**IT Support Services**

This document describes processes and services delivered by the Service Provider, to the Subscriber. It is intended to establish a level of expectations for all parties.

Given the complexity of delivering IT services and the need for simple reference material, the documentation is packaged to separate commitments from definitions. The Technical Services Agreement and its Exhibits describe terms and conditions between the Service Provider and the Subscriber. The Service Catalog items and Requirements documents describe the actions to be performed in order to deliver the services.

Documents

* **Technical Services Agreement (TSA)**
	+ A master agreement between Service Provider and Subscriber. The TSA agreement refers to Exhibits that further describe the service and commitments.
* **Exhibits**
	+ Documents further describing the offering:
		- Exhibit A – IT Support Services (this document) describes expectations of all parties to deliver IT services to the Subscriber.
		- Exhibit B – Schedule of Fees describes the Subscriber’s pricing of services from the Service Provider.
		- Exhibit C – Customer Selected Services with detailed descriptions of activities and expectations.
		- Exhibit D - Onboarding Requirements describes specific requirements that must be attained in order for services to be delivered. Failure to have the environment meet the requirements may result in delay of onboarding, denial of services, or termination of the Technical Services Agreement.

Definition of Terms

For consistent execution of our processes and to deliver a great experience, the Service Provider utilizes a framework of consistent language and definition of terms from the IT Information Library (ITIL®).

## Service Types

* **Incidents**:
	+ Fault: Identified by users or by remote monitoring systems at the occurrence of a disruption of service. Examples may include slow workstation performance, loss of internet access or a failed hard drive.
	+ Threshold Breach: System generated notification of a breach of preset criteria that may result in a potential fault. Example, an incident may be the device is running low on disk space.
* **Problems**: The underlying cause of one or more incidents.
* **Service Requests:** User generated requests to perform something that is not as a result of, or a remedy to, an incident or problem. Also includes changes to the current environment. (e.g. *“How do I hide columns in Excel?” or “I need a new PC.”)*
* **Proactive:** Activities that keep the environment functioning at optimal performance. (e.g. applying patches and antivirus updates)

The Offering

Every organization has a set of technology needs which are unique to its particular style and mission. There are elements of technology, however, that apply broadly to the needs of nearly every small and mid-sized business. The goal of our program is to address core needs with a uniform set of standards and technologies, in order to drive efficiency while delivering exemplary customer service.

## Core Offering

These items are the very basics to providing information technology (*think food, clothing and shelter*). Below is a short description of each item: *(This list is intentionally concise for readability. Please see the Exhibit C for a detailed description of activities and expectations).*

* **User Support:** Users are able to contact an engineer for help. We provide support for technology the Subscriber CURRENTLY uses. If something new is introduced into the environment, it is considered a Change Request and may modify pricing.
* **Server Support:** All servers are monitored and incidents remediated. Every server in the environment is required to be covered (on premise or cloud), included servers acting as hosts to virtual environments.
* **Data Backup:** Subscriber data is backed up and located offsite.
* **Network Protection:** Subscriber network is protected with an actively managed Unified Threat Management system.
* **Managed Email:** Each knowledge worker is provided a mailbox for communication

**Workstation Support**

**Our Responsibilities**

**Standard Service for PC** *included in support fee*

* Unlimited calls and emails to the Service Desk M-F; 7:00 am to 7:00 pm. Onsite available M-F; 8:00 am to 5:00 pm.
* Monitoring and remediation for available disk space, memory utilization, connectivity, CPU utilization, warranty, AV status, blue screens, patch status
* Individual Remote access (through Fortinet VPN/LogMeIn)
* BIOS and driver updates as needed during normal troubleshooting processes
* Proactive Maintenance
* Remote support / Remote control
* Asset Management / hardware warranty notification
* Coordination of warranty work for devices covered under current warranty

**Elective Services for PC** *available for additional fee*

* Transfer of data from one piece of hardware to another

Technical Details

* Workstations can be in the form of regular desktops, laptops, thin clients and mobile devices

**Server Support**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Unlimited calls and emails to the Service Desk M-F; 7:00 am to 7:00 pm. Onsite available M-F; 8:00 am to 5:00 pm.
* Monitoring
* Hardware health for machines with Dell Open Manage or HP Insight Manager: fan, logical drives, physical drives, powers supply, RAID status, and temperature
* Performance (disk, memory and processor utilization), connectivity, available disk space, application event logs, reboot events, system log alert events, AV status, blue screens, patch status, processes and services based on the purpose of the server (e.g. Exchange and SQL)
* We will remediate issues whenever possible
* Proactive Maintenance
* Microsoft Windows Updates
* Antivirus updates
* Diagnosis of hardware failure
* Coordination of warranty work for devices covered under current warranty

**Elective Services** *available for additional fee*

* Metadata cleanup of AD after server removal to correct topology and routing alerts

Technical Details

* Support is not offered for Linux, Unix or AS400
* Website content updates are not offered

**Proactive Maintenance**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Resolution of issues that affect the efficacy of the support tools including:
	+ Devices that have not reported in from the remote monitoring tool
	+ Devices that have stale services
	+ Devices that require reboots for software tool updates
* Device housekeeping tasks that improve the overall functioning of the machine
* Antivirus Full Scan (monthly)
* Antivirus Quick Scan (weekly)
* Microsoft Windows Updates

**Elective Services** *available for additional fee*

* Not Applicable

**Your Responsibilities**

* Notify the service desk of any machines that have been removed from the environment
* Leave workstations in a powered on, but logged off state Monday through Thursday evening

Technical Details

* Not Applicable

**Reboot and Maintenance Plans Windows**

The “Managed Services” role in your environment is attempting to provide an environment of healthy, efficient PC’s, servers, printers, and networking gear. Part of this role includes performing routine maintenance procedures on these devices. It is our intention to perform these procedures outside of normal business hours, so as not to affect your productivity time. We also want to protect work that is open on your desktop. In order to do these effectively, we request that before you go home for the day, that you leave your machines turned **ON** but in a **LOGGED** **OFF** state Monday morning through Friday morning. Prior to logging off, make sure to save and close all open documents and close out of all applications.

**What type of procedures will we run?**

In most cases the work is automated, and amounts to Anti-Virus scans and updates, Microsoft Windows Updates, and device Proactive Maintenance procedures. At times any one of these procedures may require reboots of the machine. In most cases this work is scheduled to occur on Specific Nights. At times though, especially in relation to Anti-Virus and Microsoft Windows Updates, there are “Out-Of-Band” updates. Out-Of-Band updates are considered extremely important and are meant to be applied as soon as possible.

**Procedures that we run:**

Thursday Evening is the “planned” updated and reboot evening for any PC or laptop. The exception to this would be for the “Out-Of-Band” updates as noted above. “Out-Of-Band” updates and reboots will be limited to Monday through Thursday Night. Out-Of-Band reboots are infrequent, two or three times a year.

**Microsoft Windows Updates** – On the second Tuesday, known as “Patch Tuesday”, of each month, Microsoft releases updates to their products. This includes Operating System updates like Windows 7 or Windows 8, and application updates like Word, Outlook and Excel. Microsoft organizes these by category, such as: Critical, Security, Important, Update, Feature Pack, and other categories. We will always allow all Critical and Security Updates to run. The other categories are reviewed and determined, on an “as needed” basis, whether or not to approve them for installation. All PC’s and Laptops process these updates weekly on Thursday Evening and reboot as needed. Processing updates weekly allows for the “Out-of-Band” updates that may occur.

**Anti-Virus Full Scan** – This is a once a month scan. It is CPU intensive and users may notice when this runs. Running this after hours will not affect user productivity. This type of scan will scan all files and folders as well as scan the boot partitions of the device.

NOTE: Anti-virus actively scans all new files and new files as they are opened to help prevent virus attacks. Scans review current files to make sure they are still virus free.

**Anti-Virus Quick Scan** – This is a weekly scan of new files since last full scan. This procedure usually runs in 15 minutes or less and most users usually do not notice the effect this has on the machine. Running this after hours will not affect user productivity.

NOTE: Anti-virus actively scans all new files and new files as they are opened to help prevent virus attacks. Scans review current files to make sure they are still virus free.

**Anti-Virus updates** – Anti-Virus has several types of updates. “**Definition updates**” are rules to handle all “known” viruses to prevent infection. Definition updates occur frequently, often several times a day as new viruses are constantly forming. “**Application** **Updates**” are minor updates to the Anti-Virus software. These tend to be minor in nature, occur occasionally, a couple of times a month, and they may require rebooting the machine. “**Application** **Upgrades**” are major update updates to the Anti-Virus software. These updates are infrequent, two or three times a years at most and will require a reboot of the machine. All of these reboots are scheduled for Thursday evening. “Out-Of-Band” reboots will be limited to Monday through Thursday Night.

**Monthly Proactive Maintenance** – This performs several tasks on the PC or Laptop meant to help keep its performance the best that it can be. Some of the tasks included are, but not limited to: Sync time with Domain Controller, Delete files in all “temp” folders, Delete files in the Windows Update Download folder, Delete all other temporary files though out the system, Flush DNS, run a CHKDSK (requires a reboot), and other tasks as deemed necessary to maintain performance. Proactive Maintenance will run on Thursday Evenings as reboot does occur.

**Why does my machine need to be left ON but LOGGED OFF?**

The machine needs to be left ON to run the work as noted above. Machines should always be LOGGED OFF for Security reasons. It simply makes it harder for any type of cyber-attack to occur on a machine if it is logged off whenever it is not being used. When it is logged off all desktop applications and all documents are also closed.

**To be environmentally conscious, I shut off my machine each night. How can my machine still receive these updates and Proactive Maintenance?**

Most machines have the ability to perform a “Wake-On-Lan” routine. This is a setting that needs to be enabled during the boot up process. Wake-On-Lan allows us to turn on the machine when it is off, run the necessary procedures and restart the machine. If you or your company is interested in this feature please contact us. A technician would need to come onsite and assess each machine individually. A reboot is required to turn on this feature.

NOTE: A single device does need to always be on to perform the Wake-On-Lan request to devices that are currently off. This task is usually handled by a server (which is always on).

**User Support**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Provide customer with a toll free number for all US and Canada domestic traffic to call during regular business hours
* Provide Customer Satisfaction Survey at ticket closure
* Record incoming calls for Quality Assurance purposes
* Provide service to all named (and billed for) users. Downstream consumers of IT are not covered, nor supported (your customers)
* User updates and removals
* Restoring connectivity to a network printer.
* Support software issues (see LOB support and productivity support)

**Elective Services** *available for additional fee*

* Support on personal content, including:
	+ iTunes
	+ photos
	+ personal applications
* After hours support is billed at an hourly rate

**Your Responsibilities**

* Notify the service desk of any new users or users that have left the organization

**Remote Connectivity**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Remote User Connectivity
	+ Corporate-owned assets (desktops, laptops, tablets and thin clients): VPN will be set up through the Fortinet
	+ RDP can be utilized when connected to the VPN, but will not be allowed from locations outside the network without the VPN
	+ Personally-owned assets (desktops, laptops, tablets): Log Me In will be the only supported method of connection. Support is not available on the personally-owned asset.
	+ Internet Service Provider (ISP) Support
		- All locations utilizing a supported Fortinet firewall will include ISP vendor management
			* Business Class internet connection is highly recommended
		- Public WiFi (Coffee shops, hotels, etc): No ISP vendor mgmt.
			* Help Desk will not contact support for these vendors
* VPN configuration and policies are backed up off site
* VPN connectivity troubleshooting according to Standard Service above
* Supply VPN software installation and setup instructions to approved end users

**Elective Services** *available for additional fee*

* Remote Office Connectivity
	+ Site to Site VPN tunnels can be configured between Fortinet firewalls
	+ Site to Site VPN tunnels between Fortinet and non-Fortinet devices may incur additional charges

Your Responsibilities

* Provide a list of users with approved remote connectivity and the specific requirements to internal resources
* End users must ensure that any unauthorized users are not allowed access to Corporate networks
* End users must keep secure all files, keys and passwords required to connect to the VPN

**Vendor Management**

**Our Responsibilities**

**Standard Service** *included in support fee*

* We will maintain contact and product information that is required to facilitate communications with 3rd party vendors.
* The Service Desk will make contact with a 3rd party vendor to escalate issues to the appropriate service contact.

**Elective Services** *available for additional fee*

* Not applicable

**Your Responsibilities**

* Provide all essential contact and product information to us during the onboarding process.
* Inform us of any changes in contact information for service procedures/requirements.
* Call the service desk directly for support
* Provide an accurate and detailed description of the issue
* Be willing and available to continue to work with the 3rd party’s support personnel as they trouble shoot issues.

**ISP Management**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Document and maintain ISP information provided by you
* In the event of an Internet issue:
	+ The Service Desk will independently perform any troubleshooting possible
	+ If we are unable to resolve independently, the Service Desk will call the primary and/or secondary contacts to perform on site troubleshooting
	+ If the issue cannot be resolved with the help of the on-site contacts, we will contact the ISP service desk to troubleshoot/resolve issues
* Facilitate support calls to ISP service desk for issues such as:
	+ Internet outages
	+ Internet slowness that isn’t network related
	+ Modem refreshes (When on site contact is unable to)

**Elective Services** *available for additional fee*

* + Not applicable

**Your Responsibilities**

* Be knowledgeable of the services you are being provided from your ISP
* Retain records of ISP account information and service contracts
* Notify us of any changes to ISP services and/or hardware
* The primary and secondary on site contacts should:
	+ Be educated on the physical location of ISP provided networking equipment (i.e: modem)
	+ Have access to ISP account information if needed
	+ Be prepared to assist in troubleshooting connectivity issues

**Line of Business Application Assistance**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Client updates or patches (defined as a newer release of the same software version that contains bug fixes, enhancements, security updates or additional hardware support)
* Ensure the end user can log into the application and that the server has connectivity
* Facilitate a warm transfer of the user for any issues beyond login
* Warm transfer involves conferencing in the manufacturer with the user and offering support info to the manufacturer, then disconnecting. If the manufacturer has a hold queue that is longer than 10 minutes, we will discuss with the user and then drop off the call. We will be available to be conferenced into the call between the vendor and the user if needed
* User administration (including add, remove and change), requires documented process from application manufacturer
* Contact the helpdesk with all service requests. Helpdesk will troubleshoot and if cannot resolve, will contact maintenance agreement provider to warm handoff the issue. If no maintenance agreement provider exists, a “best efforts” will be made to resolve the issue. This may require additional charges or a scoped project.
* Backup necessary files through managed backup product(s)

**Elective Services** *available for additional fee*

* Upgrades on both servers and clients (upgrades are defined as a major version change that is typically purchased.) \*This would be a project with a SOW
* Updates on the server
* Mass installation of software (new or re-installation)

**Your Responsibilities**

* Timely renewal of LOB maintenance (including phone support)
* Appoint a “power user” that is a go between for service desk and manufacturer
* Provide contact info and maintenance agreement info

Have time to work the issue when reporting it to the service desk. If the user is unable to work with the vendor during the original support call, we will provide the vendor number directly to the user and will be available for a conference call if needed

**RMM Productivity Application Assistance**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Service packs applied through RMM tool
* Installation and support of productivity applications, including:
	+ Internet Explorer
	+ Microsoft Office
	+ Java
	+ Adobe Flash Player
	+ Adobe Reader

**Elective Services** *available for additional fee*

* Not Applicable

**Your Responsibilities**

* Contact the service desk regarding incidents and service requests, provide an accurate description of the issue, including error messages and be reasonably available to work with the service desk on resolution
* Allow full access to managed equipment
* Train end users in the proper use of personal productivity and business applications
* Provide license media for all applicable software

**Phone System**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Standard process is for users to have contact information for the Phone System provider.
* Any support issues that come to the service desk will be given the appropriate contact information for phone issues. If phone support is provided by the Provider, either through a separate maintenance agreement or as an hourly service, escalations will be facilitated internally by the Provider to the appropriate support persons.

**Elective Support** *available for additional fee*

* Not applicable

**Output Device/Scanner Support**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Add network attached printer to workstation
* Troubleshoot printing issues; including driver re-install
* Troubleshoot scanning issues; including driver re-install
* Scan to email and scan to folder troubleshooting
* If device support is provided by the Provider, either through a separate maintenance agreement or as an hourly service, escalations will be facilitated internally by the Provider to the appropriate support persons.

**Elective Support** *available for additional fee*

* Set up printer shares on server
* Mass driver deployment
* Mass Address book changes
* SMTP email setup
* New driver download and install on server

**Your Responsibilities**

* Make available device service provider contact information (if not covered by us) and we’ll escalate issue accordingly

**Endpoint Security (Antivirus/Malware)**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Monitor the AV agent to ensure it is running properly and updates are being installed in a timely manner
* Run periodic scans on protected machines
* Remediate infected machines: We reserve the right to bill in excessive circumstances, or recurring instances
* Work with LOB vendor to ensure compatibility with AV Defender application, including setting and testing file/folder exclusions

**Elective Services** *available for additional fee*

* Not applicable

**DNS Filtering**

**Our Responsibilities**

**Standard Service** *included in support fee*

* DNS requests will be routed through a Cloud service that compares the record to a list of addresses known to be malicious. If the record is flagged, access to the address is denied. The user is presented with a web page indicating the address is blocked because it is known to be malicious.
* Security settings apply to all users

**Elective Services** *available for additional fee*

* Not Applicable

**Unified Threat Management**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Hardware, and full replacement warranty
	+ Next business day replacement shipping
* Automatic replacement of appliance at the end of useable life
* Operating system updates (FortiOS)
* Real-time FortiGuard signature updates for AV, content filter, intrusion prevention system
* Monitoring and management
* Web Content Filtering:
	+ The following web content categories are blocked and will not be unblocked: Proxy Avoidance, Gambling, Nudity and Risqué, Pornography, Peer-to-Peer file sharing, Malicious Websites, Phishing, and Spam URLs. Sites in these categories pose a security risk which leave customers open to malware and hacking. Legitimate white list exceptions will be made when requested by the customer: e.g. Powerball.com, etc.
	+ The following categories will also be blocked by default, but may be unblocked if the customer requests: Drug Abuse, Hacking, Illegal or Unethical, Explicit Violence, Extremist Groups, and Child Abuse.
* Appliance configuration and policies are backed up off site
* Change requests:
	+ Requested changes to routing, policies, and Network / Port Address Translation
	+ Requested changes to content filtering (global policy changes only)
	+ Investigating security alerts
	+ Investigating alerts generated by PRTG and FortiAnalyzer
	+ Monitoring signature updates
	+ Monitoring health of appliance
	+ Manually updating signatures when automatic updates fail
	+ Manually updating operating system when automatic update fails
	+ Configuration changes due to ISP change
	+ VPN support (largest number of tickets)
		- Site to site (Fortinet to Fortinet)
		- User VPN
* Ability to upgrade or downgrade to other appliances in the program

**Elective Services** *available for additional fee*

* Assistance with answering questions for compliance / regulations / audit.
* Setup, configure or make changes to hardware that we do not control (VPN set up, point to point connections, MPLS-style connections)
* Web Content Filtering, multiple policies: different web content filtering policies to apply different rules to different groups of users.
* Web Content Filtering, user reporting: gives the customer the ability to see where specific users are going on the Internet.
	+ 90 days of live data available for reporting on traffic/web utilization and UTM events
	+ 3 months of archived data available

**Your Responsibilities**

* Customer should be familiar with the location of the firewall in case the Service Desk needs the customer to assist in very basic troubleshooting. e.g. rebooting the appliance

**Hosted Email, O365 – MS Exchange**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Hosted, secure instance of Microsoft Exchange which is fully monitored and administered.
* Every user receives a mailbox, storage, calendar, contacts, notes, and tasks.
	+ Storage and Features vary from package to package.
* We will provide client email boxes customized to your company email domain.
* Support for the email service.
	+ Assist the user in resetting passwords
	+ Assist user in enabling inbox rules
	+ Investigate mail flow issues and run message audits – why was an email not received?
	+ Manage mailbox permissions (delegates, “Send As”, “Full Access”)
* Additions, removals, and changes to mailboxes, aliases, distribution lists, and company contacts.
	+ Mailbox may remain active for 90 days after employee leaves the organization.
	+ See New User Setup document
	+ Creation of .PST (upon request)
* Assist with setting up default email client on iOS, Windows and Android mobile devices.
* Configure users’ Outlook profiles to connect to the Exchange service
* Configure spam filter – white list, black list, and custom policies
* Remotely wipe mobile device, with written request (caution –completely wipes the entire device)
* Unauthenticated Relay for one public IP address per account – requires static public IP address

**Elective Services** *available for additional fee*

* Elective add-on services:
	+ Compliant Email Archival
	+ Message encryption
		- Encrypted message – user decides which emails are encrypted
		- Policy based email encryption – rules dictate which emails are encrypted
	+ Company Disclaimer automatically appended to the end of each email
	+ Resource mailboxes – typically used for reserving meeting rooms
	+ Microsoft Lync – Standard or Enterprise
	+ Microsoft Outlook License
	+ Microsoft Office Suite – Outlook, Word, Excel, PowerPoint, OneNote, and Publisher
	+ POP3 / IMAP email may be used for utility accounts only – software applications or hardware (printers, scanners, etc). POP / IMAP accounts are not for users.
* Elective support work:
	+ Change customer name in Exchange system of record – required in the cases of mergers, acquisitions, divestitures, spin-off, or breakup.
	+ Grant users “Send As” permissions from a distribution list
	+ Microsoft Lync Federation
	+ Point in time restore of mailbox data within 7 days (typically used for single email deletion)
	+ Undelete a mailbox
	+ Generate hosted Exchange user report – mailboxes, company contacts, public folders and distribution lists (including list members).
	+ Modification of inbound and outbound transport rules

**System Limitations:**

* Mailbox size varies based on package selected
* Maximum company contacts: 5000
* Maximum message size (inbound and outbound): 50 MB
	+ If larger files needed, use File Sync product and email link
* Maximum recipients per message: 500

**Backup Data Recovery**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Backup jobs and appliances are monitored 24 x 7 and issues are remediated during business hours for the following issues:
	+ Failed backup
	+ Screenshot verification (VM successfully boots to login screen)
	+ Recoveries mounted for more than 3 days
	+ Device Hardware Failures
	+ Low disk space on appliance
	+ Appliance offline more than 1 hour
	+ Cloud incrementals are out of sync by more than 5 days
* Restore individual files in the event they are lost, deleted, or corrupted
	+ Average restore time for last year is around 1 hour per file/folder
* Exchange Granular Recovery (Mailbox, Message, Contact from On-Premise Exchange)
	+ Datto Alto2 requires the purchase of a Granular Restore license.
* Ongoing proactive maintenance and testing:
	+ Proactive, regularly scheduled appliance reboots – in accordance with Datto’s best practices
	+ Mount and check all volumes in a file restore without issue – Quarterly
	+ Virtualization testing on 6 month rotational basis
		- Virtualize each protected server locally without any discrepancies – annually (opposite offsite)
		- Offsite Virtualization of each protected server – annually (opposite local)
* Datto Siris Network Attached Storage: NAS storage on the Datto Siris is reserved exclusively for backup purposes only and may not be used for active storage accessible by users. By default, we do not replicate Siris NAS data to the Cloud. For example: such a NAS would be the target for a SQL backup.
* During a continuity event:
	+ Bare Metal Restore: restore the server image to the original hardware, new dissimilar hardware, or virtualized environment
	+ Local Virtualization:
		- BDR appliances are not intended to be used as production servers for extended periods. In most cases, performance will not be as good as the original server, and backup jobs from other servers may be adversely affected. It is advised to replace or repair the production server as soon as possible – 30 days is too long to use a BDR as a production server.
		- Create a virtual instance of the server on the local appliance
		- Connect VM to the network, and ensure users can access applications and data
	+ Cloud Virtualization:
		- 30 days of Cloud virtualization are included per server, per year.
		- Create a virtual instance of the server in the Cloud
		- Includes creating a VPN connection, and ensuring the users can access applications and data
	+ Export Image:
		- Export a recovery point as a VMDK or VHD for import into a VMWare or Hyper-V virtual host environment
* Reporting: Provide information to facilitate business reviews

**Elective Services** *available for additional fee*

* Proof of Concept Virtualizations
	+ A Proof of Concept is a local virtualization above and beyond the 2 annual tests included in the standard service. These are typically requested because the customer needs first-hand verification of the integrity of their applications and data. Some exceptions apply – e.g. proof of concept virtualization is not practical for an Exchange server.
	+ Requests must be submitted at least two weeks in advance.
* Cloud virtualization beyond 30 days – this is to allow adequate time to repair / replace local servers and appliances, in the event of a disaster.
* For the specialized servers: (SQL and Exchange)
	+ Restore from what is retained in server natively
	+ If have to pull SQL backup from virtualized environment – fee is charged
	+ Best Practice: SQL backups are done to an excluded volume (so as not to have redundant copies) or local NAS share on appliance that is not replicated to the cloud

**File-Level Cloud Backup**

**Our Responsibilities**

**Standard Service** *included in support fee*

* Backup jobs are monitored 24 x 7 and remediated during business hours for the following issues:
	+ Backup Failures
	+ Backup job warnings (Job has not rung, No files changed, Warning with Notices)
* Recovery of individual files in the event they are lost, deleted, or corrupted

**Elective Services** *available for additional fee*

* Recovery of Exchange from Restored Files
* Recovery of SQL from Restored files

**Your Responsibilities**

* Awareness of what is being backed up and backup schedule
* Alerting service desk of changes to the backup job as needed

## Elective Offering

Elective technologies are optional that any environment may or may not need.

* **Email Add-ons:** Certain environments may require added functionality such as message archiving, encryption, disclaimer messaging, etc.
* **File Synchronization:** Ability to store and retrieve files via the cloud. Allows for a file storage system accessible via multiple devices and anywhere internet access is available.

Service Delivery

## Incident Management

Incidents are issues that arise when a user located at the Subscriber location is unable to function because they are experiencing an outage of a delivered service. Incidents range from minor to major issues. They can be affecting one or many users of the delivered service. We are notified of incidents via phone, email or automatic alerting via software monitoring tools.

**Ticket Creation and Prioritization**

The Service Desk is the single point of contact for initiating incidents, service requests, changes, and any requests for ticket escalation. Customers may contact the Service Desk toll free at via phone or email.

To measure (and thus minimize) rework, we may ask caller if this is a new or existing issue. This gives us the opportunity to reopen existing tickets rather than create a new one.

**It is important to note that requests received via email are categorized as a lower priority by default**. Therefore, any critical requests should be **initiated by calling** the Service Desk. If a critical need is initiated by e-mail**, it must be followed up with a telephone call to the Service Desk** to ensure proper prioritization. Failure to call may result in a ticket having a lower priority. When sending an email, summarize the nature of the need in the Subject field.

Upon ticket creation, the Subscriber will automatically be emailed a confirmation with the ticket or reference number. This confirmation notes that the request has been logged at the Service Desk and that it is being assigned. Subscriber is responsible for ensuring the Subscriber email address is provided to the Service Desk for update and resolution notification purposes.

The Service Desk assigns a priority to every incident submitted. A prioritization model is used to ensure a consistent approach to defining the sequence for ticket handling and to drive the assignment of resources. There are 4 incident priorities ranging from 1 being the most urgent & impactful to 4 being the least.

The Priority assigned to a ticket depends upon:

* Impact on the business; (number of users affected, scope and complexity of the incident)
* Urgency to the business; (time in which resolution is required)

**Ticket Handling**

Resources working tickets:

* **Tier 1 technicians** work Incidents and Service Requests
* **Tier 2 technicians** work escalated Incidents & Service Requests, Problems and Change Orders
* **Tier 3 technicians** work escalated Incidents & Service Requests, Problems and Change Orders
* **Customer Advocate team** monitors all tickets across all work roles to manage SLA performance and ensure tickets are being worked appropriately and within their respective priority
	+ This is not a technical resource, but in some cases may be able to resolve issues.

**User Support**

The Service Desk operates 7:00 a.m. - 7:00 p.m. Central time. As a “live answer” Service Desk, they offer a single point of contact for all customer submissions and inquiries relating to user incidents, problems and service requests.

A technician is on call and available after hours, on weekends and holidays for emergency support for an additional fee.

**Network Operations Center Support (NOC)**

The NOC is comprised of two teams:

* **Reactive Team**
	+ Technicians respond to Fault incidents. Something has failed and needs assistance.
* **Proactive Team**
	+ Technicians respond to Threshold Breach incidents. Something has crossed a preset threshold which generates a ticket. The incident should be addressed to avoid potential failure. This team also addresses problem tickets. *(See Problem Management)*

The NOC leverages robust software to continuously monitor Subscriber infrastructure. When an event occurs, the tools generate incident tickets in our ticketing system.

* During normal business hours, the NOC provides incident remediation, technical infrastructure analysis, problem management, and diagnostics. They also serve as an escalation point to the Service Desk during their hours of operation.
* After hours the NOC provides incident remediation. Remediation after hours consists of looking at incidents during certain intervals throughout the after-hours period and remediating incidents as a batch of work. After hours remediation does NOT apply to user workstations and only available to Subscribers consuming all Core products (*See Core*).
	+ Special Note: We must have record of a contact from the Subscriber of a resource willing and able to assist outside of business hours if needed. (Example: Go onsite to flip a power switch)

**Incident Response Levels**

The Incident Response Level determines how we respond to an incident with a resource able to reasonably able to address the incident. We commit to the Performance Objectives stated below for 90% of incidents.

**Performance Objectives by Communication Type:**

|  |  |  |
| --- | --- | --- |
| **Incident Request** | **Definition** | **Initial Tech Work Begins** |
| Priority 1 |  Issue of such criticality that it requires immediate and sustained effort through resolution | 30 minutes |
| Priority 2 | Significant disruption to business, many users impacted (or VIP user), does not require sustained effort | 2 Hours |
| Priority 3 | Operations are restricted, but a workaround is available | 12 Hours |
| Priority 4  | The product is not working as designed. There is a minor impact to usage, but it is acceptable. A workaround has typically been deployed | 24 Hours |

## Service Requests

Service requests are requests from the Subscriber user that are not related to a degradation of delivered service. Examples include asking for access to an application, name changes, etc. Generally, service requests are not material changes to the environment, and as such don’t require documentation beyond what is noted in a ticket.

* Service requests are typically performed in a first in, first out order with the goal of turnaround being 24 hours or less
* Service requests don’t require permission beyond the individual user

**Change Orders**

Change Orders are requests to alter the existing Subscriber environment. Very often, this change may result in different expectations to the Offered Services, including economic impacts. (Examples include but not limited to, new equipment placements, location additions & changes, employee additions/terminations, etc.) As mentioned above, we combine “changes” with all service requests for simplicity in tracking.

Because change orders modify the Subscriber environment, the level of support provided can be impacted. As a result we require the Service Provider’s involvement *(contact account management for the Change Process diagram)*:

* Complete proper documentation BEFORE changes are made, (change forms, configuration forms, etc.) and submit to the Service Activation team.
* Provide reasonable lead time in advance of any planned changes to the end user environment.
* Place equipment (e.g. Servers) into “maintenance mode” so as to avoid generating alerts unnecessarily during service (e.g. reboots).

## Problem Management

Problem management is the investigation into themes relating to multiple incidents or the recurrence of the same incident in a short period of time. The Proactive Support Team regularly evaluates incidents to identify patterns. When a pattern is found, a problem ticket is created and is assigned to the appropriate work role to remediate the problem (root cause). The knowledgebase is updated as appropriate.

Miscellaneous

## Maintenance Windows

From time to time, maintenance will be performed on Subscriber environments. To deliver the best possible experience with the least amount of impact/interruption to the user, maintenance windows must be established. This may include the need for “unattended access” (machine being powered on but not logged in) to a user’s workstation.

Standard maintenance windows include:

* 10:00 p.m. to 4:00 a.m. each weekday evening (local time)
* Every Saturday & Sunday

## Subscriber Premises

**Site Environmentals**

* Customer must provide reasonable protection, control and monitoring of onsite environmentals associated with the presence of technical infrastructure, including Service Provider owned assets. This includes, but not limited to, HVAC, static electricity, humidity, air circulation, electrical circuits and line fluctuations, flooding, physical access, space management, and BCP/DR plans for the environmental controls.
* If a new location or site is being considered for services, a site survey will be conducted by Service Provider, to determine if there are environmental concerns or other issues that need to be addressed as part of the Service Activation process. Any issues that cannot be addressed or that are non-standard will be documented, including additional costs (if applicable) and other actions needed to mitigate the risk or concern.

**Physical and Remote Access and changes to our equipment on premise**

* Subscriber must provide timely physical site access to provide the necessary support for the services being provided to that location. Access must be provided to assets located on customer premises, including access to server closets, wiring closets, switches and other managed devices.
* Service Provider is responsible for storing and administering security devices for customer premises. (e.g. keys, door cards, etc.)
* Our staff will reasonably adhere to customer’s security access requirements where applicable.

## Service Provider Owned Equipment

As part of the IT Support Services (“Technology Stack”), we may purchase and own equipment which is then rented to the Subscriber. This equipment may be subject to a restocking fee of up to 5 months the monthly recurring service amount.

## Security Standards and Policies

The Service Provider is responsible for ensuring that Subscriber systems, applications, processes and data are compliant with, and follow needed security standards. As an example, the Service Provider is responsible for classifying customer data and identifying additional security that may be required for data classifications such as HIPPA, PCI, etc.

Communication

## Methods

From time to time, our monitoring tools and/or platform may become unavailable, either through scheduled maintenance or unplanned outage. We will reasonably communicate with the Subscriber during these situations as needed.

## Regular Business Reviews

We will hold periodic reviews with Subscriber. The reviews will be facilitated by the Subscriber’s Account Manager as needed. The discussion revolves around a typical high-level staff meeting; (what’s going well, what are areas for improvement, etc.) relating to each specific area of delivery (sales, support, and Service Activation). The Service Provider will be provided reports to familiarize them with the services and service levels that have been delivered.

## Service Activation (Onboarding and Offboarding)

We will outline a timeline and plan for onboarding and service activation. During this time we will be onsite installing tools and services. This may require reboots of machines and user disruptions.