Town of

Wilmington

May 30, 2025

Request for Proposal

IT Services Proposal Date Due: <u>June 26, 2025 at 12:00 (noon)</u>

Contact:　　　　Scott A. Tucker, Town Manager
　　　　　　　　2 East Main Street, PO Box 217
　　　　　　　　Wilmington, Vermont 05363
　　　　　　　　802-464-8591, x-123
　　　　　　　　jarchambault@wilmingtonvt.us

The Town of Wilmington, Vermont, is an equal opportunity employer and is committed to equal opportunity in its contracting process.

Introduction

The Town of Wilmington (Town) is soliciting proposals from qualified Managed Security Service Providers (MSSP) for Information Technology (IT) support services; providers must be familiar and compliant with State of Vermont CJIS (Criminal Justice Information Services) requirements. The Town would initially like to keep their present system, and incorporate options to newer standards. The Town currently uses Unifi network, switch and router. The Town has a local server running Windows Essentials. The Town may be open to cloud-based options. The Town is looking for services for FY-2026 (July-June), with option of services for two subsequent fiscal years.

Current Environment

The number of computers vary by department: Police (7 in office; 7-mobile with VPN), Fire (2), Water (1), Sewer (2), Admin (6), Clerk (3), Highway (1). Admin computers are laptop and set-up for remote work. Firewall; Carbonite; Open VPN; Microsoft Firewall; Ransomware – Crypto Prevent. Server runs Windows Essentials; UniFi network equipment (switch, access point, router). Local, no cloud services other than cloud back-up. Proposal should include the cost of an initial audit and inventory of the current environment as a base starting point.

Services Required

The following details the services that prospective service providers should consider providing to the Town in the area of information technology services. The prospective service provider may propose to provide either a set of services or all of the services described below:

Network & Systems Administration

Scope of activity includes all town equipment including servers, switches, firewalls, routers, and other security devices. Primary maintenance including regular analysis, routine configuration changes, and installation of patches and upgrades. Alert notifications to designated personnel in the event of failure. Complete proactive monitoring of network equipment including bandwidth utilization, and other performance indicators, with reporting when specified thresholds are reached. Network performance and capacity management services, and network troubleshooting. Maintain network documentation and procedures.

Managing computer systems and networks to include complex application, database, messaging, web and other servers and associated hardware, software, communications, operating systems necessary for the quality, security, performance, availability, recoverability, and reliability of the system. Ensure scheduled preventive maintenance for equipment is properly and promptly performed; maintain the maintenance records on the equipment; develop operations, administrative, and quality assurance back-up plans and procedural documentation.

Setup new users and edit or remove existing users' environments. Server performance and capacity management services with reporting when specified thresholds are reached. Configuration management, including changes, upgrades, patches, etc. Support of other specialized software products as it relates to the server(s) and associated hardware. Management of user logins and security.

Coordinate, repair, and maintenance work with contracted repair vendors and ensure repairs are conducted in a timely fashion. Primary installation and maintenance of printers, network copiers/scanners, etc. is primarily accomplished with local IT vendor and/or office personnel.

Help Desk
Diagnose and correct desktop applications issues, configure all computers for standard applications; identify and correct end user hardware problems and perform advanced troubleshooting; install PC's, laptops, tablets, printers, peripherals, and software. Respondents shall have access and be available during normal business hours (8am-5pm, Monday through Friday) with after-hours support with mission critical issues (i.e., Police Dept.).

Onsite Support
Onsite support is provided through a local vendor; performs basic onsite support for the Town including but not limited to onsite troubleshooting, printer maintenance, setup and maintenance of IT devices and basic installation and support for day-to-day software. Local IT support must have authority to interface with selected vendor for this proposal of IT Services.

Application Support
Perform basic support functions in cooperation with local IT vendor and/or office personnel, including installing desktops, laptops, printers, peripherals, and office automation software; training and educating users; diagnosing and correcting application problems, configuring laptops and correcting end user hardware problems, and performing advanced troubleshooting. Maintain an up-to-date

inventory of computer related hardware. Maintain and update application licensing in accordance with the needs of the Town.

Security: Monitoring and Firewalls

Monitoring information leaving and coming into the Town is very important when dealing with sensitive information. Identifying issues early helps prevent them further down the road and can save the Town a large amount of capital. Typically, monitoring traffic, deploying a Firewall, and blocking suspicious Sites is the bare minimum. Maintenance of virus detection programs on servers, email, computers and laptops. Perform security audits as requested and notify personnel immediately of suspected breaches of security or intrusion detection. Configure system to enable secure remote access and provide secure remote administration.

Security: Policies and Password Management

Scope of these actions should include creation and/or implement security policies that meet the needs of the Town. Policies must be clearly linked to security and/or best security practices and not hamper the Town's ability to function. Upon installation, documentation must be made in a fashion that allows continued maintenance and effective use of solution.

Security: Secure Connections

The scope of the actions taken should implement solutions targeted at securing wireless connection and/or VPN connections in order to secure traffic to the network. These solutions should be targeted at securing access to these networks for employees not physically connected to the Town's network (i.e. remote access). If an alternative solution or hardware is required to achieve a potential solution the Town will be advised on the best course of action.

Security: Data and Machine Protection/Preservation

Data and Machine protection / preservation is very important within an enterprise when looking at the types of issues that can occur. Making sure confidential information and data is being preserved during a disaster or cyber-attack scenario is of utmost importance. Machines and Data should be protected and preserved at all costs and plans should be in place to ensure the protection and preservation of these items.

Business Continuity and Disaster Recovery

System Failures and Business Continuity

Scope of activity should include a plan of action and protocols in case of system failures. Provide detailed response services if workstations fail or software becomes corrupt. Create protocols in case of system failures and methods to prevent possible failures. Advise town staff of possible system and software issues and who to contact when system failures occur.

Physical Disasters and Recovery

Scope of activity should include back-up storage services which provide onsite and offsite

backup. Provide detailed disaster recovery services if a primary hosted solution should be unavailable. Create protocols in case of disaster and methods to prevent possible future disasters.

Cyber Attacks
Scope of activity should include plan of action and protocols in case of a cyber-attack. Provide detailed response services if a threat is detected and or, an attack is carried out. Create protocols in case of attack and methods to prevent possible attacks. Advise town staff of possible threats and the importance of security.

Strategic Planning
Engineering, planning, and design services for major system enhancements, including installations and upgrades of new or existing systems. Examples include major server upgrades, storage system upgrades, redesign of backup systems, etc. Provide technical leadership. Make recommendations for future purchasing and technology needs. Install new servers, software and hardware and transfer data when acquired. Strategic planning, design, and installation/upgrade of core network systems.

Network and Hardware Assessment
Compile/update inventory of all information technology related assets. Assess system architecture and current processes and make recommendations for improved IT systems performance. Vendors may propose alternative services or hardware, if the vendor can demonstrate alternatives that will significantly improve information technology (IT) effectiveness, enhance its quality of services, minimize its support cost, and maximize return on investment in IT.

Security and Vulnerability Assessment
Compile and assess the network's security vulnerabilities and potential attack vectors. Potential penetration testing if the Town requests. Vendors may propose alternative security services, if the vendor can demonstrate alternatives will significantly improve overall security, decrease vulnerabilities, minimize its support cost, and ensure a secure and efficient network.

Training
Cybersecurity awareness training, incorporating simulated phishing tests, requesting assistance, basic understanding of security risks and how to best avoid them.

Alternatives
Vendors may propose alternative services, if the vendor can demonstrate alternatives will significantly improve information technology (IT) effectiveness, enhance its quality of services, minimize its support cost, and or maximize return on investment in IT. Vendors may propose pricing tiers or bundled vs. a la carte options.

Submittal Requirements

Letter of Transmittal

The letter is not intended to be a summary of the proposal itself. The letter of transmittal must contain the following statements and information:

Company name, address, and telephone number(s).

- Name, title, address, e-mail address, and telephone number of the person or persons to contact who are authorized to represent the firm and to whom correspondence should be directed.
- Briefly state your understanding of the services to be performed and make a positive commitment to provide the services as specified.
- The letter must be signed by a corporate officer or other individual who is legally authorized to bind the applicant to both its proposal and cost schedule.
- Statement which indicates proposal and cost schedule shall be valid and binding for ninety (90) days following proposal due date and will become part of the agreement that is negotiated.

General Vendor Information

Please provide the following information:

1. Length of time in business of providing proposed services
2. Total number of clients
3. Number of full-time personnel in: Consulting, installation, training, sales, marketing, and administrative support
4. Office location(s) which would service this account

Positioning and Experience

Describe how your firm is positioned to provide either a set of services or all the services listed above. Provide a history of experience on providing similar services.

Approach and Methodology

Describe your approach to providing these services and your methodology for providing on-going support.

Provide References

Provide three (3) references from other small municipalities. Please provide information referencing the actual services provided, customer size (number of users), and the length of tenure providing services to this client.

Staff Resources

Identify names of principals and key personnel who will actually provide the information technology services. Summarize the technological expertise of these staff. Describe the role and responsibilities that each of these individuals will have.

Nonperformance

If your company has had a contract terminated for default during the past five years, all such incidents must be described. Termination for default is defined as notice to stop performance due to the vendor's nonperformance or poor performance; and the issue was

either (a) not litigated or (b) litigated, and such litigation determined the vendor to be in default. If default occurred, list the complete name, address and telephone number of the party.

Summary

Summarize your proposal and your firm's qualifications. Additionally, you may articulate why your firm is pursuing this work and how it is uniquely qualified to perform it. Include other pertinent information that may help Town of Wilmington determine your overall qualifications. Your proposal summary is not to exceed two pages.

Cost of Services

The proposal must contain a fee schedule that includes fixed rate business hours support and hourly rates for additional services.
1. Describe how your services are priced, and any specific pricing you can provide.
2. Define any additional charges (e.g., travel expenses).
3. If pricing will change for subsequent years, include in proposal.
4. Invoicing should be done on no less than a monthly basis with sufficient detail to verify completed work.

Evaluation Criteria and Process

A selection committee will conduct an evaluation of proposals and will rate each submittal based upon the following criteria:
1. Experience
2. Understanding of services to be provided
3. Personnel expertise
4. Compatibility with end users
5. Project approach
6. Satisfaction of clients/end users
7. Cost

Miscellaneous

The Town of Wilmington reserves the right to reject any and all proposals for failure to meet the requirements contained herein, to waive any technicalities, and to select the proposal which, in the Town's sole judgment, best meets the requirements of the project.

This RFP creates no obligation on the part of the Town to award a contract or to compensate the proposer for any costs incurred during proposal presentation, response, submission, or presentation. The Town of Wilmington reserves the right to award a contract based upon proposals received without further discussion or negotiation. The Town further reserves the right to make such an investigation as it deems necessary to determine the ability of proposers to furnish the required services, and proposers shall furnish all such information for this purpose.

Proposals must specifically identify any portions of their submittals deemed to contain confidential or proprietary information, or trade secrets. Those portions must be readily separable from the balance of

the proposal. Such designations will not necessarily be conclusive, and proposers may be required to justify why the Town should not, upon written request, disclose such materials. Under Vermont's Public Records Law, the Town of Wilmington must provide the public with access to Town records, unless the records are protected from disclosure under specific exemptions in the Law. The Public Records Act definition of 'public record' includes digital documents stored in both public and private accounts, but it extends only to documents that otherwise meet the definition of public records.

Insurance Requirements Upon Contract Approval

Certificate of Liability Insurance in the minimum amount of $1,000,000 (certificate should name the Town of Wilmington as an additional insured for the work the contractor will be doing). In addition, a Certificate of Worker's Compensation Insurance is required.