.
3. Vendor is to have a Cybersecurity and Commercial General Liability policy with limits of liability to be no less than $3 million per claim, event or occurrence, and contain no sub limits.
4. Vendor is to have a documented and demonstrable information security program and policy.
5. Vendor is to have independent information and cybersecurity assessments performed on an annual basis by a reputable provider.

Service Locations Requiring Management

I. Village of Ossining – Village Hall – 16 Croton Avenue, Ossining, NY 10562
Number of Users: 28
Number of Desktops: 51
Number of Servers: 6

II. Village of Ossining Police Department – 88 Spring Street, Ossining, NY 10562
Number of Users: 61
Number of Desktops: 31
Number of Servers: 6

III. Justice Court – Town of Ossining – 86 Spring Street, Ossining, NY 10562
Number of Users: 5
Number of Desktops: 8
Number of Servers: 1

IV. **John-Paul Rodrigues Ossining Operations Center – 101 NYS Route 9A, Ossining, NY 10562**
Number of Users: 69
Number of Desktops: 32
Number of Servers: 3

V. Joseph G. Caputo Community Center – 95 Broadway, Ossining, NY 10562
Number of Users: 20
Number of Desktops: 13
Number of Servers: 0

VI. Water Treatment Plant – Indian Brook Service Rd, Ossining, NY 10562
Number of Users: 6
Number of Desktops: 6
Number of Servers: 1

VII. Town of Ossining Highway Department, 85 Old Route 100, Briarcliff, NY 10510
Number of Users: 16
Number of Desktops: 7
Number of Servers: 0

VIII. Dale Cemetery Town of Ossining, 104 Havell Street, Ossining, NY 10562
Number of Users 2
Number of Desktops 2
Number of Servers 0

IX. Village of Ossining Fire Headquarters, 21 State Street, Ossining, NY 10562
Number of Users 1

Service Requirements

As part of this RFP, the VOO is requesting the following services.

I. Account Management – The MSP must offer an internal escalation process in tandem with the VOO to ensure the ability to have multiple points of contact available if needed depending on the items or issue encountered.

II. Technology Strategic Planning – The MSP will work with designated VOO staff to develop a long-term strategic technology plan that enables the organization to fulfill its mission in the community. Quarterly meetings are to be held to track progress with the strategic plan and make any necessary adjustments inclusive of budgetary considerations.

III. Help Desk Support - The MSP should offer 24x7x365 Help Desk support services.

IV. On-Site Support –The MSP will provide an onsite resource two days a week to facilitate with various projects. The MSP should have the ability to deploy additional onsite resources as needed to assist with issues or projects that require additional onsite support.

V. Service Levels – The MSP must be able to provide the following minimum service response times:

- Critical Issues – 1 hour.
- Non Critical Issues – 4 hours.

VI. Server, Network, End User Device System Management and Monitoring – The MSP must provide proactive 24x7 management and monitoring of the VOO; OPD server, network, and end user systems with proactive communication, response and escalation protocols based on the severity of any unscheduled outages.

Note – Device support includes printers, copiers, scanners and fax machines.

VII. Patch Management Services & Preventative Maintenance – The MSP must provide management and monitoring of critical security and system patches to all servers and systems on the network to ensure VOO's IT systems and resources are properly managed and maintained. The patching frequency should at a minimum meet the following requirements for security related updates:

- Server OS and Third Party Application Patches – Monthly
- Workstation OS and Third Party Application Patches – Monthly
- Network Devices – Quarterly

Any critical security vulnerability that has a probability of being exploited to gain access to the VOO systems and data must be patched immediately independent of the operating system or device.

VIII. Backup and Recovery – The MSP must execute a daily backup plan for the critical servers, including a regularly-tested recovery process. The backup plan must include an offsite component that is deemed to be ransomware resilient.

IX. Business Continuity and Disaster Recovery – The MSP must be able to support VOO's and OPD's ability to recover based on the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) agreed upon by organizational constituents.

The MSP will provide at a minimum, one annual disaster recovery test with the VOO.

Note: In October 2021, VOO signed a one year agreement with a vendor for back-up and disaster recovery services. It is the expectation of the VOO that the MSP selected will assume responsibility for this service at the end of the current contract.

X. Remote Access Management –The MSP must provide assistance in the identification, deployment and management of secure remote access solution.

XI. Malware and Virus Protection – The MSP must actively deploy and monitor a solution or series of solutions to manage the threat of malware or viruses. The MSP should provide options for both traditional anti-virus and a more robust Endpoint Detection and Response platform such as SentinelOne, Carbon Black, Crowdstrike, etc.

XII. End-User Security Awareness Training – The MSP must offer platform-based Security Awareness Training to teach VOO staff and employees about current threats, terms, standards and compliance to help them avoid a security incident. The platform should also have the ability to facilitate phishing exercises on a monthly basis. .

XIII. Security Systems Monitoring – The MSP must provide proactive monitoring and management of VOO's security systems, including firewalls, intrusion prevention system, secure remote access and any implementations of advanced security solutions VOO may utilize.

XIV. Asset Inventory Management – The MSP must maintain a hardware and asset inventory that includes Desktops, Laptops, Servers, Printers/Scanners and Fax Machines, The MSP will assist in tracking warranty status and asset age to facilitate the yearly asset retirement and replacement process.

XV. Software Licensing Control – The MSP will facilitate the management of software licenses for which the MSP is the reseller of the software or administrator of.

XVI. Procurement Management – The MSP must assist with the selection of server or network related equipment and software.

XVII. Network and System Documentation – The MSP must develop and maintain network and system documentation. A copy of the documentation is to be provided separately to the VOO for continuity purposes.

XVIII. Reporting – The MSP must 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. On a monthly basis, the MSP is to provide to the Village Administrator, management reports that depict the following:

1. Patch Status of all Workstation and Servers
2. Backup and Offsite Replication Status
3. AV or EDR Solution Status

XIX. Vulnerability and Threat Monitoring (Optional) - The MSP should have the capability to provide vulnerability detection and response services, such an SIEM, or SOC as A Service solutions. The MSP should provide pricing for this service as an optional item.

Response Process

Notification of Intent to Respond and Clarifying Questions

Please indicate your intention to respond to this RFP by email to the Primary RFP Contact listed below by the Intent to Respond and Questions Due date of January 28, 2022.

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.

Primary Contact and Response Delivery Instructions

The VOO requires responses to this request for proposal to be delivered in writing. You may attach documentation to support your answers, if necessary.

Please submit all responses via electronic delivery no later than February 11, 2022 to:

Karen D'Attore
Village Manager
kdattore@villageofossining.org
914-941-3554

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

Please complete the attached forms (Attachment A and Attachment B), a proposal document, pricing breakdown, and a version of any master services agreement or other contract that would be utilized if chosen.

Selection Criteria & Process

Selection Criteria

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

• Completeness of solution
• Expertise and experience
• Demonstrated customer service quality and support
• Previous relevant experience
• Vendor strength and stability
• Account management
• Reporting capabilities
• Financial considerations

Selection Process

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

- Review and scoring of the responses, as well as clarification of information as deemed necessary by the evaluation team.
- Identification of 2–3 final candidates to conduct in-depth review of capabilities, including interviews and presentations.
- Conducting on site visits and/or reference calls as deemed appropriate by the evaluation team.

Finalist Presentations

Our intention is to hold presentations/demonstrations with one or more firms as indicated in the Key Dates table. The presentations will be held online via Zoom.

Key Dates

Below is a general timeline outlining the process steps, with estimated dates for each step. 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.

RFP to be issued	**1/24/22**
Intent to Respond and Questions Due	**1/28/22**
Responses Due	**2/11/22**
Finalist Interviews/Presentations	**Week of 2/21/22**

Conditions

Village Administration, along with Corporation Counsel, will conduct preliminary evaluations of all submissions for compliance. Any submissions that do not comply with the requirements of the RFP may be disqualified.

Village staff may wish to conduct interviews with candidates following RFP submission. These interviews may be for clarification of details within the submission, to learn more about the proposed approach or fee schedule. The VOO also reserves the right to share RFP results with members of VOO staff, VOO boards and committees and community partners as part of the deliberation process.

Once consensus is reached, Village staff will make a recommendation to the Village Board of Trustees and contract negotiations may begin. Prior to contract execution, the VOO reserves the right to halt or terminate negotiations at any time.

Thank You

The Village of Ossining looks forward to reviewing your response and would like to thank you in advance for your participation. We appreciate and value your input, expertise and feedback.

Attachment A

RFP Response Form – Corporate Company Profile

Company Name:	
Company Address:	
Contact Information (Party Responsible for RFP response):	
Company Webpage:	
Main Products/Services:	
Main Market/Customers:	
Number of years in the Market:	
When did you first start providing similar solutions?	
Company location(s):	
Number of Employees:	
Number of Employees in Account Management:	
Number of Employees in Technical Support:	
Notable Acquisitions:	
Key Business Partnerships**:**	

Attachment B

RFP Response Form: Questions

1.0 General

1.1 What are the general types of organizations your clients represent?

.

1.2 Why do you believe you are a good fit with our organization?

1.3 What do you feel your overall strengths and differentiators are?

1.4 Do you serve clients with 24 X 7 requirements?

1.5 What services do you offer besides the core services of a Managed Service Provider?

1.6 What type of training do you offer either during onboarding or ongoing?

1.7 What training resources are available for team members?

1.8 What type of general expertise can you provide in key technology areas?

1.9 Do you use in-house or contracted resources for services?

2.0 Processes

2.1 Describe your process for migrating VOO to your organization?

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

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

2.5 Describe the escalation and account management process.

2.6 Where is/are your primary support center(s) located that will service the VOO?

2.7 Do you follow ITIL or other processes aligned with industry standard practices?

2.8 How do you notify users of maintenance windows or system outages?

2.9 Do you offer knowledge bases for common issues and how are they utilized?

3.0 Technology

3.1 What types of monitoring agents would you use for end user devices?

3.2 What is the back-end help desk system you use?

3.3 Do you offer managed firewalls or other managed technology?

3.4 Do you offer MDM or other mobile management technology?

3.5 Do you offer an SIEM or other security-based technology?

3.6 Do you have tools to provide system uptime metrics?

3.7 What tools do you use for network monitoring?

3.8 What tools do you use for system monitoring or general health level of end user devices?

4.0 Support

4.1 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 to satisfy the onsite requirements of the VOO.

4.2 Please provide details on your standard reporting capabilities separate from the requirements noted in the RFP.

4.3 Describe any documentation and support (e.g., user manuals, online help, interactive demos, web-based seminars and online knowledge base) that will be available, both from the technical perspective and the end user perspective.

4.4 What options are available for user training and technical training that may be required by staff?

4.5 Describe any user groups, websites, newsletters, conferences or any other means you support for sharing information and soliciting service feedback.

4.6 How do you monitor customer satisfaction and quality assurance on an ongoing basis and how might we benefit from this process?

4.7 The VOO 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.

5.0 Pricing & Contracts

5.1 Please attach cost estimates and worksheets for the following:

- The cost of monthly management, maintenance and support.
- Any one time initial assessment and onboarding fees. The associated fee should include a description of what the onboarding process fee includes.
- Hourly rates for services not included as part of the monthly management and support. Note – Respondents should clearly specify what is not included and will incur additional fees.

Optional Items to include pricing for:

1. EDR Solution Implementation
2. 24X7 Security Monitoring via SIEM or SOC as A Service
3. Any other item respondent believes will benefit the VOO.

5.2 Please attach a Master Services Agreement or other legal documents beyond a proposal which accompany a proposal.

6.0 References

6.1 Please provide at least three to five references for municipal clients where similar services were provided. Please include contact names, phone numbers, email addresses.

The RFP response should be accompanied by a letter from the responding party's principal stating that they are authorized to bind the company to the information in the proposal, and that your firm will be able to assume the role of Managed IT Service Provider to the VOO on or about March 1, 2022.

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

Appendix C Security

The Security of the VOO will be very much influenced by the security of the selected MSP. As such, it is the requirement of the VOO that the chosen MSP have a defined information security program to manage their own internal risk and the risk they present to the VOO as a by product of the services they are to provide.

Will Vendor use any multi-tenant customer management software to manage the environment, e.g. Connectwise?			
a	If Yes, please describe.		
b	Are employees provided unique accounts?		
c	How many employees will have access to manage the devices?		
d	What is the password policy?		
e	Is multi-factor authentication enabled?		
f	How is the platform monitored for unauthorized access?		
Does Vendor plan to use any subcontractors that will be granted access to or may impact, directly or indirectly, the Organization's systems and data?			
a	If Yes, please describe the relationship and role.		
b	Will contractual terms be established with the subcontractor regarding the protection of the Organization's systems and data?		
c	Has due diligence been performed on the subcontractor to ensure a reasonable security program?		
	i.	If yes, please describe the due diligence performed and when?	
Has Vendor experienced a breach or material cybersecurity incident in the last 24 months?			
a	If yes, please describe.		
Please provide a description of Vendor's cybersecurity program. The description should address the following key areas (*note* – the more information that can be provided the better):			
a	Are all employees subject to background checks?		
b	Does Vendor have a code of conduct policy?		
	i.	If yes, please provide a copy.	
c	Does Vendor have a comprehensive set of information security policies and standards? Please list and provide a copy of the policies.		
d	Are employees required to read and agree to the policies and standards?		
e	Does Vendor have cybersecurity insurance?		
	i.	Please describe the coverage.	
f	Does Vendor have professional liability insurance?		
	i.	Please describe the coverage.	

g	Does Vendor have a business continuity and disaster recovery plan? (Specifically in the context of being able to continue to provide their services to the Organization?)			
h	Does Vendor have an incident response plan?			
	i.	If yes, does it include notification to the Organization should it impact them?		
i	Are Vendor employees required to undergo cybersecurity awareness training?			
	i.	If yes, what frequency and what topics?		
	ii.	Is phishing testing part of the training?		
j	Are Vendor systems patched on a monthly basis for operating system and third party application vulnerabilities?			
	i.	Is the process centrally monitored to ensure patch distribution and installation?		
k	Are removable devices prohibited or controller?			
	i.	Please describe.		
l	Are laptops and portable devices encrypted?			
m	Does Vendor have a mobile device management solution for smart phones, etc.?			
	i.	If yes, does it require devices to have the following controls?		
		1	Password or PIN?	
		2	Idle period timeout?	
		3	Encryption?	
n	Does Vendor perform periodic, risk assessments, vulnerability scans and/or penetration tests of their environments?			
	i.	Please describe the testing performed and the frequency?		
	ii.	Is the testing independent?		
o	Vendor requires long and complex passwords that change on periodic basis. Please provide the requirements:			
	i.	Minimum length		
	ii.	Complexity		
	iii.	Expiration		
	iv.	Account lockout threshold		
	v.	Account lockout duration		
p	For any remote access into Vendor's environment is Two Factor Authentication required? (This in inclusive of any VPN or Web based email access, e.g., OWA.)			
q	Vendor deploys anti-virus for its workstations and servers.			
	i.	Is it centrally monitored?		
	ii.	Are alerts configured for high risk events?		
	iii. Is an EDR solution implemented? Please describe the product implemented.			

r	Does Vendor have a process to change any of the Organization's administrative passwords used by Vendor upon termination of an employee with access to those passwords?		
	i.	What is the standard timeframe to do so?	
s	Does Vendor monitor their network and endpoints for anomalous or malicious activity?		
	i.	Please describe the tools and processes. Specifically the SIEM used.	
t	Does Vendor securely manage and store Organization administrative passwords?		
	i.	Please describe how passwords are managed and stored?	
u	Will all passwords used in support of the Organization's environment be unique to the Organization? (i.e., Vendor does not use the same password for administrative accounts across their client base for any purpose.)		