Service Level Agreement

Service Level Agreement

Service Level Agreement

Terms used in this document

1. EyeOnLAN™ and EyeOnLAN™ Managed Services mean the IT services program offered by Twisted Technologies, Inc.
2. Service Level Agreement ("SLA") means this Agreement and the terms and conditions contained herein.
3. Throughout this SLA, Twisted Technologies, Inc. may be referred to as "Twisted Technologies" "we" or "us."
4. Throughout this SLA, the party agreement to the terms of this Agreement with Twisted Technologies may be referred to as "the client" and "you."
5. Network Operations Centre ("NOC") means the central helpdesk from where Twisted Technologies, Inc. runs its services.
6. Throughout this SLA, "Agent" shall refer to the software by Kaseya used by us. The Twisted Technologies platform architecture is central to providing maximum security. Each managed computer has a small technological Agent installed. The Agent initiates all communications back to the server. Since the Agent will not accept any inbound connections, it is impossible for a third party application to attack the Agent from the network.
7. Throughout this SLA, the client's "Environment" shall refer to the client's infrastructure, as it relates to the services being provided hereunder, specifically including, but not limited to: computers, printers, scanners, LAN lines, telephone lines (which interact with the computer system), servers and switches.

Introduction

As most traditional IT services are based around site visits by engineers, an SLA is often based upon how quickly you see someone on site. Many of the services delivered by us are 'invisible' to a non-technical end user. To ensure that our clients get value for their money, we seek to make our 'invisible' services 'visible'. To do that this SLA outlines all of the tasks that we perform as a part of the SLA, what the tasks do, how they work, and how you can tell very easily if we are performing our tasks per the SLA. Our fundamental premise is to provide better service remotely and to avoid onsite visits whenever possible, so that we can keep down the cost of providing support and reduce down-time; thus benefiting all of our clients.

Company Information

We will maintain $1,000,000 in Errors and Omissions Insurance and $2,000,000 in liability insurance.

Response times and Business Hours

It is difficult to set response times for many of the services that we provide. Many of the services are complex automated services, so our response is immediate. These need substantial care and attention to make sure that they all work correctly, but this maintenance is ongoing and continuous. However, when you contact us, we will prioritize the incident as provided herein and agree to respond within the given time frames. A response does not merely mean we will let you know we have received your message, it means we will look at your issue, start diagnosis, and shall provide you with:
1) A clear outline from us of the next step for resolution, unless additional information is required;
2) If it is urgent, an expected time frame to resolution of the problem (a 'Fix' time); and
3) Steps that resolved the problem.
In furnishing you with this information we have satisfied the 'Response' as constituted by this SLA. If you do not set the Priority, we shall use the default Priority of "High." You must also be realistic about the Priority of an incident. When possible, any incidents which have been set above their allotted Response will be designated to the appropriate Priority by a senior member of Twisted Technologies, which will also reset the count time for the incident.
PLEASE NOTE: If you designate a Priority as "Emergency" when the Priority is not Emergency, then we shall charge you our premium, after-hours rates for that service for all business hours repairs and two times the after-hours rates for all improper after-hours calls, plus all travel time, travel charges and a penalty of $100.

The target Response times for SLA are as follows:
Emergency 2 Business Hours
Urgent 4 Business Hours
High 8 Business Hours
Normal 16 Business Hours
Business Hours can carry over to the next business day and do not include non-work hours. For instance, an Urgent request at 4:30pm would carry over to the next business day with a 3 hour window starting at 8:30am the next business day and can carry from Friday to Monday. Time is not calculated during closed hours.

Business Hours are Monday through Friday 8:30am – 5:30pm. We are closed all major holidays including New Years Day, July 4, Memorial Day, Labor Day, Christmas, Thanksgiving and the following day. If Christmas or July 4 falls on a Tuesday or Thursday, then we will also be closed that Monday or Friday respectively.

After Hours are available at a rate of 1.5 times normal rates. Sundays are 2 times normal rates.

Priority

As the setting of Priority for an incident carries such an important weight in the delivery of service, it is imperative that Priority service is carried out in a consistent and fair manner for all clients. Clear definitions allow us to classify each Priority, which is based upon the business impact.

Emergency All users on a site unable to work
• Virus Outbreak
• Email server failure
• Server crash
• Network failure
Urgent 1 user unable to work or all users greatly inconvenienced
• Single virus
• Users machine crashed
• Internet outage*
• Important File unavailable
• Printer problem for important meeting
*Note: we provide you with a "loaner" PC, but urge you to maintain a spare PC onsite for use if outage is critical.
High 1 user unable to perform a single function or experiencing inconvenience
• Application fault
• File unavailable
• File restore needed
Normal general questions, inquiry or problem that does not affect any user's ability to work
• User cannot remote into PC
• How do I…?
• How much would …cost?
Note that Internet outage is not an emergency as it is a 3rd party problem – your ISP, and while we will endeavor to resolve this as quickly as possible, it is in the end outside of our control. If your ISP is CBeyond, we will classify the outage as an emergency and handle the support and resolution for you. If you use another provider, you will be responsible for resolving independently or engage us at our hourly billing rate.

If at any time you feel that your incident has either not been given the appropriate Priority, or that your incident is not being dealt with quickly enough, then you should contact your account manager. You are of course also welcome to contact our Managing Director at any time at mark@twistedtechnologies.com or 404-202-1517 x5001.

Service Level Agreement Acceptance

To ensure that both parties understand this SLA and agree on the service to be delivered, the acceptance section needs to be filled in and signed by both parties. Unless there are changes to the service being delivered, the terms of this SLA shall apply to any extra machines that are added to the agreement. Your employees need to understand these priorities and the fact that you have accepted them and are bound to this level of response. We do not and are not required to follow up tickets with telephone calls, unless an emergency. If you or any of your employees or representatives select our emergency option for a non-emergency, we will bill you and you must pay us $150 for the call, as this uses all of our phone system circuits to obtain an immediate response and prevents other calls from being received.

Charges

Services under this SLA bear the following charges:
$29 per month for PC Support
$299 per month for SBS (Small Business Server 2003 or 2008) Support
$199 per month for 2003/2008 Server Support
$99 per month for Secondary Application Server (2003 or 2008) Support
Any onsite visits will be charged at $120 per hour and the trip charge will be waived within 40 miles of our primary office, with conditions as outlined herein.
Offsite backup pricing is outlined herein.
$29.95 per computer per year Anti-virus protection
$24.95 per mailbox per year Exchange Anti-Virus protection

$299.95 each for Acronis nightly imaging NAS drives
Any support provided to a computer NOT under Managed Services will be charged at normal rates for phone, remote and onsite support with a minimum of 1 hour of labor. We charge a one-time setup fee of $99 per node, not including correcting network issues.

Invoicing

We bill on the first of each month and payment is DUE ON THE FIRST of each month. We request a credit card or checking account information on file to auto-bill. You may also send a check so that we receive it on or before the first to avoid disruption, or you can mail a check BEFORE the first (1st) of each month for uninterrupted service. On the 5th of the month, Twisted Technologies shall suspend all Agents until payment is received.

Client

I hereby accept that I have read this Service Level Agreement document and understand and agree to the conditions in place upon the service that will be delivered to me by Twisted Technologies, and in particular realizing the realistic limitations on a fixed price service.

Number of PCs:_____

Number of SBS Servers:_____

Number of Servers:_____

Size of total offsite backup in GB:_____

Client:_____

Signed:_____

Date:_____

Technical Point of Contact:_____

Twisted Technologies, Inc.

I hereby agree that I have taken any and all steps to ensure that the client understands the service that it is being offered by Twisted Technologies and will take all measures possible to ensure that Twisted Technologies delivers this service to the client by regularly delivering reports and checking client satisfaction.

Twisted Technologies, Inc. Account Manager:_____

Signed:_____

Date:_____

Service Level Agreement Terms and Conditions

1. Moves, Adds and Changes

As a part of the managed service we include per this SLA, fixed services are delivered as a part of the Managed Service cost. New items are not supported in this SLA as part of the included price. Disposal of old computers and the boxes for new computers is the client's responsibility. Software updates, additional software installations, software support and training are NOT covered, as they are considered an MAC.

2. Privacy & Data Protection

2.1. Each party shall ensure that it shall at all times during the term of this SLA comply with all the provisions and obligations imposed on it by the Data Protection legislation.
2.2. For the purpose of this SLA the Data Protection Act shall mean:
2.2.1. The Data Protection Act 1984, as long and as far as it is still applicable to the processing of personal data pursuant to this SLA;
2.2.2. The Data Protection Act 1998, as soon as it becomes applicable to the processing of personal data pursuant to this SLA; and
2.2.3. Any other data protection legislation adopted pursuant to the Data Protection Act 1998.
2.3. The Twisted Technologies support system holds only technical data, and any contact data as supplied by the client to us. We will not use this data in any way other than to provide service as outlined in this SLA. We will not share your information with any 3rd parties or use it for any marketing activities, except where you have given us permission.

3. Security

3.1. Network Access
3.1.1. To provide IT support it is necessary for us to have full administration access to your network and any supported machines. You must agree to this to allow us to fulfill the requirements of this service.
3.1.2. You must allow access for the Twisted Technologies support system by opening port 443 on your network for outbound access or by giving permission for us to set up such access (these onsite visits may be chargeable).
3.2. Passwords
3.2.1. We need passwords to access the Environment, including but not limited to: Windows Domains, Local Windows admin accounts, Routers and Firewalls.
3.2.2. We will set up Admin accounts for technical access to your systems. We will use strong password technique, but is based on a formula so that it can not be guessed and does not need to be written down or stored. We do not reveal this information to clients, and clients asking for password information will be refused. It is an offence for any member of our staff to disclose any Admin passwords to anyone outside of our security team and will result in immediate dismissal.
3.3. Listed below are the security features implemented by us as part of its management system:
3.3.1. The Twisted Technologies management system is designed with comprehensive security throughout. The Twisted Technologies system design team brings over 80 years of experience designing secure systems for commercial applications.
3.3.2. We use Agents by Kaseya.
3.3.3. We do not need to open any input ports on client machines. This lets the agent do its job in any network configuration without introducing susceptibility to inbound port probes or new network attacks.
3.3.4. We protect against man-in-the-middle attacks by encrypting all communications between the agent and server with 256-bit RC4 using a key that rolls every time the server tasks the agent (typically at least once per day). Since there are no plain-text data packets passing over the network, there is nothing available for an attacker to exploit.
3.3.5. Administrators access our server through a Web interface after a secure logon process. The system never sends passwords over the network and never stores them in the database. Only each administrator knows his or her password. The client side combines the password with a random challenge, issued by our server for each session, and hashes it with SHA-1. The server side tests this result to grant access or not. The unique random challenge protects against a man-in-the-middle attack sniffing the network, capturing the random bits, and using them later to access our server.
3.3.6. The Kaseya Server website is protected by Twisted Technologies Patch Management. The Twisted Technologies Patch scan is run on our server every day. As soon as new patches are released, the Twisted Technologies Patch scan automatically detects whether they are needed and applies all security patches automatically.

4. Basic Requirements

4.1. Description
These are the minimum requirements for clients to be able to receive any of our services.
4.2. Requirements/Pre-requisites
4.2.1. Windows Based Operating System on the following:
4.2.2. As per what Microsoft currently supports, typically the current version and one prior on the most current Service Pack.
4.2.3. Where Microsoft drops support for a product, we will let you know and a separate arrangement will be made to upgrade existing hardware/software to meet Microsoft's new requirement.
4.2.4. All PC's/Servers must perform to the specification as outlined by Microsoft for the given operating system or application system.

4.2.5. Our Agent must be installed and working (supplied by us)
4.2.6. Broadband or equivalent 'always on' internet connection with at least 256Kb's spare capacity (not a dial-up connection, unless roaming out of office). For sites with more than 10 PC's a higher specification connection may be required (for example T1).
4.2.7. Firewall/router or similar port blocking device, set to block all inbound traffic (except where required for internal functionality).
4.2.8. Access to change the firewall device above to allow outbound traffic on port 443.
4.2.9. Machines left on continuously where possible (unless agreed otherwise), without power saving (we will configure this for you).
4.2.10. We will introduce some small records into the Windows registry to keep track of internal settings for delivering the service.
4.3. Client Obligations
4.3.1 Where some part of a client Environment does not meet the criteria as specified above,
we will be unable to setup any service or continue to deliver service to that device or site (if the item affects an entire site) until the Environment is bought back in line with our minimum requirements.
4.3.2. Where service is already being delivered by us and the Environment is changed outside the aforementioned requirements by the client, by Twisted Technologies or it's partners or a 3rd party, we will at its discretion continue to deliver service to that Environment until it can be bought back into alignment with the requirements for up to 14 days or until client's next payment is due, whichever is sooner. If support is to continue thereafter, an extra charge will be levied to support a machine outside of the required specification, generally four times the normal monthly cost of supporting a machine per month or part thereof.
4.3.3. Unless the changes are directly a result of our negligence or that of its partners, client will pay us for all costs involved in bringing an Environment back in line with requirements. We will not pay any costs arising from or caused by 3rd parties.
4.3.4. We will make all endeavors to warn the client of the costs before undertaking any work, but will also try to operate in the best interests of the client and the continuation of the business, and may take it upon itself to deliver chargeable services in the spirit and manner of previous spending and decisions made by the client in accordance with the perceived business impact or possible service disruption.

Managed Services

5. Continual Audit

5.1. Requirements/Pre-requisites/Limitations
5.1.1. Must meet our minimum requirements
5.1.2. DMI/SIMBIOS compatible motherboard with PCI or above slots (not ISA)
5.1.3. RAID controllers will not be separately identified
5.2. Machines will be set to renew audit information every day and to skip if machine is not available at the time of the audit.
5.3. Deliverable
5.3.1. Monthly Executive summary report which includes license summary
5.3.2. Upon Request: (a) Report of Licensed Software (as per Kaseya Software License database) only if requested; (b) Full installed application list; (c) Operating System report; (d) Hardware report; (e) System settings and/or (f) Backup log summary.

6. Capacity Monitoring

6.1. Must meet our minimum requirements
6.2. Machines will be set to provide Capacity Monitoring on a continuous basis
6.3. Deliverable
6.3.1. Monthly Executive Report showing available space & total space percentage breakdown
6.3.2. Machine Summary report available upon request
6.4. Actions
6.4.1. If disk space falls to within 5% of total on any fixed partition, we will contact you with this information and suggested corrective action if we cannot free up needed space.
6.4.2. Upon disk space reaching 10% of total on any fixed partition we will run an automatic clean-up to try and free-up any unnecessary system files and delete any temporary user files. This is done in the best interests of the health of a machine, as a completely full HDD on a windows machine can cause complete failure, so all attempts will be made to prevent this occurrence.
6.5. Exceptions
6.5.1. This service only covers standard fixed HDD partitions, not external devices such as USB devices etc. or mapped drives.
6.5.2. Where the disks are already clean and no further room can be made the automatic cleanup will not run.
6.5.3. If the disk is filling up extremely fast (within second or minutes) then the Twisted Technologies Alert may not be quick enough to identify this event. Something would already be seriously wrong for this to take place, and under such circumstances we cannot and do not accept responsibility or liability for (lack of) capacity of the machine, or any failure of the device caused thereby. Recovery or fix is at our discretion and may be chargeable.

7. Weekly OS Inspection and Cleansing

7.1. Must meet our minimum requirements

7.2. Machines will be set to provide OS Inspection and Cleansing every day and to skip if machine is not available at the time of the service. A de-fragmentation will happen every 7 days (this will be skipped on a machine if no de-fragmentation is found). A disk scan will be done daily.
7.3. Deliverable
7.3.1. Twisted Technologies System script and clean up tool using Windows Disk Cleanup
7.3.2. Twisted Technologies System script and service running Windows and 3rd Party de-frag tools
7.3.3. Entry of cleanup and defrag into Twisted Technologies System log
7.3.4. We may add additional cleaning and performance enhancing scripts, changes and applications at our discretion
7.3.5. Monthly executive report showing count of cleansing and defrags on all machines

8. Anti-Spyware Active Protection

8.1. Requirements/Pre-requisites/Limitations
8.1.1. Must meet our minimum requirements
8.1.2. If not already installed on your PC, we will install Malware Bytes, CCleaner and KES for your protection
8.1.3. We may remove other Anti-Spyware programs from your machine if they will interfere with delivery of the service
8.2. The System will be subject to a nightly scheduled service that will ensure the Anti-Spyware program is activated is updated and that a clean-up has been run on the system.
8.3. Deliverable
8.3.1. A log entry will be created on our System so we can generate a separate report, if required
8.3.2. Anti-Spyware Definitions updated minimum daily
8.4. Actions
8.4.1. An alert will be raised with the Twisted Technologies NOC if any Spyware is found on a machine. It is expected that this would be removed by the automatic cleanup, but the ticket that this alert will raise will be followed up to validate.
8.4.2 We request that Toolbars and any other programs that state they will protect or speed up your computer not be installed without first consulting Twisted Technologies.
8.4.3 We reserve the right to remove any software we deem as problematic and causing performance issues at any time that we are notified of Environment issues via a ticket.
8.5. While we make every effort to ensure your machine is safe from Spyware, we do not guarantee that your machine cannot or will not be infected in exceptional circumstances. Where this does happen, any resulting support or service required may be chargeable at our discretion, but after consultation with the client.
8.6. We do not guaranty that you will never have spyware.
8.7. If your PC or System has an exceptional number of spyware issues, we may require you to purchase additional hardware or software or bill for each instance of service.

9. AV Total Protection

9.1. Requirements/Pre-requisites/Limitations
9.1.1. Must meet our minimum requirements
9.1.2. We will install KES (subject to change) at an additional expense with annual renewal automatically, without notification, and invoice promptly each calendar year in September, based upon the number of currently active nodes that month. Our non-refundable rates for AV are listed above.
9.1.3. Any other Anti-virus programs will be disabled and may be removed; it is up to the client to ensure it has the necessary files/paperwork to reinstall this software should it stop receiving this service from us.
9.1.4 The client is responsible for Exchange Anti-virus software and will not be provided in this coverage. We offer this software at an additional expense with annual renewal, automatically, without notification, and invoice promptly each calendar year in September, based upon the number of currently active nodes that month. Our non-refundable rates for AV are listed above.
9.2. The system will be subject to a Nightly scheduled service that will ensure the Anti-Virus program is activated is updated and that a clean-up has been run on the system.
9.3. Deliverable
9.3.1. Included in the Executive Summary may be a list of the number of scans and updates that have taken place.
9.3.2. Script log entry so separate report is possible
9.3.3. Definitions updated minimum daily
9.4. Actions
9.4.1. An alert will be raised with the Twisted Technologies NOC if any Virus is found on a machine. It is expected that this would be removed by the automatic cleanup, but the ticket will be followed up with high priority to validate.
9.4.2 We reserve the right to remove any software we deem as problematic and causing performance issues at any time that we are notified of Environment issues via a ticket.
9.5. While we make every effort to ensure your machine is safe from Viruses, we do not guarantee that your machine cannot or will not be infected in exceptional circumstances. Where this does happen, any resulting support or service required may be chargeable at our discretion, but with consultation with the client.

10. Security updates to Microsoft Software

10.1. Requirements/Pre-requisites/Limitations must meet our' minimum requirements
10.2. Frequency
10.2.1. Nightly scans to assess patch requirements

10.2.2. Our internal machines are patched Sunday with the latest patches to ensure reliability
10.2.3. PCs are patched Monday – Sunday each week, Servers on Sunday between 3 – 6 pm and rebooted afterwards
10.3. Deliverable
10.3.1. Latest patches as per Microsoft's recommendations will be installed on all managed machines
10.3.2. Included in the Executive Summary will be a list of the number of scans and updates that have taken place.
10.3.3. Script log entry so separate report is possible
10.3.4. Patch status shown in monthly executive summary report
10.3.5. Detailed patch report available on request
10.3.6. Where possible patches will be downloaded once to a central file share on the local network and then delivered across the local area network to conserve internet bandwidth
10.4. Any issues raised with the NOC will be dealt with as per normal ticket affecting 1 user.
10.5. Exceptions
10.5.1. Where a patch/hotfix causes system problems on a machine, our staff will roll back the patch/hotfix to try to resolve the problem
10.5.2. Patches come from Microsoft and not from us; therefore, we cannot and will not be responsible for any adverse reaction that a patch might have with any particular machine configuration. In the unlikely event of a machine failure, we will restore the machine to its last good backup with no charge if performed remotely.

11. Monitoring of System and Security Logs

11.1. Requirements/Pre-requisites/Limitations
11.1.1. Must meet our minimum requirements
11.1.2. Windows Event logging switched on
11.1.3. No other software interferes with Windows Event logs
11.2. Even logs will be scanned and uploaded to Twisted Technologies NOC on a continuous basis
11.3. Deliverable
11.3.1. List of event log activity will be shown in Monthly Executive Summary report
11.3.2. Full latest inclusion and exclusion list supplied on request
11.3.3. An Intrusion Detection and Prevention Report to be provided upon request if running the appropriate software
11.4. Actions
11.4.1. Alerts identified in the Twisted Technologies Inclusion list will create a ticket at the Twisted Technologies NOC.
11.4.2. Alerts arise when anything falls outside normal parameters, including, but not limited to, server reboots, backup failures, offsite backup failures, ceasing of critical services, etc. We shall review the Alert to determine whether it warrants further investigation. If so, a ticket will be created.
11.4.3. Any issues raised with the NOC will be dealt with as per normal ticket affecting 1 user.
11.4.4. The Event Logs can often pick up and identify issues which require attention, such as with applications installed on machines (please note most applications are outside the scope of our support). Any time spent fixing such problems will be chargeable, but the client will be notified before any such chargeable work is undertaken.
11.5. Exceptions
11.5.1. Monitoring will stop when machines start producing more than 100 Event Log entries per hour. This will raise an Alert and be investigated as a separate issue.
11.5.2. Where the Event Logging is stopped due to excessive event entries, the Monthly report may be affected. We shall address this problem with the client.
11.5.3. If a machine is generating an extraordinary number of Alerts, this can adversely effect our system, so we, at our discretion, will stop monitoring Event Logs on this machine until the problem is rectified (this may incur an extra charge) or discontinue support for this machine completely.

12. Desktop Policy Enforcement

12.1. Requirements/Pre-requisites/Limitations
12.1.1. Must meet our minimum requirements
12.1.2. Windows active directory and group policies, professional operating system
12.1.3. Clear client definitions and understanding of current corporate policy
12.2. This is a continuous service, but the details of the desktop policy will be reviewed annually, or more often on request
12.3. Deliverable
12.3.1. Login policy (times, places, etc.)
12.3.2. Accounts policy (admin settings, user account usage, own account, etc.)
12.3.3. Corporate screensaver if provided
12.3.4. Desktop look and feel, background, colors, fonts, IE 7 or later settings
12.3.5. Block Access to the following programs and their variations:
12.3.5.1. Kazaa
12.3.5.2. Share Bear
12.3.5.3. Audio Galaxy
12.3.5.4. BitTorrent
12.3.5.5. Getright

12.3.6. File Shares on machines (should be none on a server-based network)
12.3.7. Time synchronization with server
12.4. Actions
12.4.1. We will consult with client to create a policy if one does not exist
12.4.2. We will develop a way to implement the policy
12.4.3. We will monitor the policy and create an Alert of any deviations
12.5. Exceptions
12.5.1. Where users are given local admin rights, they will always be able to circumvent policies; therefore, we cannot enforce a policy where the user is a local administrator.
12.5.2. Please note that enforcement of policy can restrict users' ability to perform actions on their machine(s), which may mean they need to contact us to perform some actions on their machine, creating delays in some actions. We always try to keep delays to a minimum but accept no liability nor responsibility for any inconvenience caused by such delays, as this service is in place to protect the client's security.

13. Online Reports

13.1. Requirements/Pre-requisites/Limitations
13.1.1. Must meet our minimum requirements
13.1.2. Email address supplied for main onsite contact
13.2. Online reports will be updated monthly
13.3. Deliverable
13.3.1. URL's emailed for each of the following report types:
13.3.1.1. Executive Summary
13.3.1.2. Uptime History
13.3.1.3. Patch Status
13.3.1.4. Disk Usage
13.3.1.5. Machine Summary

14. Event Log Monitoring

14.1. Requirements/Pre-requisites/Limitations must meet our minimum requirements
14.2. This is an ongoing service that is constantly monitoring the Windows Event Logs. The system can pickup and respond to errors inside the Windows Event Log with 30 seconds.
14.3. Deliverable
14.3.1. The Executive Summary report will show a total each month of the number of actionable items found in the Application Event Log.
14.3.2. We filter and look through the logs for specific know problems and turns these into tickets which we will check and remedy if necessary.
14.3.3. A full list of all the Filtered events that we monitor can be found in the Appendix.
14.4. Any Events that are found via the filters and raised as a ticket will be investigated by an engineer. Any fault found will be resolved wherever possible via remote management.
14.5. Exceptions
14.5.1. Where a problem is as a result of hardware failure, this cost is not included in support
14.5.2. Where a problem requires, onsite visits are separately chargeable
14.5.3. If a problem is complex and affected by other systems, we will compile and deliver to the client a report of findings and a course of action and costs associated with corrective action

15. Hardware and Software Change Monitoring

15.1. Requirements/Pre-requisites/Limitations must meet our minimum requirements
15.2. This change monitoring takes place at the same frequency as the Continual Audit service
15.3. Deliverables
15.3.1. Separate monthly change report can be supplied upon request
15.3.2. Engineers will work through the monitored Alert list for any anomalies, and where these are found a ticket will be created and the client notified.
15.4. The hardware change report does not cover external devices such as USB keys and USB attached drives, unless these have a windows hardware driver that makes them appear as a part of the normal OS operation.

16. Bandwidth Usage Monitoring

NOTE: This service is optional and will slow down your network

16.1. Requirements/Pre-requisites/Limitations
16.1.1. Must meet our minimum requirements
16.1.2. Windows XP Pro SP3 or later or 2003 SP2 patch or later, Vista SP1 or later, server 2008
16.1.3. Installation of Kaseya Network Protection Driver
16.2. We perform "by request" runs for 7 days
16.3. We provide Bandwidth Usage report by machine and by top 10 applications across all machines, sent via email.

16.4. The system will automatically create a ticket with a 7 day due date to ensure the system is turned off after that period has elapsed
16.5. Bandwidth Monitoring requires use of a driver installed by us. This is a system level driver inserted in the TCP/IP stack. In rare circumstances this can interfere with normal operation of the machine, for example loss of network connectivity. If such issues occur we will endeavor to remove the driver and reboot the machine to enable connectivity again. If other, more adverse effects arise, we will operate on a best-endeavor basis to get the machine fully operation as soon as possible; however, onsite visits are chargeable.

17. Disaster Recovery, Imaging and Offsite Backup

17.1. Requirements/Pre-requisites/Limitations
17.1.1. We will provide NAS (Network Attached Storage) device(s) at the client's request in the initial installation and setup a disaster recovery image schedule using Acronis.
17.1.2. The client is responsible for the time to setup the disaster recovery procedure.
17.1.3. The client is responsible for retaining a disaster recovery CD in a safe and secure location or recreate when necessary from a blank CD.
17.1.4. The client is still and always responsible for changing backup tapes and maintaining any existing backup procedure independent of this service.
17.2. Frequency
17.2.1. We run full images nightly.
17.2.2. Should the client desire offsite backup, a separate folder backup will be done.
17.3. Deliverable
17.3.1. As part of the Executive Summary Report, we provide a log report of images.
17.3.2 We will discuss with each client the best times for, in order to get the most, backups. These images can be run while a user is operating the computer and take less than an hour, but imaging during operation may cause some performance degradation.
17.3.3 System and file restoration can be performed remotely. If a hard drive crashes, the manufacturer's warranty will cover onsite replacement of the hardware, and the client can boot to CD for the recovery. If the computer is out of warranty we will operate on a best-endeavor basis to get the machine fully operation as soon as possible; however; onsite visits are chargeable.
17.4. In the case of a server image failure, the system will automatically create a ticket. PCs will not provide us a "failed alert" due to their level of importance and the fact that they are commonly offline.
17.5. The Acronis DR Backup requires use of a driver and partition installed by us. This is a system level driver inserted in the drive characteristics. In rare circumstances this can interfere with normal operation of the machine (for example, loss of bootup ability). If such issues occur, we will endeavor to remove the driver and partition and reboot the machine to enable connectivity. If other, more adverse effects arise, we will operate on a best-endeavor basis to get the machine fully operation as soon as possible; however, onsite visits are chargeable if this occurs after initial setup.
17.6. Offsite Options
17.6.1. All clients will receive 100MB of offsite storage without additional charge. Any excess storage will be charged at:

Space in GB	Price Per month
5	$25
10	$45
25	$100
30	$120
35	$140
40	$160
45	$180
50	$190
55	$210
60	$230
65	$250
70	$265
75	$280
80	$295
85	$310
90	$325
95	$340
100	$350

17.6.2 We suggest keeping 5 days of full offsite backups if the data is part of a database such as Quickbooks or Medisoft.
17.6.3 The total offsite backup size charged is for the 5 day total of all data stored
17.7. Liabilities
17.7.1. We will use 256-bit encryption to transfer the files over a secure connection
17.7.2. The client is responsible for an "always on" and reliable high speed connection

17.7.3. All backups are stored in a locked and alarmed facility, but we are not and will not be responsible nor liable for the integrity or safety of any data. In the event of a compromise, we will immediately disclose such fact to all clients.
17.7.4 We do not guarantee disaster recovery images will work under all conditions and should be considered a safety net instead of a failsafe.

18. Onsite Visits Policy

18.1. Requirements/Pre-requisites/Limitations
18.1.1. We will only send an engineer onsite when all other options have been exhausted, in order to minimize chargeable events to the client.
18.1.2. The Engineer will only stay onsite for the length of time required to address the relevant issue and will not undertake any other work while onsite, unless the client agrees to the work to be performed, the extra time to be spent and the charge to be incurred.
18.2. We schedule no pre-booked onsite visits as a part of the Service Level Agreement. We charge for all ad-hoc onsite visits.
18.3. Deliverable
18.3.1. Time onsite charges in .5 hour blocks with a minimum of one chargeable hour.
18.3.2. Travel to site does not incur normal trip charges.
18.4. If the client is more than 1 hour travel time via conventional vehicle one way from our office, we charge travel at $45. The Client may also incur costs for travel by means other than a car and a small charge for mileage if the site is over 100 miles away from us. All excessive travel charges are incurred by agreement.

19. Loaner PC Policy

19.1. Terms and Conditions
19.1.1. We will keep 3 Dell computers loaded with Office 2007 and XP Professional available for loan at no charge to the client while the client's new PC is being procured from Dell from us. We charge labor time to install applications and join to domain with the loaned computer.
19.1.2 Loan term is for a maximum of 20 days without charge.