Service Level Agreement

2.1 Operational Support
Service Provider will have no support obligations for any products, services or events outside of Service Provider's span of control or if Customer's devices do not have operating systems that are currently supported by the manufacturers.

Service Provider will remediate incidents identified by Service Provider or Customer, according to the level of support purchased. Service Provider will take corrective action for incidents within its span of control so long as Customer has provided all required information to Service Provider.

During the resolution period of each incident, Service Provider will issue updates to Customer based on the severity of the Incident, as described later in this SLA.

Any incident caused by or involving third party vendors or content providers contracted directly by Customer is outside of Service Provider's span of control. Customer must pursue the resolution of an incident directly with the vendors and content providers. During the resolution period, Service Provider will provide information to Customer to assist an expeditious resolution of the incident.

2.2 Service Availability
The Service Provider Service Desk (the "Service Desk") is the single point of contact for initiating incidents, service requests, changes, and any requests for ticket escalation. User may contact the Service Desk toll free at 877.715.8484 or via email at a personalized email address that Service Provider provisions for each Customer that ends in "@myitrequest.com" (or via live chat for applicable offerings).

The Service Desk operates 7:00 a.m. – 7:00 p.m. Central Time Monday through Friday, other than on observed holidays.

A technician is on call and available after hours, on weekends and on observed holidays for emergency support. An answering service will take after hours calls and create a ticket. A technician will respond to the end user within one hour of the ticket creation. After hours support is billable in 15 minute increments (minimum 30 minutes) at the then-current hourly rate unless the agreement includes 24x7-user support.

2.3 Scheduled Maintenance Windows
From time to time, maintenance will be performed on Customer environments. To deliver the best possible experience with the least amount of impact/interruption to end users, maintenance windows are established. This may include the need for "unattended access" (machine being powered on, but not logged in) to an end user's workstation.

Service Provider’s standard maintenance windows include:

- 10:00 p.m. to 4:00 a.m. each weekday evening (local time based on the time zone settings of each device)
- Every Saturday & Sunday

2.4 Network Operations Center Support

The Service Provider Network Operations Center (“NOC”) provides incident remediation, technical infrastructure analysis, problem management, and diagnostics 7:00 a.m. – 7:00 p.m. Central Time, Monday through Friday, other than on observed holidays. They also serve as an escalation point to the Service Desk during its hours of operation (see Section 2.2 above).

2.5 Incident Management

Incidents are issues that arise when an end user at Customer 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 end users of the delivered Service(s). Service Provider is notified of incidents via phone, email, live chat or software monitoring alerting tools.

Requests received via email are categorized as a lower priority by default. Therefore, any critical issues should be reported 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.

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

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 the assignment of resources. There are four incident priorities ranging from one being the most urgent and impactful to four being the least.

The incident prioritization is dependent on:

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

2.6 Change Management

Service requests are requests from the Customer that are not related to a degradation of a delivered service. Examples include asking for access to an application, name changes, etc. Generally, service requests are not material changes to the environment. Service requests are typically performed in a first in, first out order and are assigned a priority four.

Change Orders are requests to alter the existing Customer environment. Often, this change may result in different expectations to the services being delivered, including economic impacts. Examples include, but are not limited to, new equipment placements, location additions and changes, employee additions/terminations.

Change Orders may modify the Customer environment; therefore, we require the Customer's involvement to:

- Provide proper documentation before changes are made which could include, but are not limited to, change forms and configuration forms
- Provide at least two business days' notice of any planned changes to the End User Customer environment
- Place necessary equipment into "maintenance mode" to avoid generating unwanted alerts during service

2.7 Service Activation (Onboarding and Offboarding)
The Service Provider Service Activation Team is the point of contact for all new service orders as well as service disconnects. All additions or removal of service requests should be executed by submitting appropriate forms.

The Service Activation team will connect with Customer to gather information related to the End User Customer environment being onboarded. Service Provider's ability to deliver the highest possible remote resolution rates and first call resolution rates may be affected if all requested information is not provided in the onboarding process.**3 Supplied Equipment**

3.1 Customer-Supplied Equipment
Customer recognizes that for Service Provider to effectively provide the Offered Services, the Customer's information technology systems must meet certain requirements and specifications, which will be provided in separate document.

If during the Term, Service Provider determines that any part of a Customer's system becomes unsupportable or in need of replacement for Service Provider to perform the Services, Service Provider will promptly notify Customer. If the Customer does not replace or upgrade the unsupportable device/program, Service Provider may discontinue providing the Services with respect to such device/program upon thirty (30) days' written notice to Customer. In no event shall Service Provider be liable for the costs incurred to upgrade or replace obsolete or defective hardware and/or software.

3.2 Service Provider-Supplied Equipment
As part of the Service Provider Offering, Service Provider may purchase and own Fortinet firewalls, access points and switches that are then rented to the Customer. In some instances, equipment may be subject to a term requirement. If equipment is returned with damaged or missing parts, Service Provider may invoice customer an amount equal to the MSRP of the device minus fees Customer already paid Service Provider for that device.

4 Service Levels

4.1 Service Levels to Customer

Service Provider tracks activity via tickets in our professional services automation system, remote monitoring system and knowledge base system

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

Service Provider will hold periodic reviews with the Customer. The reviews (commonly referred to as alignment meetings) will be facilitated by the Service Provider Strategic Business Advisor assigned to that Customer on a quarterly basis, or as needed.

4.2 Service Levels to End User Customer

Service Provider commits to the service levels stated in the table below for 80% of Service Desk incidents.

Incident Request	Definition	Initial Tech Work Begins
Priority 1	Issue of such criticality that it requires immediate and sustained effort through resolution	0.5 Business Hours
Priority 2	Significant disruption to business, many users impacted, does not require sustained effort	2 Business Hours
Priority 3	Operations are restricted, but a workaround is available	12 Business 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 Business Hours

End users have the ability to request higher priority in extreme situations. Service Provider monitors this ability and reserves the right to revoke if inappropriately used by Customer personnel.

4.3 Service Level Failures

<u>Failure to Perform – Service Provider</u>

If, as of the end of a given month, Service Provider has failed to meet the 80% commitment on the above service levels for any eligible Customer over a trailing three-month period, Customer is eligible to receive a credit equal to 5% of the recurring charges that were to be invoiced for in the given month. In order to be eligible, Customers must (a) meet the minimum requirements referenced here within (b) have had a total of 35+ user tickets worked by Service Provider over that trailing three-month period.

Failure to Perform – Customer

If Customer fails to meet the below stated expectations:

- Failure to submit documentation (order forms, configuration forms, etc.)
- Failure to respond to Service Provider requests/escalations for support

Service Provider retains the right to:

- Escalate all incidents relating to violation back to the Customer
- Charge for curative actions (e.g. labor) performed due to errors, omissions or negligence on the part of the Customer or other third party

5 Change to SLA language

Service Provider reserves the right, in its sole discretion, to reasonably, without materially diminishing the overall support services herein, change, modify, append or discontinue any of the support services outlined in this document with 30 days' notice to Customer.

Appendix A: Schedule of Fees

**Based on X users, X workstations and X servers*

- NOC + Service Desk Monthly Support Price of **$$$$**
  - Pages 8-20 Appendix C
- NOC Monthly Support Price of **$$$$**
  - Pages 8-11 Appendix C
- Basic User Support Monthly Support Price of **$$$$**
  - First section on page 8 Appendix C

NOC + Service Desk	Users	$42/month
	Servers	$85/month
NOC services	Workstations	$15.75/month
	Servers	$66/month
Basic User Support	Users	$28/month

Appendix B: Selected Services

Ongoing Support Services	Quantity
Server Support	
Workstation Support	
User Support	

- Hourly rate for all service and project work outside of scope of IT Support Services is $200.00.

Appendix C: Included Services

Basic User Support

Our Responsibilities

Standard Service *included in support fee*

- Unlimited calls and emails to the Service Desk from 8:00 am to 8:00 pm eastern time zone (Continental US).
    - Vendor engagement, including ISP and phone systems
    - Line of business application assistance
    - Productivity application assistance
- Microsoft Windows Workstations
    - User assistance for supported operating systems
    - Password resets and account unlocks
    - Creation of Outlook profiles
    - Email password resets
    - Changes to mailboxes and distribution lists
- Mobile Devices
    - Email account setup

**The Basic User Support offering requires a 12-month commitment to service.*

Workstation Support

Our Responsibilities

Standard Service for PC *included in support fee*

- 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*

- 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, warranty, 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
- Performance issues
- 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 efficiency 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

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 your machines remain **ON** in a **LOGGED OFF** (When you have gone home for the day) state Monday morning through Friday morning. Prior to logging off save and close all applications and open documents as needed.

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 (see Procedure that we run on PC's and Procedures that we run on Servers below). At times though, especially in relation to Anti-Virus and Microsoft Windows Updates, there are "Out-Of-Band" updates. These are considered extremely important and are meant to be applied As Soon As Possible. This could then be a Monday, Tuesday, or Wednesday evening and would likely cause a reboot. The Out-Of-Band updates are the ones that require leaving the machines ON and LOGGED OFF each night (for PC's and Laptops); not just Thursday Night.

Why does my machine need to ON and LOGGED OFF?

The machine needs to be 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. This is task is usually handled by a server (which is always on), and most environments have one.

Procedures that we run on PC's:

Thursday Evening is the "planned" 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" 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 categories like Critical, Security, Important, Update, and Feature Pack, and several 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 (See “What type of procedures will we run?” above).

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.

User Support

Our Responsibilities

Standard Service *included in support fee*

- Unlimited calls and emails to the Service Desk from 8:00 am to 8:00 pm eastern time zone (Continental US).
- 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 in 15-minute increments with a 30-minute minimum.
  - Our SLA is to start working the issue within the hour

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 contacts 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 their 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), following documented process
- Pass all service requests to us if there is no valid, documented maintenance agreement
- Backup necessary files through we 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

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 beyond us for phone support.
- Any support issues that come to the service desk will be given the appropriate contact information for phone issues

Elective Support *available for additional fee*

- Not applicable

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 support 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

Switches

Our Responsibilities

Standard Service *included in server support fee*

- Troubleshoot connectivity issues
- Supported brand/models:
    - Catalyst by Cisco

    - ProCurve by HP
- Provide reliable Ethernet LAN connectivity

  Elective Services available for additional fee
    - Network design

Your Responsibilities

- Know where switch is physically located
- Provide a person to cycle power, in the event NOC determines it should be done
- Provide administrative access information
    - Access method (GUI, Telnet, SSH, etc)
    - Username and Password

Wireless Networking

Our Responsibilities

Standard Service *included in support fee*

- Monitor installed equipment and Investigates alerts generated by PRTG and FortiAnalyzer
- Ensure operating system remains up to date
- Maintain firmware
- Repair malfunctioning equipment
- Replace defective equipment
- Provide assistance in determining Wi-Fi coverage

Your Responsibilities

- Ensure that only corporate owned, managed devices are on corporate Wi-Fi networks
- All personal devices are to utilize the guest networks

Hosted Email – 3rd Party (Office 365)

Our Responsibilities

Standard Service *included in support fee*

- Limited support for the email service only
    - Assist the user in resetting passwords
    - Assist the user with setting up Outlook profile
    - Assist the user with setting up default email client on mobile devices
    - Assign mailbox permissions (delegates, “Send As”, “Full Access”)
    - Creating mailboxes when licenses are available
    - Creating distribution lists
    - Changes to existing mailboxes and distribution lists
- Provide support for any service other than email (Company contacts, calendar, tasks, etc.)
- Provide support for any permissions issues experienced by user
- Provide support for server side issues (Service Desk will verify ability to log into OWA, if unable to log in there, will pass issue to Service Provider)
- Provide support for mobile devices beyond basic setup and verifying connectivity
- Mailbox and distribution list removals

Your Responsibilities

- Provide Administrative credentials to Office 365 Administrative Portal

Security Information and Event Management

Features

- 24/7/365 monitoring of SIEM events on specified devices
- Daily/Continuous log review
- Trend Analysis Reviews and Tuning
- Advanced Proprietary Threat Intelligence
- Demonstrate compliance with industry and regulatory mandates
- Proof to auditors and other third parties that IT controls are in place and effective
- Continually ensuring the integrity and privacy of critical data by:
    - Security Event Automation
    - Real-time monitoring and alerting
    - Multi-dimensional correlation
    - Compliance guidance and management
    - Integrated incident resolution management

- Reporting and analytics
- Remediation support

Our Responsibilities

Standard Service *included in support fee*

- Initiate sale of 3rd Party SIEM offering
- Implement data collection on specified (supported) devices
- Receive and acknowledge alerts from SIEM provider
- Remediate issues on supported SIEM devices
- Escalate issues to appropriate 3rd party on non-supported devices

Elective Services available for additional fee

- N/A

Your Responsibilities

- N/A

Appendix D: Onboarding Requirements

Servers

- **Servers must meet minimum requirements**
  - Disks must have 20% free space at onboarding (recommend maintaining 10% free at all times). Additionally, the minimum size for C drives is 40GB *(recommend 100GB)*.
  - RAM requirements are 4GB for Domain Controllers and 8GB for application servers, increasing as the application demands it. All servers (physical and virtual) must meet recommended specifications as published by the OS and application manufacturers.
  - RAID all new servers must be hardware RAID, Single purpose physical servers should be a minimum of RAID 1 and virtual hosts should be a minimum of a 4 disk, RAID 5 set.
    - If existing servers are software RAID, upgrade cycle will require hardware RAID.
  - Operating System must be a version currently supported by manufacturer.

Workstations and Peripherals

- **Workstations** must meet minimum requirements
  - Operating System Professional Microsoft Windows Operating System, must be versions currently supported by Microsoft, home versions are not allowed
  - RAM 4GB minimum