

This Service Schedule describes and contains additional terms that apply to EarthLink’s Endpoint Management & Security Services (the “Service”). This Service Schedule supplements, or amends and restates, each Agreement For Service (“AFS”) and other documents used to order the Services by the Customer identified in the AFS (“Customer”) and the other documents comprising the agreement between the Customer and EarthLink with respect to providing, accessing and using the Service (collectively, the “Agreement”) as follows:

1. **Service Overview.** EarthLink’s Endpoint Management & Security Service combines a robust, reliable IT infrastructure, proactive management capabilities and automated processes, all working seamlessly in the background, to keep your end-users on PCs and Macs productive, protected and satisfied.

2. **Term.** The Service can be ordered for a term of 1, 2 or 3 years (“Term”) as set forth on the Agreement. Each Term commences at the earliest date between when the Service is available for use or sixty (60) days after the Service Agreement has been signed. (“Service Commencement Date”). Unless either Party provides the other with at least thirty (30) days written notice prior to expiration of the Term, the Service will continue, subject to the terms and conditions of the Agreement, as defined in EarthLink’s Standard Terms and Conditions.

3. **Billing and Payment.** Billing will commence on the Service Commencement Date. The first invoice will include the initial set-up fee, any installation or seed load charge, a pro-rated monthly recurring charge (“MRC”) for the Service from the Service Commencement Date through the date for which the invoice is issued. It will also include the MRC invoiced monthly in advance. Ongoing, the invoice will include the MRC invoiced monthly in advance and any applicable non-recurring charges, which will be billed monthly in arrears. If arrangements for payments by credit card have been made, EarthLink may charge the Customer’s account on or after the invoice date. Unless otherwise described in this Service Schedule, all invoiced amounts are due and payable within thirty (30) days of the invoice date in accordance with the terms of the Agreement.

4. **Core Components (broken out between Endpoint Security and Endpoint Management & Security)**

Feature and Description:	Additional Info:	EP Security	EP Management & Sec
SaaS Anti-Malware (Anti-Virus/Spyware Protection)	Workstations are protected with the latest anti-virus definitions through daily, real time updates along with policy based on access scanning as well as weekly scheduled full system scans during the desktop maintenance window	Yes	Yes
SaaS Patch Management	Microsoft Critical Security patches are tested and automatically distributed to your user community with no disruption to your service. We do not release any patch until it has passed our Quality Assurance testing. Most critical patches are fully tested and released within 48 hours.	Yes	Yes
SaaS Tools Self-healing for EarthLink	Endpoint Management tool self-healing ensures that all required management tools are installed and functioning correctly via proprietary entitlement values in the system registry and leveraged by the Tivoli Endpoint Manager	Yes	Yes

SaaS Asset Tracking (Dashboard)	System hardware and OS versions are tracked throughout your environment, with reporting available via the web portal whenever you need it.	Yes	Yes
Event Notification (Notify Only)	Proactive notification provided to customers should items such as a malware outbreak occur.	Yes	Yes
Event Management (Receive, Log, Classify & Track)	Proactive notification provided to Customer should items such as a malware outbreak occur, including issue tracking and remediation by the EarthLink Support Team.	No	Yes
Incident Management & Remediation	The EarthLink Support Team will track, manage and resolve any incidents arising from or related to any Endpoint Security and Management Tool or Service.	No	Yes
SaaS Software Distribution	<p>EarthLink can distribute software to Endpoints. This software includes the EarthLink Management Tool Suite as well as well as 3rd party applications required by our Customers.</p> <p>Requests can be made to package as required and distribute on demand. Packaging of the software is done on a Professional Services basis, but deployment is included in the monthly service.</p>	No	Yes
SaaS Automated Hard Drive Defragmentation	Disk Defragmentation powered by Diskeeper prevents the majority of fragmentation before it can happen. Included in the tool are critical system file protection and file optimization to maintain the fastest possible response times. <i>*Only available for PC.</i>	No	Yes
Continuous Configuration Management	Ongoing assurance that security levels are maintained and workstations are stable and optimized through use of our proprietary Continuous Configurator, which automatically makes adjustments should critical aspects of a user's system falls out of compliance with standards.	No	Yes

24x7 Staffed Monitoring as a Service (MaaS): EarthLink operates geo-redundant Network Operations Centers (NOCs).	The NOC Uses Microsoft's System Center Operations Manager (SCOM) to monitor the EarthLink infrastructure to make sure the Customer's Service is operational	No	Yes
24x7 Staffed Admin/IT Helpdesk w/Case Tracking & Reporting	EarthLink provides 24x7 support to Customer technical contacts and authorized technical team members relative to subscribed tools and services	No	Yes
Data Defense (Encryption)	Combining intelligent encryption with enterprise-controlled data elimination, Encryption automatically eliminates specified data on lost or stolen laptops to prevent its compromise or misuse.	Optional	Optional
Data Protection (Back up)	Computers on the Data Protection (Backup) service are backed up daily utilizing the HP Autonomy Backup Solution, gaining the ability to quickly restore either individual files or entire systems. Individual files can be restored in minutes, while an entire system can usually be restored within 24 hours.	Optional	Optional
Web Content Filtering	EarthLink's Web Content Filtering allows the enablement and enforcement of web browsing policies in support of corporate internet usage policies. The system is Active Directory integrated and allows for policy management via AD group membership.	Optional	Optional
24x7 Staffed End User Helpdesk w/ Case Tracking & reporting	EarthLink's helpdesk team is available 24x7x365 to support end users across all technology and service platforms as both a first point of contact, and resolution helpdesk	Optional	Optional

5. Endpoint Management & Security Supported Platforms

In general, the following are the currently, supported platforms: Windows Vista, Windows 7, Windows 8, Windows 8.1 and MAC OS X 10.7, MAC OS X 10.8 and MAC OS X 10.9

6. Workstation Maintenance Schedule

6.1 Weekly Workstation Maintenance Window

The EarthLink maintenance window occurs every **Thursday between 11:00pm and 3:00am (Client Local Time)**. During the maintenance window, routine updates are distributed to your workstation to resolve known issues and to protect your computer from security vulnerabilities. Of course, EarthLink delivers critical security updates to your workstation whenever threats arise, usually without waiting for the maintenance window. It is permissible to keep working on your system during the maintenance windows; however, response time occasionally may be sluggish, and you may be prompted to reboot your computer when updates complete.

- Patches are only deployed to systems that are specifically relevant to the particular application / operating system (we don't deploy every security patch to every system.)
- A weekly reboot request action is sent as part of the weekly maintenance, after the patches have been deployed.

6.2 Guidelines to Ensure Proper Maintenance

During the weekly maintenance window, any or all EarthLink-Managed Workstations may be delivered application and operating system updates and patches. Below are some guidelines that will ensure that your system receives the latest updates and patches as they are delivered to your system on **Thursday nights**:

- Your system must be powered ON. *Please also disable "standby" or hibernation*
- Your system must be connected to a network
- Users should be logged off from their machines
- If your system is not connected to the network or the Internet in time for the Thursday night update, any distributed updates will be delivered to your workstation the next time you connect to the Internet or to the network.

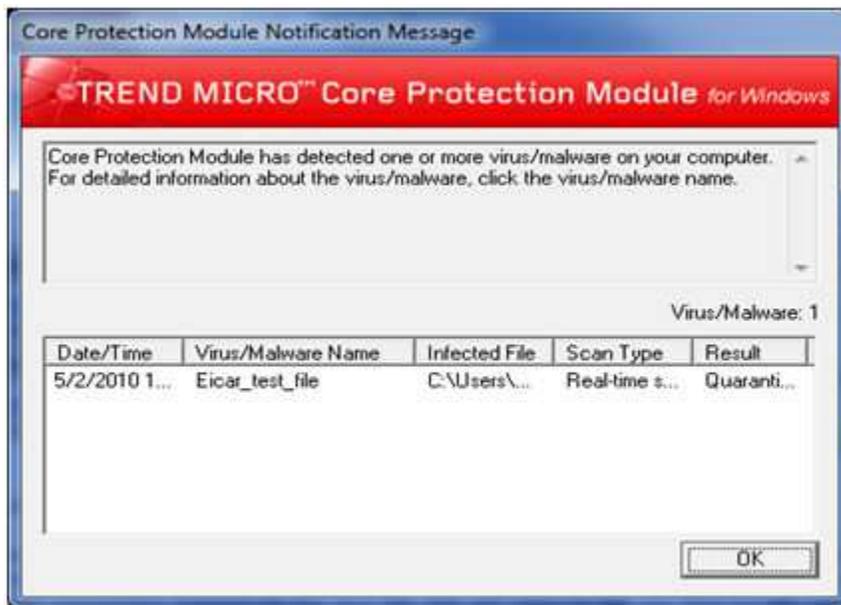
Note: We strongly encourage occasional distribution of this notification as a reminder to your user base of this window and the services that are performed on their behalf. This proactive maintenance process is in place to protect your end-user systems as close to real-time as possible.

7. Reporting

Along with hardware information, Big Fix also collects information relative to installed applications, allowing EarthLink to assist our Customers in the area of software reporting, better managing software deployments and upgrades, etc.

8. Anti-Malware (Anti-Virus / Spyware Protection)

Prevents damage from viruses, Trojans, worms, and other new malware variants, including blended threats. Identifies and completely removes discovered spyware, including hidden rootkits (a collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more). Users will be alerted of detections of virus/malware with the following prompt:



Clicking on the Virus/Malware Name will open a browser window detailing that particular threat.

Anti-Malware update and pattern definition status is available for review anytime at my.centerbeam.com under the Assets > Security tab

9. **Patch Management**

Big Fix is used to manage patch distribution to all EarthLink Managed Systems. Microsoft critical security patches are staged for distribution every Thursday during the desktop maintenance window

In order to minimize impact to the user, systems should be left powered on, connected to the network and logged off. This ensures all patches are delivered transparently during the maintenance window

Endpoint patch status is available for review anytime at my.centerbeam.com under Assets > Security tab

10. **Defragmentation**

As part of EarthLink's End Point Management and Security Suite, EarthLink's Disk Defragmentation powered by Diskeeper prevents the majority of fragmentation before it can happen. Included in the tool are critical system file protection and file optimization to maintain the fastest possible response times. **Only available for PC and only available with Management & Security*

Features of Diskeeper:

HyperFast is the first ever optimizer exclusively designed for faster performance and extended lifespan of SSDs running on Microsoft® operating systems. It is nothing short of a "must have" for all the new laptops, desktops and netbooks that are now using solid state drive technology.

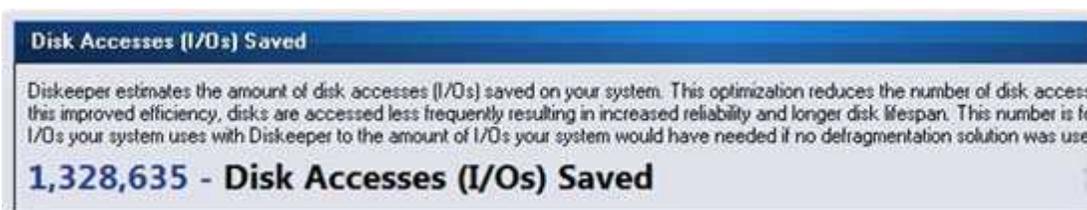
IntelliWrite™ fragmentation prevention technology prevents up to 85% of the fragmentation every system suffers from. It intelligently writes contiguous files to the disk so system resources are not wasted creating fragmentation. The result? A whole new level of system speed and efficiency.

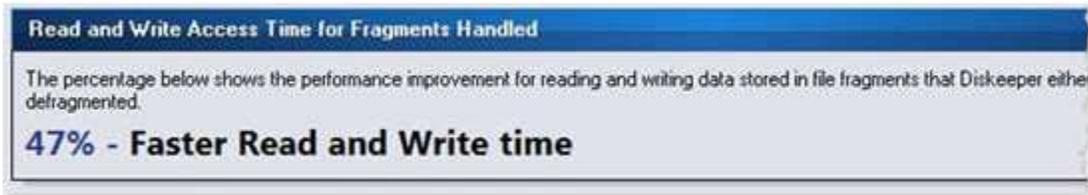
Diskeeper is the only defragmenter with InvisiTasking® technology, a real-time background processing technology that allows Diskeeper to defragment your system as fragmentation occurs, even during heavy traffic times, without using active system resources. InvisiTasking eliminates the need for scheduling and administrator attention.

Diskeeper I-FAAST® 2.0 (Intelligent File Access Acceleration Sequencing Technology) accelerates file access times to meet the heavy workloads of file-intensive applications. Utilizing a specially formulated technology, I-FAAST closely monitors file usage, and organizes the most commonly accessed files for the fastest possible access, up to 80% faster.

Systems with Diskeeper run more efficiently saving corporations thousands of dollars in energy costs each year. Diskeeper can save an estimated \$3.22 per workstation per year in energy costs.

Diskeeper 2011 provides Enhanced Analysis Reports easily accessed in quick tabs that graphically display performance gains achieved with defragmentation. Diskeeper also evaluates the condition of your disk against documented factors known to affect reliability and stability. Different reports include: Fragmentation Analysis, Performance Analysis and Reliability Analysis and I/Os Eliminated.



**Requirements:**

Diskkeeper Professional runs on Windows XP Home, Windows XP Tablet PC, Windows XP Media Center, Windows XP Professional (x86/x64), Windows Vista/7 Home Premium (x86/x64), Windows Vista/7 Ultimate (x86/x64), Windows Vista Business (x86/x64), Windows 7 Professional (x86/x64) and Windows Vista/7 Enterprise (x86/x64) platforms (including compatible CPUs from other manufacturers).

Disk subsystems supported: (all part of Diskkeeper)

- Primary Partitions
- Extended Partitions
- Logical Drives
- Volume Sets
- RAID Arrays (hardware and software)
- Mirrored Disks
- Mounted Volumes (letter-less drives)

11. Data Protection

Data Protection eliminates the risk of data loss from enterprise desktops and laptops, whether protected locally or remote. By automatically protecting data in the background, Data Protection ensures complete data protection without interrupting users. Data Protection also provides a secure web-based access portal and mobility support, through which users can easily retrieve data -- without helpdesk intervention.

11.1 The core components/features of EarthLink's Data Protection Services include:

- **Backup:** Scheduled and automated disk to disk backup is transparent to users and fast, even over dial up connections.
 - Backup window scheduled between 7pm and 5am
 - If a machine is not available for backup during this window the end user will be notified by the client that a backup was missed upon next boot up and offered the opportunity to manually back up, defer or cancel the scheduled backup
 - If a user cancels 7 daily backups successively, a backup will be forced ensuring a workstation backup occurs at least once every 7 days.
 - Daily backups are delta block level backups which are first compressed, then encrypted using native 256 AES based encryption prior to sending data over the internet to EarthLink's Data Protection infrastructure
 - Data remains encrypted within the EarthLink Data Protection infrastructure
 - Data is only unencrypted once restored to a machine with the correct Data Protection account number
 - Because users have the option of deferring or cancelling backups if required, EarthLink manages the Data Protection service to a KPI of 80% of subscribed workstations backed up within 7 days

- **Recovery:** Users can recover lost files quickly and easily, whenever and wherever needed.
 - User may choose to recover files themselves via the Restore tab of the Data Protection client, or if subscribed to the EarthLink helpdesk service, by contacting Customer Care and requesting assistance
 - File restore instructions can be found here:
 - My.EarthLink.com > TIPS > Service How To's > EarthLink Data Protection - Backup Client for PC/Mac
- **MyRoam:** Web-based access portal lets users access their backed up data anywhere without IT support intervention.
- **The Data Retention Settings for the Online Backup Service are as follows:**
 - Files that have more than 10 versions or are older than 30 days are deleted, but your most recent version is always kept.
 - Files that you deleted from your system are deleted from the data center after 30 days.
 - Files that you backed up and then deselected from your backup are deleted after 30 days.
 - Files of accounts that were cancelled are deleted 30 days after cancellation.
 - Any account that has had no activity for 90 days will be automatically purged from the data center.

11.2 System Requirements for Data Protection

- The application will only run on the following operating systems with either 32 or 64 bit:
 - Windows Vista
 - Windows 7 (Ent or Pro)
 - Windows 8 (Ent or Pro)
 - MAC OS 10.7
 - MAC OS 10.8
 - MAC OS 10.9
- **Excluded File Types by Category:**
 - Audio Files - such as AA, AIF, AIFF, CDA, IFO, M4A, M4P, MID, MP1, MP2, MP3, MPE, MUS, RA, RAM, WAV, WMA, etc.
 - Disk Images Files - such as GHO, IMG, ISO, NRG, TIB, WIM, etc.
 - iPhone App Files - such as IPA, etc.
 - Temp and Cache Files - such as BAK, LOG, OST, etc.
 - Video Files - such as AVI, AVS, M2TS, M4V, MKV, MOOV, MOV, MOVIE, MP4, MPEG, MPG, QT, QTM, RMVB, SCM, VOB, WMV, etc.
 - Virtual Machine Disks Files - such as VDI, VHD, VMDK, etc.
 - Misc Junk Files - such as \$\$\$, CHK, HFV, HIB, MOZ, TEMP, TMP, SWP, etc.
- **Included File Types by Category:**
 - Compressed Files - such as ARC, CAB, GZ, JAR, RAR, SIT, TAR, ZIP, etc.
 - Common Files Types - such as 123, CSV, FP, FPT, GMB, IML, REP, VSC, VSD, VSS, VST, VSW, WK1, WK3, WK4, WDB, WKS, WPS, WQ1, etc.
 - Image Files - such as AI, BMP, GIF, JFF, JFIF, JPEG, JPG, PDD, PNG, PSD, PWP, TIF, TIFF, etc.
 - Lotus Files - such as NCF, NDL, NLR, NS2, NS3, NS4, NSF, NSG, NSH, NTF, etc.
 - MS Office Files - such as ACCDB, ACCDE, ACCDR, ACCDT, DOC, DOCM, DOCX, DOT, DOTM, DOTX, LDB, MDA, MDB, MDE, MNT, MPP, MPT, NK2, OFT, OLK, ONE, POT, PPS, PPT, PPTM, PPTX, POTM, POTX, PPAM, PPSM, PPSX, PST, PUB, VSD, XLS, XLA, XLB, XLT, XLW, XLSX, XLSM, XLTX, XLTM, XLSB, XLAM, XSN, WPS, etc.

- SPSS Files - such as SAV, SPS, SPV, etc.
- Various Files - such as DBX, FOL, ILM, JSD, MBX, MSG, PAB, PST, PDF, REP, RTF, TOC, TXT, WAB, WBK, etc.
-

11.3 Data Protection Availability

When installed, Data Protection will perform a full system backup based on data type inclusions section from any internet connection. Daily backups of file differentials every 24-36 hours thereafter

Data Protection also allows end users to select files they wish to back up OR restore on demand 24/7 from any internet connection.

11.4 Installing/Removing Data Protection

- Only an Authorized Technical Contact (ATC), Business Contact (BC), or Internal Support (IS) user can initiate requests to install or remove Data Protection Services via the web Service Order Form.
- Upon receipt of the Service Order Form a Customer Care Specialist will either deploy or remove the Data Protection client from the specified workstation via the Tivoli EndPoint Manager base on the specific request