ITPartners+

Town of Westlake - Backup & Disaster Recovery Renewal

Quote Number: QUOTE10157
Prepared For: Town of Westlake

Expiration Date: Wednesday, 31 January 2024

We make protecting data easy.

Datto BCDR (Business Continuity and Disaster Recovery) offers a comprehensive solution to safeguard critical business data, ensure uninterrupted operations, and minimize downtime in potential disasters. This solution combines state-of-the-art technology, robust data backup and recovery capabilities, and proactive monitoring to deliver a reliable and efficient business continuity strategy.

The risk of disaster to your business has increased significantly

The threats to your business data have evolved well beyond natural disasters over the past few years. Cyber threats have now become the biggest cause of disruptions that end up in data loss and/or long-term business outages. In 2023, there are an estimated 2,200 cyber attacks every day. Accordingly, modern backup, disaster recovery and continuity solutions need to protect your business from a broader range or threats including:

Ransomware

Malicious software secretly infiltrates businesses and encrypts critical business data.

Targeted hacking by malicious parties

Hackers target your business directly using a combination of tactics to steal data.

- **Disgruntled employee**
- **Human error**
- **Natural disaster**
- **Loss of utility services**
- **Theft**
- **Partners going out of business**

Co-op Purchasing Agreement

We welcome the opportunity to work with the Town of Westlake. We currently work with other agencies to provide backup and disaster recovery solutions through Datto. We are happy to provide references upon request.

ITPartners+ is a current TIPS Contract Holder for Technology Solutions Products & Services that can be used for Texas agencies:

TIPS Contract #200105

Verification: **https://www.tips-usa.com/vendorProfile.cfm?RecordID=31A485EBACB8DF9FC59230F4F3936B8D.**

The ITPartners+ Advantage

Datto & ITPartners+ have teamed up to provide a truly unique experience in business continuity. Our solution provides recovery, whether local or in the cloud, in mere minutes and provides industry-leading features.

UNLIMITED CLOUD STORAGE

UNLIMITED RAPID RESPONSE SERVICE

LIGHTENING FAST RESTORES & RECOVERY

datto
A Kaseya COMPANY

Datto Business Continuity provides recovery within an hour

The Datto Difference

Datto Cloud is purpose built as both a secure backup repository and cloud recovery (DRaaS) platform.

In the event of a disaster with total loss of your local infrastructure, ITPartners+ will be able to run a replica of your environment in the Datto Cloud. Once local infrastructure is available again, this solution greatly simplifies the restoration of your systems and data.

Datto SIRIS appliance & business continuity and disaster recovery solution

Based on your infrastructure, the Datto SIRIS appliance is well situated to manage backups, replicate data to the Datto's secure cloud and provide virtualization of servers in the event of a hardware failure.

Based on your infrastructure, the Datto SIRIS appliance is well situated to manage backups, replicate data to the Datto's secure cloud and provide virtualization of servers in the event of a hardware failure.

- Inverse Chain Technology™ for reliable backup
- Patented ransomware scanning
- Patented Screenshot Verification for recovery assurance
- Intuitive Recovery Launchpad for failproof recovery
- Patented Fast Failback™ to primary system after a disaster
- Instant virtualization recovery, local or in the cloud

Security is a key tenet to SIRIS with features that span login to the cloud

Two factor authentication Datto Backup Portal login

Hardened backup appliance

Backup copies kept in the immutable Datto Cloud to protect from attacks like ransomware

Cloud Deletion Defense™ to "undelete" malicious or accidental agent or backup snapshot deletion

Backup files that cannot be corrupted by ransomware

Datto Security Features

There are many security features built into the Datto SIRIS product which help prevent ransomware, unauthorized access and tampering with your data, whether in transit or at rest.

Immutable Backups: Datto SIRIS creates immutable backups, which means that once a backup is taken, it cannot be modified or deleted by ransomware or any other malicious software for 90 days. This ensures that even if a ransomware attack occurs, the backed-up data remains intact and can be used for recovery purposes.

Ransomware Detection and Alerts: Datto SIRIS includes patented built-in ransomware detection capabilities. The solution monitors backup data for suspicious behavior and indicators of ransomware activity. If a potential ransomware infection is detected, administrators are promptly alerted, allowing them to take immediate action and mitigate the impact of the attack.

Encryption: Datto SIRIS employs robust encryption algorithms to secure data both during transit and at rest. Data is encrypted using AES-256 encryption, which is widely recognized as a highly secure encryption standard. This ensures that even if unauthorized access occurs, the data remains inaccessible without the encryption key.

Crucial Relationship

Datto is not just a vendor we work with. ITPartners+ is a Datto Blue Partner—the highest level of Datto partnership. All of our partner support engineers hold multiple Datto certifications and are experienced with all Datto products. And, as part of the Datto Global Advisory Committee, we have access to Datto's leadership and provide feedback on their future plans.

Secure Data Transfer: Datto SIRIS ensures secure data transmission through the use of Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. These protocols establish a secure communication channel between the protected systems and the Datto SIRIS appliance, preventing interception or tampering of data during transit.

Role-Based Access Control (RBAC): Datto SIRIS incorporates RBAC to enforce granular access controls. RBAC allows administrators to assign specific roles and permissions to individual users, ensuring that only authorized personnel can access and manage the backup and recovery infrastructure. This reduces the risk of unauthorized access and data breaches.

Continuous Automated Protection: Datto BCDR utilizes continuous data protection technology to ensure that critical business data is continuously backed up and replicated. This minimizes the risk of data loss and enables rapid recovery in the event of a disruption.

TRADITIONAL VS INTELLIGENT BUSINESS CONTINUITY

TRADITIONAL	CONTINUITY
Can take weeks to recover data after a disaster occurs, if the data is recoverable	Downtime after a disaster is reduced to hours, minutes, or even seconds
High risk of failure due to heavy manual administration: 58% of downtime is due to human error1	Fully automated backup process—very little manual management required
Difficult to test if a backup is working properly	Automated screenshots are taken of each image-based backup, to verify a successful backup
Time consuming and expensive to make a copy of, and store, backups in multiple locations. 61% of SMBs still ship tapes to an off-site location2	Each image-based backup is automatically saved in multiple locations for redundancy; local appliance and secure data centers
Backup speeds are slower	Quick and efficient transfer of files to off-site data centers, even with low bandwidth or busy networks
Difficult to prioritize important data, files and applications	Critical data can be prioritized, to be transferred offsite first
Physical to virtual conversions can be time consuming and have a high failure rate	Instant virtualization in mere seconds, due to both proprietary technology and already saved VMDKs
Data and backups are at risk when based in only one location, either local OR in the cloud	Avoid risk of downtime from a local disaster, as backups are stored in both local device AND secure cloud
Limited options for encrypting data, may not pass industry regulations (i.e., HIPAA, SOX)	AES 256 and SSL key-based encryption ensures data is safe both at rest and in transit, to meet industry regulations (ie. HIPAA, SOX)
Tape failure rates can exceed 50%	Minimal risk of corrupted backups or data loss
Potential for theft of loss of media	Off-site backups stored in SSAE16 Type II data centers, ensuring security
Perceived cost savings are deceiving–average cost of downtime is $163,674 per hour3	The ability to keep your business running in the event of disaster has immeasurable value

1. “Enterprise Data and the Cost of Downtime,” IOUG, July 2012 ©2014
2. InformationWeek
3. Aberdeen Group

We get IT.

We live by one guiding principle: We do what we say we are going to do. Additionally, our partners love our response time and the fact that everything we sell comes with unlimited service and support. When you need us, we've got your back.

Security First

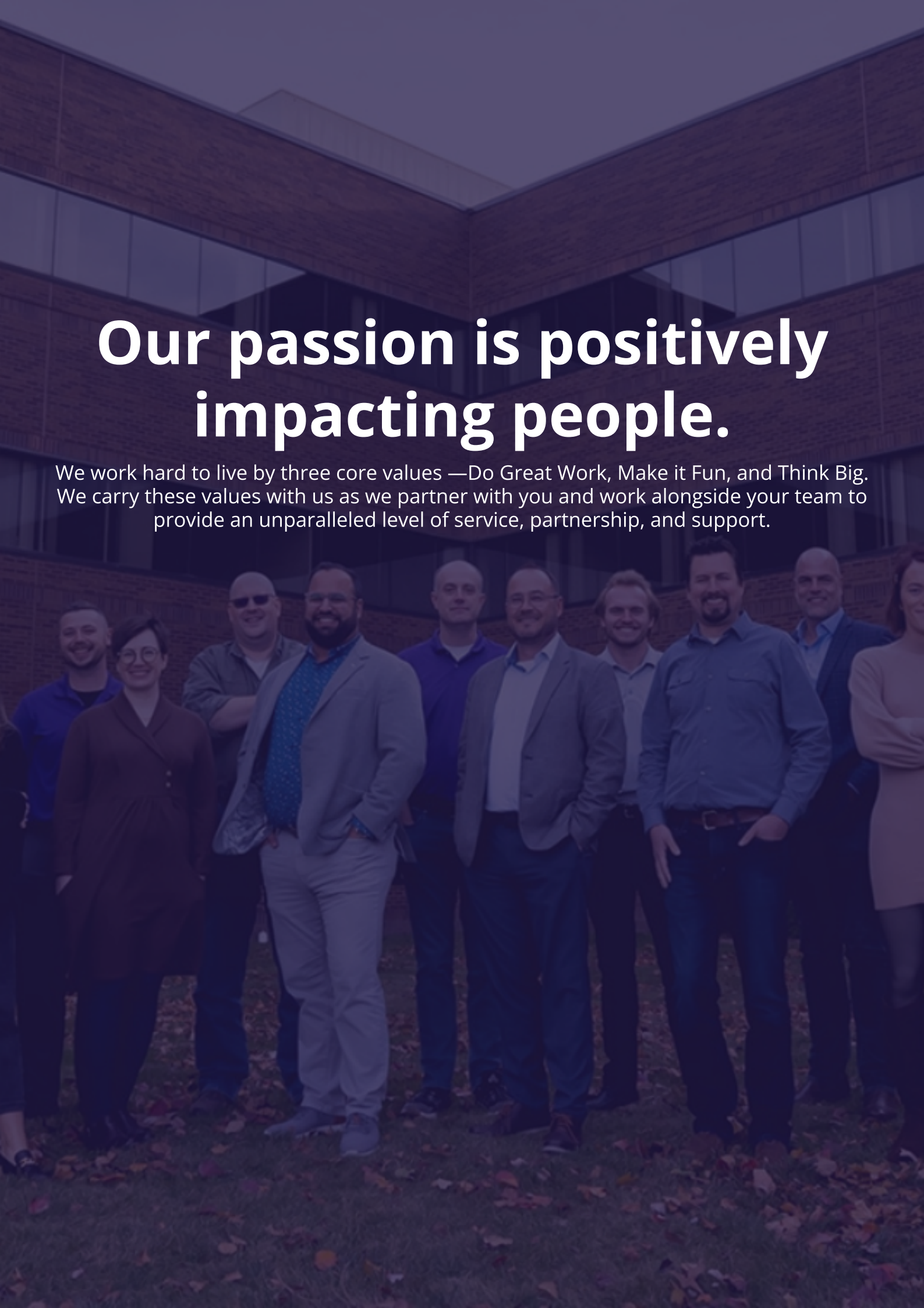
We proactively prioritize security to help protect you from emerging cyber threats.

Partnership

We work in tandem with your team to support your unique IT needs.

Responsiveness

There is typically a 2-minute response time from an Engineer.



Our passion is positively impacting people.

We work hard to live by three core values —Do Great Work, Make it Fun, and Think Big. We carry these values with us as we partner with you and work alongside your team to provide an unparalleled level of service, partnership, and support.

Your Investment

Your BCDR solution includes hardware at no cost with a three year term. The only upfront charges you pay are those for setup of the BCDR service.

Upfront Costs				**$0.00**
Product		**Quantity**	**Price**	**Amount**

Monthly Costs					**$21,588.00**
Product			**Quantity**	**Price**	**Amount**
datto	Datto SIris 4 12TB Co-Managed DRaaS Unlimited Cloud Storage | Infinite Cloud Retention Unlimited Direct-to-Tech Support from ITPartners+ Service from Jan 1, 2024 - Dec 31, 2024	Yearly	12	$1,799.00	$21,588.00

One Off	$0.00
Yearly	$21,588.00
Shipping	$0.00
Tax	$0.00
Total	**$21,588.00**

Silver Microsoft Partner

THE CHANNEL CO. CRN MSP 500 2023

WEST MICHIGAN'S BEST AND BRIGHTEST COMPANIES TO WORK FOR WINNER 2023

datto BLUE DIAMOND Global Partner Program

Inc. 5000

AICPA SOC aicpa.org/soc4so

Terms

Master IT Services Agreement (MSA)

By accepting this quote, you, hereby referred to as the "Partner," represent that you possess the authority to enter into this agreement. You commit to any recurring services presented in this quote for an initial term of three (3) years, which will thereafter automatically renew for successive twelve (12) month terms, as outlined in the ITPartners+ Master Services Agreement. You also acknowledge and consent to be entirely bound by the terms and conditions set forth in the said Master Services Agreement, available at https://quote.itpartners.com/termsofservice.

Service Level Agreement (SLA)

Introduction:

This Service Level Agreement documents the relationship between ITPartners+ (also referred to as ITP) and the customer (also referred to as the partner). This SLA includes the agreed upon Ticket Methods, Service Request Response Time, Partner Requirements, and Service Provider Requirements.

We recognize that since 2019 our first response times average for all tickets has been below five minutes. However, these response guidelines were developed to hold us accountable, even under unexpectedly heavy workloads.

Also, this document covers response time. We cannot guarantee resolution times since many of our services rely upon third parties.

Definitions:

Ticket: Tickets are service requests that are submitted to ITPartners+ as a formal request. Tickets are either submitted via phone call or emailed to ticket@itpartners.com. For Fully Managed partners a Help Button method will also be available. It should be noted that only tickets are counted against the SLA, whereas communication directed to specific people through email, phone calls and texts, etc. are not.

Fully Managed: Organizations without an established IT Department, wherein ITP is responsible for all IT-related services. This designation will be specifically indicated on a signed quote.

Co-Managed: Organizations with an existing IT Department that collaborates with ITP for specific services or solutions.

Ticket Methods:

Standard Business Hours Support

Available 7:30AM to 5:00PM Monday – Friday (excluding Holidays)

- Help Button: Submit a ticket via the Help Button connected to the monitored PC (Preferred method)
- Telephone Support: (616) 828-1010
- Email Support: ticket@itpartners.com

Emergency Email Support

Available After-Hours, Weekends, Holidays, and Emergencies during Business Hours

- Email: emergency@itpartners.com

Service Request Response Time:

Each ticket receives a severity level that will be initially set by the partner. Depending on the severity of the issue, ITP reserves the right to drop the severity level of any ticket in accordance with the description listed below. Support cases can be assigned one of the following priorities:

Severity Level	Description	Response Time
Low	Issues that do not impact business or backup functions, or do not have time constraints, but may cause problems in the future, such as warning messages or wish list items.	24 business hours
Normal	Issues that do not impact normal business functions, but cause problems with backups, such as failed backups or error messages, minor issues affecting one user, or other similar issues.	10 business hours
High	Issues that impact business, but do not hinder normal operations.	4 business hours
Emergency	Issues that directly impact business functions and hinder normal operation during normal business hours.	2 business hours

Note that all tickets deemed as **High** or **Emergency** should be submitted via phone, (616) 828-1010, or the emergency email address (emergency@itpartners.com). Any ticket submitted via the standard channel (ticket@itpartners.com) will automatically be assigned a **Low** or **Normal** priority.

Partner Requirements for Fully Managed:

ITP requires the following from the partner for Remote Monitoring and Management to function as intended:

1. Computers must be left on overnight and on the weekends. This is necessary for ITP to install Windows Updates, install third-party patches, carry out computer maintenance, and remote control. They may be rebooted during the agreed upon normal business hours.
2. Specific ports and port ranges must be opened in the firewall (both hardware and software) to allow ITP to properly monitor and manage all computers. ITP can handle this process if necessary.
3. All applications must be closed out on workstations to allow for computer restarts after updates. Arrangements can be made for specific computers and servers that need to keep critical applications running at all times. The standard patch/reboot window is as follows:

- Workstation Patching and Reboot: 2:00AM to 5:00AM
- Server Patching: 2:00AM to 5:00AM
- Server Reboot: Manually by ITP (usually after 9PM on Wednesday and Saturday)

Partner Requirements for Fully Managed and Co-Managed :

The partner agrees to abide by all access requirements in the MSA so that ITP can effectively resolve tickets.

1. ITP documents the IT environment to the best of its ability based on the scope of services provided. This is critical for assisting the partner, especially during infrastructure downtime. To do this, ITP stores relevant passwords and device information in their secure documentation portal. It is necessary that all relevant passwords and information of managed devices be released by the partner to ITP.
2. ITP maintains response time agreements depending on the severity of the ticket. To resolve tickets as quickly as possible, the partner must be timely and responsive, including answering emails, phone calls, and being available onsite.

Service Provider Requirements [ITPartners+] for Fully Managed Partners:

ITP will also adhere to several requirements to ensure optimal Remote Management and Monitoring. They are as follows:

1. Respond to support cases in accordance with the response times listed in the above chart. Please note that response time is not the same as resolution time, and although ITP will do its best to resolve issues as quickly as possible, it cannot guarantee that all issues will be resolved within the response time.
2. ITP will Remotely Monitor and Manage (RMM) all devices under the initial contract. Any requests to add or remove devices from the list in the initial contract must be requested to ITP in writing before they are added or removed from RMM and billing is updated accordingly. Standard RMM includes the following services:

- Install and maintain enterprise-grade virus-protection
- Windows patch management/deployment
- Hardware health monitoring
- Software updates
- Third-party patch management
- Preventative maintenance, including disk defrag and disk cleanup
- 24-hour monitoring of critical events
- Purchasing assistance
- Full documentation of IT environment

3. ITP will put all Technology Recommendations in writing. If partner chooses to not go forward with any Technology Recommendations as outlined by ITP, ITP reserves the right to remove the device from specific SLA terms. ITP will always put forward a good faith effort to continue to support the device, but in the instance ITP deems the device out of date or unusable, it may not be possible to resolve issues in accordance with the **Service Request Response Time** chart listed above.
4. At ITP's discretion, we will remove software that we deem is not conducive to business operations. This may require remote control of monitored computers.

Remote Control Policy:

Part of Remote Monitoring and Management (RMM) is the installation of remote-control software on every managed computer. By default, when purchasing RMM ITP has access to view the screen as well as remotely connect to every computer that is under the RMM contract. If the partner does not want to grant ITP universal access, arrangements can be made requiring the partner to grant remote access on an individual basis.

Violation of SLA:

Although ITP strives to respond to every ticket before the agreed upon response time, in the instance where this does not transpire, this SLA limits the monetary penalty of ITP to $50 per violation. Requests must be received in writing with proof of claim.