# IT Services RFQ Template Options Catalog

## Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of contents</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>How to Use This Catalog</td>
<td>2</td>
</tr>
<tr>
<td><strong>1.0 Systems and Network Support</strong></td>
<td>3</td>
</tr>
<tr>
<td>1.1 Network &amp; Systems Administration</td>
<td>3</td>
</tr>
<tr>
<td>1.2 Help Desk</td>
<td>4</td>
</tr>
<tr>
<td>1.3 Onsite Support</td>
<td>5</td>
</tr>
<tr>
<td>1.4 Application Support</td>
<td>6</td>
</tr>
<tr>
<td>1.5 Hosting and Cloud Services</td>
<td>7</td>
</tr>
<tr>
<td><strong>2.0 Security</strong></td>
<td>8</td>
</tr>
<tr>
<td>2.1 Monitoring and Firewalls</td>
<td>8</td>
</tr>
<tr>
<td>2.2 Security Policies and Password Management</td>
<td>9</td>
</tr>
<tr>
<td>2.3 Secure Connections</td>
<td>10</td>
</tr>
<tr>
<td>2.4 Data and Machine Protection/Preservation</td>
<td>10</td>
</tr>
<tr>
<td><strong>3.0 Business Continuity &amp; Disaster Recovery</strong></td>
<td>11</td>
</tr>
<tr>
<td>3.1 System Failures &amp; Business Continuity</td>
<td>12</td>
</tr>
<tr>
<td>3.2 Physical Disasters &amp; Recovery</td>
<td>12</td>
</tr>
<tr>
<td>3.3 Cyber Attacks</td>
<td>13</td>
</tr>
<tr>
<td><strong>4.0 Strategic Planning</strong></td>
<td>14</td>
</tr>
<tr>
<td>4.1 Network and Hardware Assessment</td>
<td>14</td>
</tr>
<tr>
<td>4.2 Security and Vulnerability Assessment</td>
<td>15</td>
</tr>
<tr>
<td>4.3 Projects</td>
<td>16</td>
</tr>
<tr>
<td><strong>5.0 Training</strong></td>
<td>17</td>
</tr>
</tbody>
</table>

This document was developed by faculty, staff and students from the Champlain College Leahy Center for Digital Forensic & Cybersecurity in collaboration with the Vermont League of Cities and Towns.
Introduction

This catalog is designed to be used in conjunction with the accompanying IT Services Request for Quote (RFQ) template. It describes service options for desired solutions and provides technical language to request those services. Each section breaks down service options and asks questions that assist the RFQ preparer in selecting the solution module(s) that fit their need(s). Solution modules are designed to be copied into Section 3 of the RFQ template. Please note, this catalog is intended to provide guidance for a range of services that different municipalities may need, so you need to evaluate which options meet your specific needs and only includes those in your RFQ.

The RFQ template specifies the process and terms of the engagement and asks the responding vendor to describe their business and their proposed solution(s). The template includes standard RFQ language, and you should customize it to fit your municipality's specific requirements. Once completed, your RFQ is ready to send to vendors. Remember to update the RFQ template with your municipality’s name in the body of the document as well as the header and footer, replace the logo too and double check formatting.

How to Use This Catalog

This catalog is modular and designed as a self-guided tool that asks a series of questions that determine the need for a particular service. Each section has four parts: Guiding Questions, Description, Key Terms, and Insert.

To begin, find what you are interested in requesting and work your way down the list of questions. If you find yourself saying you do not need that service, simply move on to the next section. If you are more technical, scan the Table of Contents and skip directly to the section that addresses your need.

When a section is applicable, copy and paste only the section labeled INSERT into Section 3 of the RFQ template. After pasting, be sure that the auto numbering of the section is correct.

Then, move to the next section.

IMPORTANT NOTES

1. The RFQ template is in Microsoft Word format (.DOCX). To preserve formatting and the Table of Contents, be sure to use MS Word to edit the template.
2. In the RFQ template, leave the section titled “Alternatives” as your last subsection of Section 3.
1.0 Systems and Network Support

Do you need network administration or help desk support for your town? This section covers services that address ongoing day-to-day and ad hoc, on-demand IT needs.

1.1 Network & Systems Administration

GUIDING QUESTIONS

- Are you interested in full time network and systems support?
- Are you interested in part time network and systems support?

DESCRIPTION

Network Administrators are the backbone of an information technology (IT) infrastructure. They are technical people who manage the hardware and software and who collaborate with internal technical and non-technical staff, and who interface with external vendors. Network Administrators also assist with planning, design and implementation, and ensuring that the network is highly available and secure. Some sample tasks of the Network Administrator:

- Maintaining computer networks and systems including software, firewalls, and other physical hardware
- Installing and configuring network equipment to update or fix hardware or software issues
- Updating virus protection software to keep data and communications protected
- Monitoring computer systems to improve network performance for computer systems and networks
- Communicating networking issues to other employees and management
- Employee training including technology usage and security best practices
- Fixing software and hardware issues for users on-demand or from inspection of the systems
- Network design, installation, and management
- Managing backups and backup integrity
- User and workstation management and administration
- Documentation of systems and networks
- Managing network access and credentials

KEY TERMS
**1.2 Help Desk**

**GUIDING QUESTIONS**

Are you looking for support for more day-to-day technical needs? The ability to call for help and get a reliable, timely response.

Do you have remote assistance/support?

**DESCRIPTION**

Help Desk technicians often do troubleshoot and support for devices like laptops, printers and Wi-Fi. Helpdesk can also be useful for software and application installation and troubleshooting. When a problem does arise that is out of their depth they can contact further support like network administrators or external network support.
### KEY TERMS

- Workstation troubleshooting
- Printer and Fax troubleshooting and support
- Software installation
- Wi-Fi Troubleshooting
- Escalation of issues
- Setting up new laptops and computers

### INSERT

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, phones (physical and software), peripherals, and software. Respondents shall have access and be available during normal business hours (8am-5pm, Monday through Friday) with after-hours support as required (additional costs may vary).

### 1.3 Onsite Support

#### GUIDING QUESTIONS

- Are you looking for regular, scheduled on-site support and technical needs?
- Do you want a technician to visit on a regular basis to address “punch list” items?
- How fast would you like on-site support to respond?

#### DESCRIPTION

On-site support technicians are often called in to help and troubleshoot issues that can only be resolved through in-person support. Depending on the particular type of issue, an enterprise may want on-site support that is able to respond to problems within a rather short period of time depending on the priority of the issue. Response times can range from within the day to a week or more for lower priority issues.

#### KEY TERMS

- In person troubleshooting
- Printer maintenance
- Setup and maintenance of PC’s, laptops, tablets, printers, phones
- Install and basic configuration of software
1.4 Application Support

GUIDING QUESTIONS

Are you interested in managed application support?
Who is called when issues with business applications occur?

DESCRIPTION

Managed application support is utilized to provide help and troubleshoot issues involving business applications and processes that are used on a daily basis. Depending on the particular issue, an enterprise may want application support to be able to respond to problems within a short period of time. Depending on the issue, managed application support can typically be done remotely over the Internet through connecting to enterprise workstations.

KEY TERMS

- Application Licensing
- Cloud Services
- Email
- Microsoft Office Suite
- Zoom and other virtual meeting software
- Application authentication and credentials
- Who to call for application support

INSERT

Perform basic support functions 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
1.5 Hosting and Cloud Services

GUIDING QUESTIONS

Does your organization have services in the “cloud” including file storage and applications like QuickBooks and NEMRC?

If your Town/City has cloud services, how is it supported and by whom?

Do you understand the benefits and drawbacks that cloud services can provide?

DESCRIPTION

Cloud hosting lets your town/city have services that are provided by a third party who host physical servers and services for you. Most hosting companies manage the servers and services themselves while letting the client use the service or server that they have purchased.

Examples of things that are hosted in the cloud can be found below.

KEY TERMS

- Office 365: Outlook
- Website hosting
- Google cloud
- Dropbox
- NEMRC cloud
- Database Management
- Accounting

INSERT

Hosted environment will be private cloud or dedicated hosting, to meet data security requirements of the City/Town. Hosted services cannot be in the public cloud. The hosting facility will have an appropriate security environment, as well as redundant internet connectivity and power. The environment will include current services and be easily expandable. If hosted/cloud services are already in place, support and management options should be outlined in the RFQ response.
# 2.0 Security

## GUIDING QUESTIONS

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you interested in full managed security support for your town?</td>
<td></td>
</tr>
<tr>
<td>What is most important to the town that needs to be protected?</td>
<td></td>
</tr>
<tr>
<td>What is the most vulnerable currently?</td>
<td></td>
</tr>
<tr>
<td>Is there a policy in place for secure termination of employees?</td>
<td></td>
</tr>
<tr>
<td>Does proper sanitization of data and hardware take place on retired hardware?</td>
<td></td>
</tr>
</tbody>
</table>

## DESCRIPTION

This section covers security and backups to ensure a reliable and resilient IT infrastructure. Security is a key part of maintaining a functional reliable network. Without proper security, every part of your organization is put at risk.

## 2.1 Monitoring and Firewalls

## GUIDING QUESTIONS

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does your town/city have a firewall to protect against Internet intruders?</td>
<td></td>
</tr>
<tr>
<td>Is the firewall regularly updated?</td>
<td></td>
</tr>
<tr>
<td>Do you monitor your systems and what is happening on them?</td>
<td></td>
</tr>
<tr>
<td>Are you interested in blocking malicious sites?</td>
<td></td>
</tr>
</tbody>
</table>

## DESCRIPTION

Monitoring is key to understanding what is happening with your IT infrastructure and device. Monitoring allows you to identify malicious behavior and use that information to prevent further damage. Firewalls and Site blocking is a great line of defense against unwanted traffic and malicious content. Monitoring in conjunction with firewalls can help prevent attacks and aid in dealing with any threat that gets through.

## KEY TERMS

- Firewall
- Monitoring
- Site Blocking
Monitoring information leaving and coming into the enterprise is very important when dealing with sensitive information. Identifying issues early helps prevent them further down the road and can save your enterprise 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.

2.2 Security Policies and Password Management

GUIDING QUESTIONS

Do you have security policies in place for your town/city?
Are you enforcing strong passwords and keeping them safe?
Would multi-factor authentication be something you want to implement?
Does your computer auto lock after leaving it unattended?
Do you wish to implement greater security measures in terms of employee network certification?
Do you wish to implement certain data and access restrictions per employee?

DESCRIPTION

Security policies and strong passwords are some of the best ways to keep your data and devices secure. Multi-factor authentication is as simple as typing in a 4-digit code from your phone but it can help keep your account safe even if someone has access to the password. These solutions can often be cheap and highly effective when it comes to maintaining security.

KEY TERMS

- Password Solutions
- Multi-Factor Authentication
- Security Policies
- Ensuring computers automatically lock
- Enforce strong passwords

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

2.3 Secure Connections

GUIDING QUESTIONS

<table>
<thead>
<tr>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is your city/town interested in having remote workers connect securely to the office?</td>
</tr>
<tr>
<td>Are you confident that your wireless network is secure and isolates the “guest network”?</td>
</tr>
</tbody>
</table>

DESCRIPTION

Securing the traffic on a network is a great way to improve overall security. Monitoring and controlling Wi-Fi and internet access can be an effective line of defense against nefarious traffic and unwanted users. A VPN is a virtual private network that provides an encrypted connection for all devices connected to the network. VPNs allow computers outside of the network to connect as if they are on the network. This is a solid way to improve security for remote workers.

KEY WORDS

- VPN - connecting to the office securely
- Wi-Fi Access control

INSERT

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 users not physically connected to the town/cities network. If an alternative solution or hardware is required to achieve a potential solution the town/city will be advised on the best course of action.

2.4 Data and Machine Protection/Preservation

GUIDING QUESTIONS

<table>
<thead>
<tr>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of data protection and preservation do your devices have?</td>
</tr>
<tr>
<td>Does your town have managed security support?</td>
</tr>
<tr>
<td>Do you have antivirus software and if so is it effective?</td>
</tr>
</tbody>
</table>
Data / Machine protection and preservation are one of the most important tasks an enterprise should take into consideration when they are dealing with sensitive information. Ensuring that workstations are secure and protected against malicious attacks remain highly important, and having a plan in place to preserve data in case of emergency.

**KEY TERMS**

- Data Protection
- Data Preservation
- Managed Security support
- Antivirus

**INSERT**

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.

### 3.0 Business Continuity & Disaster Recovery

**GUIDING QUESTIONS**

Are you interested in full disaster recovery procedure implementation?
Do you have a plan for data recovery in case of a disaster?
Do you have a written plan to keep the office running when a disaster strikes?
Do you have a plan to manage a cyber-attack?
Will you pay the ransom or not?
This section covers system failures, physical disasters and cyber-attacks.

3.1 System Failures & Business Continuity

GUIDING QUESTIONS

What happens when a hard drive becomes corrupted in a workstation?
When your internet goes out what is the response?
Workstation failures occur. Is there any procedure or plans for those occasions?
What happens if your internal server becomes unresponsive or corrupted?

DESCRIPTION

System failures include corrupted software, operating systems. Disruptions caused by failures, interrupt business operations. A plan in place for these things can be a great thing to have. Not only will it reduce downtime but also allows planning for the future.

KEY TERMS

- Corruption of business software / operating system
- Workstation system failure
- Wireless internet interruption

INSERT

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.

3.2 Physical Disasters & Recovery

GUIDING QUESTIONS

What happens if a snowstorm knocks out the power?
Is there a plan in place for natural disasters?
How would your town go about recovering and rebuilding if their facility burned down?
Are there back up locations where work could be picked up?
Physical Disasters can cripple your ability to continue IT based work. Having a plan in place can greatly decrease downtime. Below are a few things to consider when it comes to handling physical disasters. Prevention is a great way to mitigate the risks of a disaster however it never removes all of the risk. Protocols and Procedures are key to managing the risks that your town may face.

**KEY TERMS**

- Full Disaster Protocol
- Disaster Recovery Procedures
- Data Recovery Procedures
- Disaster Prevention
- Viable Back Up Locations

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.

### 3.3 Cyber Attacks

**GUIDING QUESTIONS**

Does your Town/City have anything in place to deal with these kinds of threats?

**DESCRIPTION**

Cyber-attacks can come in many forms listed below are a few examples but this list is ever growing. Attacks can be done for many different reasons but usually it involves some sort of monetary gain for the hackers. Denial of service attacks (DOS) attacks are used to shut down or attack a network and impede functionality until the attack has either run its course or a ransom is paid up.

**KEY TERMS**

- Denial of service Attack
- Ransomware
- Data theft
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.

## 4.0 Strategic Planning

### GUIDING QUESTIONS

- Is your town looking to improve their IT capabilities?
- Do you know what you need or would external guidance help?
- How well trained are your employees?
- If you implement a solution will employees need to be trained?

### DESCRIPTION

This section focuses on things that are outside of the day to day IT needs. Strategic planning covers assessments, improvements and training options to ensure you can achieve the network you need. Each option in this section is aimed at making the most out of technology and its use in your day to day work.

### INSERT

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.

## 4.1 Network and Hardware Assessment

### GUIDING QUESTIONS

- Is your Town/City interested in Assessments in order to properly gauge your network and software infrastructure’s strengths and weaknesses?
An Assessment can be very helpful to get a professional third-party opinion of what solutions may work best to ensure safe and reliable IT infrastructure. This assessment would establish any necessary networking and hardware needs. In turn increasing effectiveness and enhance user experience.

**KEY TERMS**
- Hardware Assessment
- Network 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.

**4.2 Security and Vulnerability Assessment**

**GUIDING QUESTIONS**

Is your Town/City interested in Assessments in order to properly gauge your security and vulnerability infrastructure's strengths and weaknesses?

**DESCRIPTION**

An Assessment can be very helpful to get a professional third-party opinion of what solutions may work best to ensure safe and reliable IT infrastructure. This assessment would cover security needs. In turn providing you with a starting point for security and vulnerability improvements, ultimately improving overall security infrastructure.
Compile and assess the network's security vulnerabilities and potential attack vectors. Potential penetration testing if the Town/City 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.

4.3 Projects

GUIDING QUESTIONS

Is the Town/City looking to change or upgrade their IT infrastructure?
Do you need new computers?
Are you interested in migrating to the cloud?

DESCRIPTION

This section aims to help tackle projects that are on the horizon. Projects can take a long time to get in motion. RFQs for a project will allow your town/city to start getting the guidance to accomplish the end goal. Upgrades and updates include new versions of hardware and software. Often accompanied by short-term interruptions. Need to be planned and scheduled.

KEY TERMS

- Hardware Upgrade
- Technology Refresh
- Migrate services into the cloud (Email, accounting)
- Hardware relocation

INSERT

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.
# 5.0 Training

## GUIDING QUESTIONS

<table>
<thead>
<tr>
<th>Question</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Would your enterprise benefit from basic technology and workstation training?</td>
<td></td>
</tr>
<tr>
<td>How do the employees feel about their level of workstation knowledge?</td>
<td></td>
</tr>
<tr>
<td>What improvements can be made for better work time efficiency?</td>
<td></td>
</tr>
</tbody>
</table>

## DESCRIPTION

This RFQ is designed to help your employees get the training they need to safely and effectively work with their technology. As well as to learn proper troubleshooting techniques in times of need. This can be applicable training in all areas of operation such as software and hardware issues, protection and prevention, as well as workstation literacy and data protocol.

## KEY TERMS

- Basic workstation literacy (desktop, email, anything needed for work)
- Who to call for software issues
- Who to call for hardware issues
- Basic scam/malware/virus protection and prevention
- Basic data protection protocol

## INSERT

Effective training solutions targeted for employees to ensure an understanding of basic IT operations and best security practices. Demonstrations and or presentation to ensure employees are proficient with Basic Workstation Literacy, requesting assistance, basic understanding of security risks and how to best avoid them. Town/City will provide details on more specific training requirements for employees.