Services Guide

This Services Guide contains provisions that define, clarify, and govern the scope of the services described in the quote that has been provided to you (the "Quote"), as well as the policies and procedures that we follow (and to which you agree) when we provide a service to you or facilitate a service for you. If you do not agree with the terms of this Services Guide, you should not sign the Quote and you must contact us for more information.

This Services Guide is our "owner's manual" that generally describes all managed services provided or facilitated by Framework IT, LLC ("Framework IT," "FWIT", "we," "us," or "our"); **however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services").**

This Services Guide is governed under our Master Services Agreement ("MSA"). You may locate our MSA through the link in your Quote or, if you want, we will send you a copy of the MSA by email upon request. Capitalized terms in this Services Guide will have the same meaning as the capitalized terms in the MSA, unless otherwise indicated below.

Activities or items that are not specifically described in the Quote will be out of scope and will not be included unless otherwise agreed to by us in writing.

Please read this Services Guide carefully and keep a copy for your records.

Initial Audit / Diagnostic Services

In the Initial Audit/Diagnostic phase of our services, we audit your managed information technology environment (the "Environment") to determine the readiness for, and compatibility with, ongoing managed services. Our auditing services may be comprised of some or all the following:

- Audit to determine general Environment readiness and functional capability
- Review of hardware and software configurations
- Review of current vendor service / warranty agreements for Environment hardware and software (Must be HP, Dell, Lenovo, SonicWALL, Meraki, or Cisco equipment)
- Basic security vulnerability check
- Basic backup and file recovery solution audit
- Speed test and ISP audit
- Office telephone vendor service audit
- Email hosting audit
- IT support process audit

If deficiencies are discovered during the auditing process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and provide you with options to correct the deficiencies. **Please note, unless otherwise expressly agreed by us in writing, auditing services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the auditing process**. Issues that are discovered in the Environment after the auditing process is completed may be addressed in one or more subsequent quotes.

Onboarding Services

In the Onboarding phase of our services, we will prepare your IT environment for the ongoing, recurring managed services described in the Quote. During this phase, we will work with your Authorized Contact(s) to review the information we need to prepare the targeted environment, and we may also:

- Uninstall any monitoring tools or other software installed by previous IT service providers*
- Compile a full inventory of all protected servers, workstations, and laptops.
- Uninstall any previous endpoint protection and install our managed security solutions (as indicated in the Quote)
- Install remote support access agents (*i.e.*, software agents) on each managed device to enable remote support**
- Configure Windows® and application patch management agent(s) and check for missing security updates
- Optimize device performance including disk cleanup and endpoint protection scans
- Review firewall configuration and other network infrastructure devices
- Review status of battery backup protection on all mission critical devices
- Review and document current server configuration and status
- Determine existing business continuity strategy and status; prepare backup file recovery and incident response option for consideration
- Review password policies and update user and device passwords.
- As applicable, make recommendations for changes that should be considered to the managed environment

This list is subject to change if we determine, at our discretion, that different or additional onboarding activities are required.

If deficiencies are discovered during the onboarding process, we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of our monthly managed services. **Please note, unless otherwise expressly stated in the Quote, onboarding-related services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the onboarding process.**

The duration of the onboarding process depends on many factors, many of which may be outside of our control—such as product availability/shortages, required third party vendor input, etc. As such, we can estimate, but cannot guarantee, the timing and duration of the onboarding process. We will keep you updated as the onboarding process progresses.

* Note: Removal of existing monitoring tools/software/agents is included in this service; however, if the removal requires us to rebuild a device, then the rebuilding process will be out of scope and will be billed you on a time and materials basis at our then-current hourly rates.

** Note: Software agent installation will be attempted remotely; however, if remote installation is not possible, then we will require you to arrange a mutually convenient time with us when we can install software agents onsite.

Ongoing / Recurring Services

Ongoing/recurring services are services that are provided to you or facilitated for you on an ongoing basis and, unless otherwise indicated in a Quote, are billed to you monthly. Some ongoing/recurring services will begin with the commencement of onboarding services; others will begin when the onboarding process is completed. Please direct any questions about start or "go live" dates to your account manager.

Managed Services

SERVICES	GENERAL DESCRIPTION
Backup and Disaster Recovery	Implementation and facilitation of a backup and file recovery solution from our designated Third Party Provider. • Off-site cloud storage of backed up data in a Tier 3 data storage location • On-site backup to a local storage device ("Backup Appliance") for rapid onsite recovery • Backup locations are continuously scanned for changes. • Incremental snapshots • Application and Operating System imaging • 24/7 monitoring of backup system, including the offsite backup and the Backup Appliance • Preventive maintenance and management of imaging software. • Firmware and software updates of Backup Appliance. • Problem analysis by the network operations team. • Monitoring of backup successes and failures. • Daily backup job integrity checks. Backup Data Security: Data is encrypted with 265 AES encryption both in-transit and at rest as well as for HIPAA, GDPR and SOC 2 Type II compliance. All facilities housing backed up data implement physical security controls and logs, including security cameras, and have multiple internet connections with failover capabilities. Backup Retention: Backed up data will be retained for the periods indicated below, unless a different time period is expressly stated in the Quote. • *On-Premise Backups* All on-premise backups will be stored on a Network Attached Storage (NAS) device, which will be kept in a secure location with restricted access. On-premise backups will be performed daily and retained on a rolling thirty (30) day basis. • *Cloud Backups* All cloud backups will be stored in a secure, off-site location that meets the organization's security standards. Cloud backups will be performed daily and retained on a rolling six (6) month basis. Backup Alerts: Managed servers will be configured to inform of any backup failures. Recovery of Data: If you need to recover any of your backed up data, then the following procedures will apply: • Service Hours: Backed up data can be requested during our normal business hours. • Request Method. Requests to restore backed up data should be made through one of the following methods: ○ Email: helpdesk@frameworkit.com

	○ Web: https://na.myconnectwise.net/Support/index.htm?Company=fwccom ○ Telephone: 312-564-4888 • Restoration Time: We will endeavor to restore backed up data as quickly as possible following our receipt of a request to do so; however, in all cases data restoration services are subject to (i) technician availability and (ii) confirmation that the restoration point(s) is/are available to receive the backed up data. ○ Guaranteed Server Recovery Time to a Cloud Disaster Recovery Server: Four (4) hour recovery time (during normal business hours) of a virtual image of the server in the cloud. Note: This guaranteed recovery time does not include time expended to make changes to Client's managed network as may be necessary to accommodate/access the cloud-based backup. Any such changes, if required, will be performed at Framework IT's then-current hourly rates. • Restoration Fees: **Unless explicitly stated in the Quote, restoration of backed-up data is not included in Framework IT's backup service.** Restoration services, if required, will be billed to Client at Framework IT's then-current hourly rates.
Backup Monitoring	Implementation and facilitation of a backup monitoring solution from our designated Third Party Provider. Features include: • Monitoring backup status for certain backup applications then-installed in the managed environment, such as successful completion of backup, failure errors, and destination free space restrictions/limitations. • Helping ensure adequate access to Client's data in the event of loss of data or disruption of certain existing backup applications. **Note: Backup monitoring is limited to monitoring activities only and is not a backup and file recovery solution.**
Compliance-as-a-Service (CaaS)	**Implementation and facilitation of a regulatory-compliance solution from our designated Third-Party Provider** • Enable Client to monitor its compliance across multiple regulations, including HIPAA Security, HIPAA Privacy, and SOC 2. (Please see the Quote for the regulation(s) for which this service will be applicable). • Provide access to platform training videos, recommended processes, and templates relevant to Client's specific compliance needs (i.e., instruction on how to use the compliance platform itself, not substantive regulatory training for Client staff). • Collect and continuously update compliance evidence by integrating with Client's existing IT infrastructure and security solutions, as supported by the upstream vendor. • Enable Client to create automated reminders for upcoming and past-due compliance-related dates. • Generate personalized certificates automatically upon completion of applicable platform-based training modules. *Note:* CaaS requires Client's ongoing cooperation and participation. To the extent that Client provides incomplete, inaccurate, or outdated information, the results of the CaaS may be incorrect or incomplete and should not be relied upon. Certification of completion of regulatory compliance is valid as of the date on which such certification is awarded, but does not guarantee that Client will continue to be regulatory compliant in the future. It is strongly suggested that Client always maintain this Service with no lapse in the provision of this Service to help ensure that Client's business operations, processes, and procedures are and remain regulatory compliant on an ongoing and consistent basis.
Dark Web Monitoring	Automated dark web surveillance from our designated Third Party Provider for compromised domains and credentials.

	Credentials supplied by Client will be added into a system that continuously uses human and machine-powered monitoring to determine if the supplied credentials are located on the dark web. If compromised credentials are found, they are reported to Help Desk Services staff who will review the incident and notify affected end-users. Please note: This is a monitoring and alert service only. Remediation of compromised credentials is not included in this service. Dark web monitoring can be a highly effective tool to reduce the risk of certain types of cybercrime; however, we do not guarantee that the dark web monitoring service will detect all actual or potential uses of your designated credentials or information. * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Email Security	Implementation and facilitation of a trusted email threat protection solution from our designated Third Party Provider. • Managed email protection from phishing, business email compromise (BEC), SPAM, and email-based malware. • Friendly Name filters to protect against social engineering impersonation attacks on managed devices. • Protection against social engineering attacks like whaling, CEO fraud, business email compromise or W-2 fraud. • Protects against newly registered and newly observed domains to catch the first email from a newly registered domain. • Protects against display name spoofing. • Protects against "looks like" and "sounds like" versions of domain names. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.** **All hosted email is subject to the terms of our Hosted Email Policy and our Acceptable Use Policy.**
Endpoint Antivirus & Malware Protection	Implementation and facilitation of an endpoint malware protection solution from our designated Third Party Provider. • Artificial intelligence and machine learning to provide a comprehensive and adaptive protection paradigm to managed endpoints. • Detection of unauthorized behaviors of users, applications, or network servers. • Blocking of suspicious actions before execution. • Analyzing suspicious app activity in isolated sandboxes. • Antivirus and malware protection for managed devices. • Protection against file-based and fileless scripts, as well as malicious JavaScript, VBScript, PowerShell, macros and more. • Whitelisting for legitimate scripts. • Blocking of unwanted web content. • Detection of advanced phishing attacks. • Detection / prevention of content from IP addresses with low reputation. • Protects managed devices against the exploitation of zero-day vulnerabilities. *** Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**

Managed Extended Detection & Response (MXDR)	Implementation and facilitation of an endpoint malware protection solution with extended functionalities from our designated Third Party Provider. • Automated correlation of data across multiple security layers, endpoint, server, and the managed network, enabling faster threat detection. • Provides extended malware sweeping, hunting, and investigation. • Allows whitelisting for legitimate scripts. • Next-generation deep learning malware detection, file scanning, and live protection for workstation operating system. • Web access security and control, application security and control, intrusion prevention system. • Data loss prevention, exploit prevention, malicious traffic detection, disk and boot record protection. • Managed detection, root cause analysis, deep learning malware analysis, and live response. • On-demand endpoint isolation, advanced threat intelligence, and forensic data export. * Requires at least two layers (*e.g.*, endpoint, email, network, servers, and/or cloud workload.) **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
End User Security Awareness Training	Implementation and facilitation of a security awareness training solution from an industry-leading third party solution provider. • Online, on-demand training videos (multi-lingual). • Online, on-demand quizzes to verify employee retention of training content. • Baseline testing to assess the phish-prone percentage of users; simulated phishing email campaigns designed to educate employees about security threats. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Managed Firewall as a Service **(firewall appliance provided by Framework IT)**	• Provide a firewall configured for your organization's specific bandwidth, remote access, and user needs. • Helps to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; provides website content filtering functionality. • Firewall appliance is subject to "Hardware as a Service" terms and conditions located in this Guide. • Firewall appliance must be returned to Framework IT upon the termination of service. Client will be responsible for missing or damaged (normal wear and tear excepted) appliance. * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Hardware as a Service (HaaS)	The provisions and descriptions below apply to all hardware, devices, and accessories that are provided to you on a "hardware as a service" basis. • Scope. Provision and deployment of hardware and devices listed in the Quote or other applicable schedule ("HaaS Equipment").

	• Deployment. We will deploy the HaaS Equipment within the timeframe stated in the Quote, provided that you promptly provide all information that we reasonably request from you to complete deployment. This deployment guaranty does not apply to any software, other managed services, or hardware devices other than the HaaS Equipment. In addition, this deployment time frame may be extended as necessary to accommodate delays that are outside of our reasonable control, such as embargoes, labor or supply chain shortages, or other force majeure events. • Delayed Deployment. If you wish to delay the deployment of the HaaS Equipment, then you may do so if you give us written notice of your election to delay no later than five (5) days following the date you sign the Quote. Deployment shall not extend beyond two (2) months following the date on which you sign the Quote. You will be charged at the rate of fifty percent (50%) of the monthly recurring fees for the HaaS-related services during the period of delay. Following deployment, we will charge you the full monthly recurring fee (plus other usage fees as applicable) for the full term indicated in the Quote. • Repair/replacement of HaaS Equipment. Framework IT will endeavor to repair or replace HaaS Equipment within five (5) business days following the business day on which the applicable problem is identified by, or reported to, Framework IT and has been determined by Framework IT to be incapable of being remediated remotely. This warranty does not include the time required to rebuild your system, such as the time required to configure a replacement device, rebuild a RAID array, reload the operating system, reload and configure applications, and/or restore from backup (if necessary). • Technical Support for HaaS Equipment. We will provide technical support for HaaS Equipment in accordance with the Service Levels listed in this Services Guide. • Usage. You will use all HaaS Equipment for your internal business purposes only. You shall not sublease, sublicense, rent or otherwise make the HaaS Equipment available to any third party without our prior written consent. You agree to refrain from using the HaaS Equipment in a manner that unreasonably or materially interferes with our other hosted equipment or hardware, or in a manner that disrupts or that is likely to disrupt the services that we provide to our other clientele. We reserve the right to throttle or suspend your access and/or use of the HaaS Equipment if we believe, in our sole but reasonable judgment, that your use of the HaaS Equipment violates the terms of the Quote, this Services Guide, or the Agreement. • Return of HaaS Equipment. Unless we expressly direct you to do so, you shall not remove or disable, or attempt to remove or disable, any software agents installed in the HaaS Equipment. **Doing so could result in network vulnerabilities and/or the continuation of license fees for the software agents for which you will be responsible, and/or the requirement that we remediate the situation at our then-current hourly rates, for which you will also be responsible.** Within ten (10) days after the termination of HaaS-related Services, Client will provide Framework IT access to the premises at which the HaaS Equipment is located so that all such equipment may be retrieved and removed by us. If you fail to provide us with timely access to the HaaS Equipment or if the equipment is returned damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.
Managed Detection & Response (MDR)	FWIT will implement and facilitate a top-tier MDR solution from our designated Third Party Provider. 24/7/365 managed detection and response (MDR) platform combines network visualization, tradecraft detection, and endpoint security to rapidly detect and neutralize potential threats and lateral movement in its earliest stages.

	The MDR solution provides: • 24x7 Managed detection and response. • Contextually aware breach detection and response program leveraging a security operations and incident response platform and SOC. • Real time and continuous (24x7) monitoring and threat hunting. • Real-time threat response: MDR analysts triage all alerts and involved devices, reviewing created processes, network connections, currently running processes and other data as deemed appropriate. If malicious activity is observed, the SOC will take action to isolate impacted machines and mitigate the threat, including device isolation, device un-isolation, and can disable, delete, and restore scheduled tasks if deemed malicious. • The SOC will provide an Incident Response Report containing: A summary, specific times of events, devices and accounts involved, binary names, commands seen, installed security products, indicators of compromise, ticket information, post-incident actions or recommendations the Client can take to prevent or mitigate similar threats in the future. • Automatically suspend malicious processes executing malware or ransomware and alert the SOC. • SIEM (Security Information & Event Management System) Logging of Events, as deemed necessary by the SOC, from the Endpoint Detection & Response (EDR) and Managed Detection & Response (MDR) agents (assuming Client has purchased these services from FWIT). • 24x7x365 access to a security team for incident response* • Alerts handled in accordance with our Service response times, below. * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Managed Security Operations Center ("SOC")	Security Operations Center provided by our designated Third Party Provider. 24/7 SOC service manages and monitors your Managed Detection and Response (MDR) solutions, as well as MXDR, SIEM, and vulnerability management solutions (assuming Client has purchased these services from FWIT). If a threat is detected, the SOC will take immediate action to mitigate the threat to prevent unauthorized network infiltration, loss of data, and/or damage to the managed environment. The SOC has several mechanisms in place to respond, contain, and/or prevent compromises within a network. The SOC response options include: Windows Devices • Device Isolation: The device is not able to communicate to the network and nothing is able to communicate to it. The only exception to this is the agent required to retain SOC connectivity, allowing the SOC to monitor the isolated device during an active incident. • Device Un-Isolate: Device isolation can be lifted after isolation. • Scheduled Tasks: The SOC can disable, delete, and restore Scheduled Tasks if deemed malicious. Mac Devices • Device Isolation: The device is not able to communicate to the network and nothing is able to communicate to it. The only exception to this is the agent required to retain SOC connectivity, allowing the SOC to monitor the isolated device during an active incident. • Device Un-Isolate: Device isolation can be lifted after isolation. Microsoft 365 Through Cloud Response (Requires Cloud Response) • Disable User Account: An abused user account can be disabled and have all associated tokens expired to prevent further abuse.

	• Disable External Mail Forward Rule: A rule forwarding a user's emails to an external source can be disabled by the SOC to minimize damage. • Disable Enterprise Application: If an Enterprise Application is determined to be malicious, it can be disabled. Google Workspace Through Cloud Response (Requires Cloud Response) • Login from Unapproved Country: A user signs in from a country not on the approved list. • Suspicious Login: A login is flagged as suspicious by our analytics engine. This could be due to successful logins from TOR, risky countries, malicious VPN usage, or anomalous residential proxy usage. • Suspicious Email Filtering Rule Created: An email filter rule that's flagged as suspicious by our analytics engine. • External Email Forwarding Rule Created: A new email forward rule is created that sends mail to a mailbox outside your organization. • Ability to disable a Google Account * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Web Security	Implementation and management of Web Security service from our designated Third Party Provider. Features include: • Blocking users from landing on sites that contain malware. • Ensuring that file downloads are safe and free of malware. • Enforcing policies related to acceptable use of the Internet and control the types of websites that users can visit. • Protecting data from exfiltration attacks. • Improving Client's understanding of how its employees use the web for work. * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Moves, Additions & Changes ("MAC") Requests	MAC requests are service requests for enhancements, changes, moves, or additions to technology systems. In some instances, an incident resulting in the degradation or failure of a technology system will require a MAC service request to properly resolve. MAC requests will be determined by FWIT based upon ITIL definitions and standards. Common examples of Service Requests (MACs) include: • Employee onboarding and offboarding • Workstation/Laptop Upgrades • Workstation/Laptop Application Installation • Email changes related to mailboxes, distribution groups, public folders, access, etc. • Any other Service Request (MAC), as determined by FWIT, based upon ITIL definitions and standards. Framework IT will cover minor MACs, as defined above, unless they constitute a Project. Project work is defined as services that have a definitive end date (such as an installation or development project), as well as (i) services that impact more than one user or a core piece of infrastructure, or (ii) services that are estimated to take, or actually take, more than 8 hours to complete, or (iii) services that require multiple FWIT resources to implement (such as a service that would require a technician and a project manager).

Mobile Device Management (MDM)	This service enables FWIT to control, secure, and enforce policies on managed mobile devices. This service enables FWIT to: • Deploy new applications to mobile operating system devices. • Put a device into lost mode. • Locate a device through GPS. • Wipe the device. • Implement any other services or capabilities included with the MDM solution; provided, however, that such other services will only be covered if the additional service can be implemented by FWIT in 2 hours or less. Any onsite service pertaining to MDM will be billable at FWIT's standard tier 1 hourly rates. Client must initially meet, and continue to meet, all of the following requirements in order to receive MDM services: • Client must register all Apple devices with Apple Business Manager. • If registration in Apple Business Manager requires wiping the devices, FWIT will not be responsible for backing up or restoring the data on the mobile device unless otherwise agreed to in writing by FWIT. • Remediation or reformatting of devices so that they are eligible for enrollment in Apple Business Manager, and enrolling MacOS devices in Apple Business Manager, is **not included** in this Service and is subject to FWIT's standard hourly rates unless a Fixed Fee Quote is signed for said Service. • Client must also purchase appropriate MDM licensing for each device, which is not included in the MDM fee from FWIT. FWIT can quote the appropriate MDM licensing for the Client. • Insofar as FWIT needs physical possession of a mobile device to implement MDM services, Client will be responsible for all applicable shipping and handling charges, and Client will remain responsible for the risk of loss or damages to devices being shipped.
NIST 2.0 Risk Assessment	Perform a cybersecurity assessment under NIST CSF 2.0. Please see the NIST 2.0 Framework Assessment Service attached to this Services Guide.
Password Manager	Implementation and facilitation of a password management protection solution from our designated Third Party Provider. • Password Vault: Securely store and organize passwords in a secure digital location accessed through your browser or an app. • Password Generation: Generate secure passwords with editable options to meet specific criteria. • Financial Information Vault: Securely store and organize financial information such as bank accounts and credit card information in a secure digital location accessed through your browser or an app. • Contact Information Vault: Store private addresses and personal contact information within your vault accessed through your browser or an app.

	• Browser App: Browser extension permits easy access to your information including the vaults, financial information, contact information, and single sign-on through the app. • Smart-Phone App: Mobile phone app enables access to your vault and stored information on your mobile device. * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Penetration (Pen) Testing	Penetration testing (or "pen" testing) simulates a cyberattack against your IT infrastructure to identify exploitable vulnerabilities. Unlike ongoing vulnerability scanning services that provide a constant, static level of network scanning, pen testing may involve several stages of reconnaissance and actual attack methodologies (such as brute force attacks and/or SQL injection attacks) and may include unconventional and targeted attacks that occur during business and non-business hours. Pen testing may consist of any of the following: **External Pen Testing:** exposes vulnerabilities in your internet-facing systems, networks, firewalls, devices, and/or web applications that could lead to unauthorized access. **Internal Pen Testing:** Validates the effort required for an attacker to overcome and exploit your internal security infrastructure after access is gained. **PCI Pen Testing:** Using the goals set by the PCI Security Standards Council, this test involves both external and internal pen testing methodologies. **Web App Pen Testing:** Application security testing using attempted infiltration through a website or web application utilizing PTES and the OWASP standard testing checklist. Please see additional terms for Penetration Testing below. * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Helpdesk Services	• Remote support provided during our normal business hours, as stated on the signed Quote, for managed devices and covered software, including: - Router and Switch and Support - Computer Support (Level 1 and 2 support) - User Login/Authentication Support - Email System Support - Printer, Copier, Scanner Support - Storage Device or Cloud Storage Support • Tiered-level support provides a smooth escalation process and helps to ensure effective solutions. If remote efforts are unsuccessful, then Framework IT will dispatch a technician to the Client's premises to resolve Covered Incidents. The timing of onsite support is subject to technician availability and scheduling. Covered Incidents shall be limited to the interruption or degradation of the performance of one or more technology services covered under a Quote.
Infrastructure Maintenance & Support	• Configuration, monitoring, and preventative maintenance services provided for the managed IT infrastructure. • If remote efforts are unsuccessful, then Framework IT will dispatch a technician to the Client's premises to resolve covered incidents (timing of onsite support is subject to technician availability and scheduling).
Remote Monitoring and Management	Software agents installed in Covered Equipment (defined below) report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.

- Includes capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD partitions, not external devices such as USB or mapped drives)
- Includes routine operating system inspection and cleansing to help ensure that disk space is increased before space-related issues occur.
- Review and installation of updates and patches for supported software.

Requirements:

- MacOS devices are required to be enrolled in the client's Apple Business Manager account.
- If Framework must enroll the client's MacOS devices in Apple Business Manager, the labor will be billed at Framework's standard hourly rates.

In addition to the above, our remote monitoring and management service will be provided as follows:

Event	Server	Windows OS Computers	Mac OS Computers
Hardware Failures	Yes	No	No
Device Offline	Yes	No	No
Failed/Missing Backup	Yes	No	No
Failed/Missing Updates	Yes	Yes	No
Low Disk Space	Yes	No	No
Agent missing/misconfigured	Yes	Yes	Yes
Excessive Uptime	Yes	No	No
Automatic reboots within 24 hours of a patch being deployed	No	Yes	No

Security Incident & Event Monitoring (SIEM)

Implementation and facilitation of an industry leading SIEM solution from our designated Third Party Provider.

The SIEM service utilizes threat intelligence to detect threats that can exploit potential vulnerabilities against your managed network.

- Initial Assessment. Prior to implementing the SIEM service, we will perform an initial assessment of the managed network at your premises to define the scope of the devices/network to be monitored (the "Initial Assessment").

- Monitoring. The SIEM service detects threats from external facing attacks as well as potential insider threats and attacks occurring inside the monitored network. Threats are correlated against known baselines to determine the severity of the attack.

- Alerts & Analysis. Threats are reviewed and analyzed by third-party human analysts to determine true/false positive dispositions and actionability. If it is determined that the threat was generated from an actual security-related or operationally deviating event (an "Event"), then you will be notified of that Event.

  Events are triggered when conditions on the monitored system meet or exceed predefined criteria (the "Criteria"). Since the Criteria are established and optimized over time, the first thirty (30) days after deployment of the SIEM services will be used to identify a baseline of the Client's environment and user behavior. During this initial thirty (30) day period, Client may experience some "false positives" or, alternatively, during this period not all anomalous activities may be detected.

Note: The SIEM service is a monitoring and alert-based system only; remediation of detected or actual threats are not within the scope of this service and may require Client to retain Framework IT's services on a time and materials basis.

*** Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**

Server Monitoring & Maintenance	As part of our RMM service, we will monitor and maintain managed servers as follows: • Software agents installed in covered servers report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below. • Online status monitoring, alerting us to potential failures or outages • Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives) • Performance monitoring, alerting us to unusual processor or memory usage • Server essential service monitoring, alerting us to server role-based service failures • Endpoint protection agent monitoring, alerting us to potential security vulnerabilities • Routine operating system inspection and cleansing • Secure remote connectivity to the server and collaborative screen sharing • Review and installation of updates and patches for Windows and supported software • Asset inventory and server information collection Note: All maintenance services will be handled remotely. If Client requires FWIT to perform maintenance services onsite, or in any manner that deviates from FWIT's standard maintenance processes, then all such services, including travel time to and from Client's location, shall be billed to Client on a time and materials basis.
Multi-Factor Authentication	Implementation and facilitation of a two-factor authentication solution from our designated Third Party Provider. • Advanced two factor authentication with advanced administrative features • Secures on-premises and cloud-based applications • Permits custom access policies based on role, device, location • Identifies and verifies device health to detect "risky" devices * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Server Next-Generation Antivirus	Implementation and facilitation of a top-tier, next generation antivirus protection solution from our designated Provider. Software agents installed in covered server devices protect against malware and prevent intruder access. Used in coordination with other endpoint security layers and security solutions to form a comprehensive defense strategy. • Next-generation deep learning malware detection, file scanning, and live protection for Server OS • Web access security and control, application security and control, intrusion prevention system • Data loss prevention, exploit prevention, malicious traffic detection, disk and boot record protection * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Updates & Patching	• Remotely deploy updates (e.g., x.1 to x.2), as well as bug fixes, minor enhancements, and security updates as deemed necessary on all managed hardware. • Perform minor hardware and software installations and upgrades of managed hardware.

	• Perform minor installations (i.e., tasks that can be performed remotely and typically take less than thirty (30) minutes to complete). • Deploy, manage, and monitor the installation of approved service packs, security updates and firmware updates, as deemed necessary by Framework IT, on all applicable managed hardware. Please note: We will keep all managed hardware and managed software current with critical patches and updates ("Patches") as those Patches are released generally by the applicable manufacturers. Patches are developed by third party vendors and, on rare occasions, may make the Environment, or portions of the Environment, unstable or cause the managed equipment or software to fail to function properly even when the Patches are installed correctly. We will not be responsible for any downtime or losses arising from or related to the installation or use of any Patch. We reserve the right, but not the obligation, to refrain from installing a Patch if we are aware of technical problems caused by a Patch, or we believe that a Patch may render the Environment, or any portion of the Environment, unstable. Note: All maintenance services will be handled remotely. If Client requires FWIT to perform maintenance services onsite, or in any manner that deviates from FWIT's standard maintenance processes, then all such services, including travel time to and from Client's location, shall be billed to Client on a time and materials basis.
Virtual Chief Information Officer (vCIO)	The vCIO at Framework IT plays a pivotal role in providing comprehensive support to our clients across three key functions: 1. Partner Account Administration The vCIO is your primary contact for inquiries about service agreements with Framework IT, including cost and pricing details. They provide clarity on billing aspects and aid in understanding your service package. Client interactions are predominantly managed through scheduled meetings and email correspondence for effective communication and resolution. 2. Project Management As an integral part of our project delivery team, the vCIO is responsible for managing and executing projects recommended either through the Strategic Business Review process or in response to ad-hoc client requirements. The vCIO ensures that each project aligns with the client's objectives and is delivered with Framework IT's commitment to excellence. 3. Trusted Advisor and Consultation The vCIO serves as a key advisor, guiding technology decisions within your organization. This role includes up to 9 hours of consultation per quarter as part of your agreement, with a focus on strategic planning, forecasting, and technology road mapping. Please note, additional consultation is billed at Framework IT's Tier Engineer Hourly Rate, and the allocated quarterly hours are not transferable or accumulative. Consultation Focus Areas: • Aligning IT solutions and strategies with business goals and objectives. • Recommending IT products and strategies that support your business needs. • Conducting Strategic Business Reviews each quarter, accounting for 5 of the 9 allocated hours, to plan and forecast technological growth and budget management. • Overseeing technology budget as part of the Strategic Business Review. • Lifecycle management of hardware resources. • Assistance in managing and negotiating vendor contracts. • Enhancing the overall partner experience with Framework IT.

	• Advising on technical training for end-users to enhance skill sets. Note: The vCIO is committed to fostering a robust and strategic partnership with each client, ensuring that your technological needs are met with expertise and foresight.
Voice Over IP (VoIP) Services **(May also be referred to as: Cloud Phone System, VoIP Service, Hosted Phone System, Hosted PBX, Cloud Unified Communications, Cloud Call Center, or Cloud Contact Center)**	Implementation and facilitation of an industry-recognized VoIP solution from our designated Third Party Provider. Please speak to your technician for the features that are specific to the VoIP solution listed in your Quote. Please note, messaging services may be subject to a number of legal requirements, including those established under the Telephone Consumer Protection Act (TCPA); the CAN-SPAM Act; the Communications Act of 1934, as amended; the Federal Trade Commission Act; and implementing regulations and decisions adopted by the Federal Communications Commission and Federal Trade Commission. By accessing or using any hosted service for any messaging purposes (including but not limited to "consumer" Person to Person (P2P) and "Non-Consumer" Application to Person (A2P) messages via 10 Digit Long Code (10DLC)), Client agrees to adhere strictly to all applicable laws, rules, and regulations for such services. **Important**: There are additional terms related to the VoIP service, including your use of E911 features, toward the end of this Services Guide. Please read them carefully. You may be required to sign an additional consent form indicating your understanding and acceptance of the limitations of 911 dialing using the VoIP services.
Vulnerability Management	Implementation and facilitation of an industry-recognized vulnerability scanning solution from our designated Third Party Provider. Vulnerability Management delivers vulnerability reporting for internal (Requires Microsoft Defender), external, and cloud services, providing increased visibility into potential threats across endpoints, servers, internet-exposed services, and cloud services. INTERNAL SCAN (REQUIRES MICROSOFT DEFENDER FOR ENDPOINT*): Internal Scan evaluates managed internal, remote, and cloud-hosted virtual devices for known vulnerabilities and security risks that adversaries may leverage to compromise devices and spread across the network. Internal Scan is available through our integration with Microsoft Defender for Endpoint, enabling partners to view their Microsoft 365 security directly within the portal. *Note: Ensure your Microsoft Defender for Endpoint Plan includes Vulnerability Management. EXTERNAL SCAN: External Scan evaluates publicly exposed services within one or more external IP addresses for known vulnerabilities and security risks that adversaries may leverage to breach your network. CLOUD SCAN: Cloud Scan evaluates configurations across your Microsoft 365 environment to identify missing security configurations, when stacked up against CIS Microsoft 365 Benchmarks. Controls are directly mapped within our portal, so you can easily review and implement changes to secure your cloud configurations. Vulnerability Management findings will be discussed during business review meetings with the Client, or more frequently as deemed appropriate by FWIT. Vulnerability Management reports will be made available to the Client upon request. Please see additional terms for vulnerability scanning below. * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**

Cloud Response	Implementation and facilitation of an industry-recognized Microsoft 365 or Google Workspace security monitoring solution from our designated Third Party Provider. Cloud Response extends the FWIT MDR into Microsoft 365 and Google Workspace environments. With Cloud Response, FWIT delivers active monitoring and unified response across the following cloud services: • Microsoft 365: Azure Active Directory (AD), Exchange, and SharePoint • Google Workspace: Google Account and Gmail Cloud Response enables our 24/7/365 SOC to see contextual data within your cloud environment and provide immediate and active response against anomalous behavior. Cloud Response enables FWIT to set up policy features to implement cyber hygiene processes across all users and monitor events through custom notifications. • SOC will be alerted to, and will investigate, logins from proxies, Tor, suspicious user agents, and/or risky countries. Consideration of the above factors, as well as previous user activity, previously detected events, and geopolitical research may lead to the SOC taking action and disabling the account. • The SOC will follow up with an IR Report containing the timeline, devices involved, accounts involved, processes observed, indicators of compromise, and post-incident actions that are recommended. Identity Response for Azure (Included in Cloud Response for Microsoft 365): Identity Response for Azure AD gathers contextual analysis about the unauthorized use of Azure SSO logins and the applications that requested the authentication. This information helps better protect your Azure environment and connected Azure SSO services from unauthorized logins and provides valuable context to assist in remediation efforts and impact assessment. * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Managed Application Control	Implementation and facilitation of an industry-recognized Managed Application Control solution from our designated Third Party Provider. Managed Application Control provides simplified oversight into application usage, on all Windows devices, regardless of location. Managed Application Control includes: • Blacklisting and blocking known malicious applications. This innovative solution takes a modern look at Zero Trust, delivering a prepackaged list of policies designed to block known, bad applications that have been observed by our Security Operations Center (SOC) in real attacks. • Blocking other applications, as requested by the Client. * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Managed Wireless Networking	Framework IT will manage Wireless Access Points at Client's premises to help ensure that wireless internet access is available in those areas requiring wireless network coverage, as agreed upon by Framework IT and Client. • Framework IT will maintain, supervise, and manage the wireless system. • Installed equipment, if provided by Framework IT, will be compatible with the then-current industry standards. • Framework IT will provide remote support services during normal business hours to assist with device connectivity issues. (Support services will be provided on a "best efforts" basis only, and Client understands that some end-user devices may not connect to the wireless network, or they may connect but not perform well).

	Please note: Any Wi-Fi devices, such as access points or routers, that are supplied by Client cannot be older than five (5) years from the applicable device's original date of manufacture, and in all cases must be supported by the manufacturer of the device(s).
Workstation Next-Generation Malware Solution	Implementation and facilitation of an industry-recognized, next generation workstation malware protection solution from our designated Third Party Provider. Software agents installed in covered devices protect against malware and prevent intruder access. Used in coordination with other endpoint security layers and security solutions to create a comprehensive defensive strategy. • Next-generation deep learning malware detection, file scanning, and live protection for Workstation OS. • Web access security and control, application security and control, intrusion prevention system. • Data loss prevention, exploit prevention, malicious traffic detection, disk, and boot record protection. * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Workstation Monitoring & Maintenance	Software agents installed in covered workstations report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below. • Online status monitoring, alerting us to potential failures or outages (Only on Windows OS computers).. • Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives) (Only on Windows OS computers). • Performance monitoring, alerting us to unusual processor or memory usage (Only on Windows OS computers). • Endpoint protection agent monitoring, alerting us to potential security vulnerabilities. • Routine operating system inspection and cleansing (Only on Windows OS computers). • Secure remote connectivity to the workstation and collaborative screen sharing. • Review and installation of updates and patches for Windows and supported software (Only on Windows OS computers). • Asset inventory and workstation information collection.
Managed Internet (Sometimes referred to as Managed Fiber Internet)	Framework provides managed internet service via a partnership with AT&T. Managed Internet Service may include Broadband internet, cellular internet, and Managed Fiber Internet. • The type of Managed Internet and the internet speeds will be specified on the signed Quote. Framework will provide local access and network connectivity to the client's demarcation point at their location. Any internal wiring required to extend the internet from the demarcation point to the client's network equipment, or any other physical accommodations required to deliver this Service, are out of scope and billed at FWIT's hourly rates. Managed Fiber Internet includes an edge-router provided and owned by FWIT. The edge-router is considered Hardware as a Service and is subject to the applicable terms in the Service Guide and MSA for Hardware as a Service.

	For Managed Fiber Internet Specifically: We will respond to problems, errors, or interruptions in the provision of the Services in the timeframe(s) described in Appendix A, attached. Severity levels will be determined by Framework IT in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; Framework IT will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.
Vendor Support & Management	Vendor support & management refers to the practice of FWIT troubleshooting directly on the client's behalf with other third-party technology vendors providing services to the Client. Vendor Support Management May Include: • Internet Service Provider • Third Party Copier/Scanner/Fax Peripheral Network Connection Management • Application Vendors - Software Assurance Management • Hardware Vendors - Warranty Management • Cloud Services Vendors
Standard Business Application Support	Full support is offered on the following standard business applications: Microsoft 365 suite, Microsoft Office Suite, Adobe, and G Suite.
Monthly Management Reporting	Monthly Management Reports that include Service Key Performance Indicators.
Technology Documentation Management	Framework IT will create and maintain the documentation of the Technology Environment that is covered by a particular Service, and which is necessary, or deemed valuable by FWIT, to provide Services to the Client.
Framework AI as a Service	**GENERAL DESCRIPTION** Implementation and facilitation of a secure, multi-LLM AI platform designed to enhance business productivity. This service provides your organization with the tools to leverage artificial intelligence for automation, workflow optimization, and agent-based tasks. • **Secure AI Platform:** Includes unlimited user access to a secure platform featuring most major Large Language Models (LLMs). • **Builder Platform:** Access to an integrated Automation, Workflow, and Agent Builder Platform. • **Training Resources:** Includes access to AI training resources to help your team get started. • **Credit Allotment:** A monthly allotment of credits is included. Exceeding this allotment will lead to degraded performance and may render certain services unavailable. Credit plans can be upgraded at any point. **Covered Support Services from Framework IT:** • Platform access and performance issues. • User management, including adding/removing users and password resets. • Please note: Q&A, help with platform features, and even assistance with building automations, workflows, and AI Agents is all available within the AI Platform itself natively.

	Excluded Services: The following services are not included in the monthly recurring fee: • Prompt coaching and prompt writing. • Building Custom GPTs, Workflows, Automations, or Agents. • Finding Custom GPTs, Workflows, Automations, or Agents in the marketplace. **One-Time Services:*** • **Custom Development:** Custom GPT, Workflow, Automation, or Agent building is available as a one-time, flat-priced service. This service is capped by hours and requires the client to fill out a discovery document and provide necessary knowledgebase materials. Framework IT will handle the build, initial testing, and one round of revisions based on client feedback. **These one-time services are not included in the recurring service fee and will be quoted separately on a time and materials basis.*

Fixed Fee and/or Pre-Paid Service Hours

If you purchase pre-paid service hours from us, then we will provide our professional information technology consulting services to you from time to time on an ongoing, "on demand" basis and debit your bank of pre-paid service hours with the number of hours we spend on your work. There is a minimum thirty (30) minute debit that will be made on each occasion that we provide on-demand services to you under this paradigm ("On-Demand Services"), and all such services will be debited in 15-minute increments, with partial increments rounded to the next highest increment.

The specific scope and timing of On-Demand Services (collectively, "Specifications") will be determined between you and us at or about the time that you request the On-Demand Services from us. If we determine that the Specifications need to be revised due to previously unknown unforeseen events or occurrences, then we will provide you with notice of the situation and revise the Specifications to accommodate the circumstances. If you do not object to the proposed revisions within two (2) business days after receiving them, then you will be deemed to have accepted the Specifications as revised by us.

You and we may finalize the Specifications (i) by exchanging emails confirming the relevant terms, or (ii) by you agreeing to an invoice, purchase order, or similar document we send to you that describes the Specifications (an "Invoice"), or in some cases, (iii) by us performing On-Demand Services or delivering the applicable deliverables in conformity with the Specifications.

If we provide you with an email or an Invoice that contains details or terms for the On-Demand Services that are different than the terms of the Quote, then the terms of the email or Invoice (as applicable) will control for those Services only.

An On-Demand Service will be deemed completed upon our final delivery of the applicable portions of Specifications unless a different completion milestone is expressly agreed upon in the Specifications ("Service Completion"). Any defects or deviations from the Specifications must be pointed out to us, in writing, within ten (10) days after the date of Service Completion. After that time, any issues or remedial activities related to the On-Demand Services will be billed to you at our then-current hourly rates.

Unless we agree otherwise in writing, On-Demand Services will be provided only during our normal business hours. Services provided outside of our normal business hours are subject to increased fees and technician availability and require your and our mutual consent to implement.

The priority given to On-Demand Services will be determined at our reasonable discretion, considering any milestones or deadlines expressly agreed upon in an invoice or email from Framework IT. If no specific milestone or deadline is agreed upon, then On-Demand Services will be performed in accordance with your needs, the specific requirements of the job(s), and technician availability.

Policies and Procedures Applicable to Services

Software Licensing: All software provided to you by or through Framework IT is licensed, not sold, to you ("Software"). In addition to any Software-related requirements described in Framework IT's Master Services Agreement, Software may also be subject to end user license agreements (EULAs), acceptable use policies (AUPs), and other restrictions all of which must be strictly followed by you and any of your authorized users.

When installing/implementing software licenses in the managed environment or as part of the Services, we may accept (and you agree that we may accept) any required EULAs or AUPs on your behalf. You should assume that all Software has an applicable EULA and/or AUP to which your authorized users and you must adhere. If you have any questions or require a copy of the EULA or AUP, please contact us.

Covered Environment.
Unless otherwise stated in the Quote, Covered Devices will only include technology assets (such as computers, servers, and networking equipment) owned by the Client's organization. As an accommodation, Framework IT may provide guidance in connecting a personal device to the Client's organization's technology, but support of personal devices is generally not included in the Scope of Services.

If the Quote indicates that the Services are billed on a "per user" basis, then the Services will be provided for up to the number of users indicated in the Quote; additional users can be added at additional cost. Please see our User Registration Policy, located here: https://octanecdn.com/frameworkitcom/frameworkitcom_594254270.pdf

We will provide support for any software applications that are licensed through us, as well as standard business applications such as Microsoft 365 suite, Microsoft Office Suite, Adobe, and G Suite. Line of Business ("LoB") application support is limited to supporting the underlying system the LoB application is installed on and supporting the performance and access of that supported underlying system. In all cases, software be supported on a "best effort" basis only and any support required beyond Level 2-type support will be facilitated with the applicable software vendor/producer.

If we are unable to remediate an issue with software (LoB or otherwise), then you will be required to contact the manufacturer/distributor of the software for further support. Please note: Manufacturers/distributors of such software may charge fees, some of which may be significant, for technical support; therefore, we strongly recommend that you maintain service or support contracts for all non-Supported Software ("Service Contract"). If you request that we facilitate technical support for non-Supported Software and if you have a Service Contract in place, our facilitation services will be provided at no additional cost to you.

In this Services Guide, Covered Hardware and Supported Software will be referred to as the "Environment" or "Covered Equipment."

Physical Locations Covered by Services. Services will be provided remotely unless, in our discretion, we determine that an onsite visit is required. Framework IT visits will be scheduled in accordance with the priority assigned to the issue (below) and are subject to technician availability. Unless we agree otherwise, all onsite Services will be provided at Client's primary business location. Additional fees may apply for onsite visits: Please review the Service Level section below for more details.

Minimum Requirements / Exclusions. The scheduling, fees and provision of the Services are based upon the following assumptions and minimum requirements, all of which must be provided/maintained by Client at all times:

- Server hardware must be under current warranty coverage
- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software and have all the latest Microsoft service packs and critical updates installed.
- All MacOS and iOS devices must be enrolled in the client's Apple Business Manager.
- All software must be genuine, licensed, and vendor- or OEM-supported.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The managed environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored.
- All wireless data traffic in the managed environment must be securely encrypted.
- All servers must be connected to working UPS devices.
- Recovery coverage assumes data integrity of the backups or the data stored on the backup devices. We do not guarantee the integrity of the backups or the data stored on the backup devices. Server restoration will be to the point of the last successful backup.
- Client must provide all software installation media and key codes in the event of a failure.
- Any costs required to bring the Environment up to these minimum standards are not included in this Services Guide.
- Client must provide us with exclusive administrative privileges to the Environment.
- Client must not affix or install any accessory, addition, upgrade, equipment, or device on to the firewall, server, or NAS appliances (other than electronic data) unless expressly approved in writing by us.

Exclusions. **Services that are not expressly described in the Quote will be out of scope and will not be provided to Client unless otherwise agreed, in writing, by Framework IT**. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by Framework IT in writing:

- Monitoring, supporting, diagnosing and/or remediation of any backup or cybersecurity solution that is not purchased through FWIT.
- Remediation of any Security Incident (defined below).
- Remediation of a full disaster-related situation.
- Recovery of lost or corrupted data.
- Replacing failed networking, server, or storage equipment or installing new networking, server, or storage equipment.
- Remediation of issues caused by lightning strikes, electrical surges, or force majeure events.
- Customization of third party applications, or programming of any kind.
- Support for operating systems, applications, or hardware that is no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- Battery backup replacement.
- Equipment relocation.
- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.
- Linux Operating System support.

- Removal of another IT vendor's monitoring or security software (other than in the Onboarding process, described above).
- Performance of administrative tasks that typically do not require the knowledge or expertise of an IT professional. This may include, for example, creating/modifying email signatures, setting out of office replies, creating meetings/invites on Client's behalf, clerical data entry tasks, maintaining file share organization (what files belong in which folders), etc.
- Shipping, courier, or logistics expenses.
- Technology training and orientation, including line of business applications.
- VoIP phone system support, configuration and administration.
- Support for equipment or devices that are not Covered Devices (defined above).
- Home network and home internet support, including personal computer support.
- Mobile device support, setup, and management.
- Audio visual systems support.
- Legal discovery, *i.e.*, providing support, assistance, or information in relation to a legal situation, lawful service of process, subpoena, discovery request or other court ordered obligation.
- The cost to bring the managed environment up to the minimum requirements listed above (unless otherwise noted in the Quote).

Service Levels for Service Desk / Customer Support. Our service desk / customer support services are provided as follows:

- Normal business hours: M-F, 8 AM – 5 PM Central Time
- After Hours & Weekend Service Desk Hours:
  - Monday – Friday 5 PM – 9 PM Central Time
  - Saturday – Sunday 8 AM – 5 PM Central Time
- Emergency Hours:
  - FWIT will cover emergencies, defined as (Priority 1 – Critical) issues 24x7
  - Priority Levels are determined by FWIT using a matrix of Impact & Severity, which is explained in here.

The above exclude legal holidays and Framework IT-observed holidays (as listed below). The specific business hours for services provided to you may vary; please check your Quote to determine whether the hours listed above differ from the hours during which the Services will be provided to you.

Unlimited Remote and Onsite Support.

FWIT shall provide unlimited remote and onsite support for "Incidents." Incidents are events that result in the interruption or degradation of the performance of one or more technology services or technology systems. Incidents do not include any Excluded Services (defined above).

FWIT seeks, but cannot guarantee, to resolve all issues remotely for expediency and efficiency. Onsite support for Incidents will be provided, as needed, at FWIT's sole and exclusive discretion, to meet FWIT's service obligations and goals.

Service Level Agreement ("SLA") Response Time

SLAs are for "Incidents," as defined above, and not for vCIO consulting or Service Requests, also known as Available Moves, Adds, Changes ("MACs"), which are defined below.

Ticket Priority is determined by FWIT, at its sole and exclusive discretion, in accordance with industry standards.

Response time is measured as the amount of time between FWIT's initial receipt of a reported issue (a ticket is created in FWIT's Professional Services Automation system) and FWIT's first interaction with the reported issue, defined as a review of the reported issue by an FWIT representative to determine the appropriate next step.

Response SLA Minutes & Hours are measured only during the relevant Service's business hours, as stated on the signed Quote for said Services.

Priority Levels are determined by FWIT using a matrix of Impact & Severity, which is explained in here.

Priority	Regular Service Desk Hours SLA	After Hours & Weekends SLA
Priority 1 (Critical)	30 Minutes	2 Hours
Priority 2 (High)	1 Hour	2 Hours
Priority 3 (Medium)	2 Hours	2 Hours
Priority 4 (Low)	4 Hours	4 Hours

FWIT's hourly rates can be found at our Rate Schedule pages, located at:

- https://octanecdn.com/frameworkitcom/frameworkitcom_530475436.pdf
- https://octanecdn.com/frameworkitcom/frameworkitcom_771316257.pdf

We reserve the right to modify our hourly rates from time to time, and modifications will apply to services provided to you after the date that the modifications take effect.

Framework IT-Observed Holidays: Framework IT observes the following holidays:

- New Year's Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- The day following Thanksgiving Day
- Christmas Eve
- Christmas Day
- New Year's Eve

Service Credits: Our service level target is meeting or exceeding 90% of the response times indicated above, as measured over a calendar month ("Target Service Level"). If we fail to adhere to the Target Service Level and Client timely brings that failure to our attention in writing (as per the requirements of our Master Services Agreement), then Client will be entitled to receive a pro-rated service credit equal to 1/30 of that calendar month's recurring service fees for the applicable Service (excluding hard costs, licenses, etc.) for each day on which the Target Service Level is missed. Under no circumstances shall credits exceed 30% of the total monthly recurring service fees under an applicable Quote. You must notify us of any missed Target Service Level within sixty (60) days after the date of the failure, otherwise you automatically waive that failure.

Fees. The fees for the Services will be as indicated in the Quote.

Additional Terms.

Reconciliation. Fees for certain Third Party Services that we facilitate or resell to you may begin to accrue prior to the "go-live" date of other applicable Services. (For example, Microsoft Azure or AWS-related fees begin to accrue on the first date on which we start creating and/or configuring certain hosted portions of the Environment; however, the Services that rely on Microsoft Azure or AWS may not be available to you until a future date). You understand and agree that you will be responsible for the payment of all fees for Third Party Services that are required to begin prior to the "go-live" date of Services, and we reserve the right to reconcile amounts owed for those fees by including those fees on your monthly invoices.

Changes to Environment. Initially, you will be charged the monthly fees indicated in the Quote. Thereafter, if the managed environment changes, or if the number of authorized users accessing the managed environment changes, then you agree that the fees will be automatically and immediately modified to accommodate those changes.

Travel Time. If onsite services are provided and, at our reasonable discretion, is required to provide or facilitate a Service that we manage for you, then we will travel to your location at no additional cost to you. On all other occasions, all travel time is billable and will be invoiced to you at our then-current hourly rates. Regardless of whether onsite service is covered under your managed services plan, you will be responsible for all tolls, parking fees, and related expenses that we incur in our provision of onsite services.

Appointment Cancellations. You may cancel or reschedule any appointment with us at no charge by providing us with notice of cancellation at least one business day in advance. If we do not receive timely a notice of cancellation/re-scheduling, or if you are not present at the scheduled time or if we are otherwise denied access to your premises at a pre-scheduled appointment time, then you agree to pay us a cancellation fee equal to two (2) hours of our normal consulting time (or non-business hours consulting time, whichever is appropriate), calculated at our then-current hourly rates.

Access Licensing. One or more of the Services may require us to purchase certain "per seat" or "per device" licenses (often called "Access Licenses") from one or more Third Party Providers. (Microsoft "New Commerce Experience" licenses as well as Cisco Meraki "per device" licenses are examples of Access Licenses.) Access Licenses cannot be canceled once they are purchased and often cannot be transferred to any other customer. For that reason, you understand and agree that regardless of the reason for termination of the Services, fees for Access Licenses are non-mitigatable and you are required to pay for all applicable Access Licenses in full for the entire term of those licenses. Provided that you have paid for the Access Licenses in full, you will be permitted to use those licenses until they expire.

Managed Service Commencement. For managed services, the Services will commence, and billing will begin, on the date indicated in your invoice ("Commencement Date") and will continue through the initial term listed in the Quote ("Initial Term"). We reserve the right to delay the Commencement Date until all onboarding/transition services (if any) are completed, and all deficiencies / revisions identified in the onboarding process (if any) are addressed or remediated to Framework IT's satisfaction.

Per Seat/Per Device Licensing: **Regardless of the reason for the termination of the Services, you will be required to pay for all per seat or per device licenses that we acquire on your behalf. Please see "Access Licensing" in the Fees section above for more details.**

Removal of Software Agents; Return of Firewall & Backup Appliances: Unless we expressly direct you to do so, you will not remove or disable, or attempt to remove or disable, any software agents that we installed in the managed environment or any of the devices on which we installed software agents. Doing so without our guidance may make it difficult or impracticable to remove the software agents, which could result in network vulnerabilities and/or the continuation of license fees for the software agents for which you will be responsible, and/or the requirement that we remediate the situation at our then-current hourly rates, for which you will also be responsible. Depending on the particular software agent and the costs of removal, we may elect to keep the software agent in the managed environment but in a dormant and/or unused state.

Within ten (10) days after being directed to do so, you must remove, package and ship, at your expense and in a commercially reasonable manner, all hardware, equipment, and accessories leased, loaned, rented, or otherwise provided to you by Framework IT "as a service." If you fail to timely return all such equipment to us, or if the equipment is returned to us damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

Offboarding. Subject to the requirements in the MSA, Framework IT will off-board Client from Framework IT's services by performing one or more of the following:

- Removal / disabling of monitoring agents in the Environment.
- Removal / disabling of FWIT-provided endpoint software from the Environment.
- Removal / disabling of FWIT-provided Microsoft 365 from the Environment (unless the licenses for Microsoft 365 are being transferred to your incoming provider; please speak to your Framework IT Virtual Chief Information Officer (vCIO) for details.)
- Termination of SQL or Remote Desktop licenses provided by Framework IT.
- Removal of FWIT administrator credentials from the Environment.
- Removal of FWIT-provided backup software from the Environment.

Additional Policies

Authenticity

Everything in the managed environment must be genuine and licensed, including all hardware, software, etc. If we ask for proof of authenticity and/or licensing, you must provide us with such proof. All minimum hardware or software requirements as indicated in a Quote or this Services Guide ("Minimum Requirements") must be implemented and maintained as an ongoing requirement of us providing the Services to you.

Monitoring Services; Alert Services

Unless otherwise indicated in the Quote, all monitoring and alert-type services are limited to detection and notification functionalities only. Monitoring levels will be set by Framework IT, and Client shall not modify these levels without our prior written consent.

Configuration of Third Party Services

Certain third party services provided to you under a Quote may provide you with administrative access through which you could modify the configurations, features, and/or functions ("Configurations") of those services. However, any modifications of Configurations made by you without authorization could disrupt the Services and/or cause a significant increase in the fees charged for those third party services. For that reason, we strongly advise you to refrain from changing the Configurations unless we authorize those changes. You will be responsible for paying any increased fees or costs arising from or related to changes to the Configurations.

Modification of Environment

Changes made to the Environment without our prior authorization or knowledge may have a substantial, negative impact on the provision and effectiveness of the Services and may impact the fees charged under the Quote. You agree to refrain from moving, modifying, or otherwise altering any portion of the Environment without our prior knowledge or consent. For example, you agree to refrain from adding or removing hardware from the Environment, installing applications on the Environment, or modifying the configuration or log files of the Environment without our prior knowledge or consent.

Anti-Virus; Anti-Malware

Our anti-virus / anti-malware solution will generally protect the Environment from becoming infected with new viruses and malware ("Malware"); however, Malware that exists in the Environment at the time that the security solution is implemented may not be capable of being removed without additional services, for which a charge may be incurred. We do not warrant or guarantee that all Malware will be detected, avoided, or removed, or that any data erased, corrupted, or encrypted by Malware will be recoverable. To improve security awareness, you agree that Framework IT or its designated third party affiliate may transfer information about the results of processed files, information used for URL reputation determination, security risk tracking, and statistics for protection against spam and malware. Any information obtained in this manner does not and will not contain any personal or confidential information.

Breach/Cyber Security Incident Recovery

Unless otherwise expressly stated in the Quote, the scope of the Services does not include the remediation and/or recovery from a Security Incident (defined below). Such services, if requested by you, will be provided on a time and materials basis under our then-current hourly labor rates. Given the varied number of possible Security Incidents, we cannot and do not warrant or guarantee (i) the amount of time required to remediate the effects of a Security Incident (or that recovery will be possible under all circumstances), or (ii) that all data or systems impacted by the incident will be recoverable or remediated. For the purposes of this paragraph, a Security Incident means any unauthorized or

impermissible access to or use of the Environment, or any unauthorized or impermissible disclosure of Client's confidential information (such as user names, passwords, etc.), that (i) compromises the security or privacy of the information or applications in, or the structure or integrity of, the managed environment, or (ii) prevents normal access to the managed environment, or impedes or disrupts the normal functions of the managed environment.

Environmental Factors

Exposure to environmental factors, such as water, heat, cold, or varying lighting conditions, may cause installed equipment to malfunction. Unless expressly stated in the Quote, we do not warrant or guarantee that installed equipment will operate error-free or in an uninterrupted manner, or that any video or audio equipment will clearly capture and/or record the details of events occurring at or near such equipment under all circumstances.

Fair Usage Policy

Our Fair Usage Policy ("FUP") applies to all services that are described or designated as "unlimited" or which are not expressly capped in the number of available usage hours per month. An "unlimited" service designation means that, subject to the terms of this FUP, you may use the applicable service as reasonably necessary for you to enjoy the use and benefit of the service without incurring additional time-based or usage-based costs. However, unless expressly stated otherwise in the Quote, all unlimited services are provided during our normal business hours only and are subject to our technicians' availabilities, which cannot always be guaranteed. In addition, we reserve the right to assign our technicians as we deem necessary to handle issues that are more urgent, critical, or pressing than the request(s) or issue(s) reported by you. Consistent with this FUP, you agree to refrain from (i) creating urgent support tickets for non-urgent or non-critical issues, (ii) requesting excessive support services that are inconsistent with normal usage patterns in the industry (*e.g.*, requesting support in lieu of training), (iii) requesting support or services that are intended to interfere, or may likely interfere, with our ability to provide our services to our other customers.

Hosted Email

You are solely responsible for the proper use of any hosted email service provided to you ("Hosted Email").

Hosted Email solutions are subject to acceptable use policies ("AUPs"), and your use of Hosted Email must comply with those AUPs—including ours. In all cases, you agree to refrain from uploading, posting, transmitting or distributing (or permitting any of your authorized users of the Hosted Email to upload, post, transmit or distribute) any prohibited content, which is generally content that (i) is obscene, illegal, or intended to advocate or induce the violation of any law, rule or regulation, or (ii) violates the intellectual property rights or privacy rights of any third party, or (iii) mischaracterizes you, and/or is intended to create a false identity or to otherwise attempt to mislead any person as to the identity or origin of any communication, or (iv) interferes or disrupts the services provided by Framework IT or the services of any third party, or (v) contains Viruses, trojan horses or any other malicious code or programs. In addition, you must not use the Hosted Email for the purpose of sending unsolicited commercial electronic messages ("SPAM") in violation of any federal or state law. Framework IT reserves the right, but not the obligation, to suspend Client's access to the Hosted Email and/or all transactions occurring under Client's Hosted Email account(s) if Framework IT believes, in its discretion, that Client's email account(s) is/are being used in an improper or illegal manner.

Backup (BDR) Services

All data transmitted over the Internet may be subject to malware and computer contaminants such as viruses, worms and trojan horses, as well as attempts by unauthorized users, such as hackers, to access or damage Client's data. Neither Framework IT nor its designated affiliates will be responsible for the outcome or results of such activities.

BDR services require a reliable, always-connected internet solution. Data backup and recovery time will depend on the speed and reliability of your internet connection. Internet and telecommunications outages will prevent the BDR services from operating correctly. In addition, all computer hardware is prone to failure due to equipment malfunction, telecommunication-related issues, etc., for which we will be held harmless. Due to technology limitations, all computer hardware, including communications equipment, network servers and related equipment, has an error transaction rate that can be minimized, but not eliminated. Framework IT cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Framework IT shall be held harmless if such data corruption or loss occurs.

Unless otherwise expressly stated in a Quote, BDR services do not permit archiving or retrieval of historical document or file versions; only the then-latest version of a stored document or file is recoverable. If Client requests that Framework provide BDR Services to the Client's network drives or workstation hard drives, the Client's administrator is responsible for providing Framework with written direction of the specific drives that should be routinely backed up, *i.e* the specific drives and storage areas that Client is requesting be backed up. Reconfiguring or moving folders within backed up directories could result in those folders no longer being backed up. **As such, if Client alters the configuration of any of its network drives or its workstation drives, the Client's administrator must provide immediate notice to Framework and receive written confirmation from Framework that the new configuration is being backed up by Framework**. Client assumes all responsibility and liability for failure to properly designate the specific drives that should be backed up using BDR Services.

BDR Services may be provided directly or through a third-party vendor. Client bears full responsibility for ensuring that the BDR Services are creating accurate backups. If the BDR Services are not successfully backing up the Client's designated data, Framework shall have no legal responsibility to the Client and/or any affected third party. Client agrees to indemnify and hold harmless Framework for any failure to properly backup the Client's (or a third party's) data and/or electronically store information. Framework bears no liability or legal responsibility for failure to preserve any electronically stored information.

Procurement

Equipment and software procured by Framework IT on Client's behalf ("Procured Equipment") may be covered by one or more manufacturer warranties, which will be passed through to Client to the greatest extent possible. By procuring equipment or software for Client, Framework IT does not make any warranties or representations regarding the quality, integrity, or usefulness of the Procured Equipment. Certain equipment or software, once purchased, may not be returnable or, in certain cases, may be subject to third party return policies and/or re-stocking fees, all of which shall be Client's responsibility in the event that a return of the Procured Equipment is requested. Framework IT is not a warranty service or repair center. Framework IT will facilitate the return or warranty repair of Procured Equipment; however, Client understands and agrees that (i) the return or warranty repair of Procured Equipment is governed by the terms of the warranties (if any) governing the applicable Procured Equipment, for which Framework IT will be held harmless, and (ii) Framework IT is not responsible for the quantity, condition, or timely delivery of the Procured Equipment once the equipment has been tendered to the designated shipping or delivery courier.

Business Review / IT Strategic Planning Meetings

We strongly suggest that you participate in business review/strategic planning meetings as may be requested by us from time to time. These meetings are intended to educate you about recommended (and potentially crucial) modifications to your IT environment, as well as to discuss your company's present and future IT-related needs. These reviews can provide you with important insights and strategies to make your managed IT environment more efficient and secure. You

understand that by suggesting a particular service or solution, we are not endorsing any specific manufacturer or service provider.

VCTO or VCIO Services

The advice and suggestions provided by us in our capacity as a virtual chief technology or information officer (if applicable) will be for your informational and/or educational purposes only. Framework IT will not hold an actual director or officer position in Client's company, and we will neither hold nor maintain any fiduciary relationship with Client. Under no circumstances shall Client list or place Framework IT on Client's corporate records or accounts.

Sample Policies, Procedures.

From time to time, we may provide you with sample (*i.e.*, template) policies and procedures for use in connection with Client's business ("Sample Policies"). The Sample Policies are for your informational use only, and do not constitute or comprise legal or professional advice, and the policies are not intended to be a substitute for the advice of competent counsel. You should seek the advice of competent legal counsel prior to using or distributing the Sample Policies, in part or in whole, in any transaction. We do not warrant or guarantee that the Sample Policies are complete, accurate, or suitable for your (or your customers') specific needs, or that you will reduce or avoid liability by utilizing the Sample Policies in your (or your customers') business operations.

Penetration Testing; Vulnerability Scanning

You understand and agree that security devices, alarms, or other security measures, both physical and virtual, may be tripped or activated during the penetration testing and/or vulnerability scanning processes, despite our efforts to avoid such occurrences. You will be solely responsible for notifying any monitoring company and all law enforcement authorities of the potential for "false alarms" due to the provision of the penetration testing or vulnerability scanning services, and you agree to take all steps necessary to ensure that false alarms are not reported or treated as "real alarms" or credible threats against any person, place, or property. Some alarms and advanced security measures, when activated, may cause the partial or complete shutdown of the Environment, causing substantial downtime and/or delay to your business activities. We will not be responsible for any claims, costs, fees, or expenses arising or resulting from (i) any response to the penetration testing or vulnerability scanning services by any monitoring company or law enforcement authorities, or (ii) the partial or complete shutdown of the Environment by any alarm or security monitoring device.

No Third Party Scanning

Unless we authorize such activity in writing, you will not conduct any test, nor request or allow any third party to conduct any test (diagnostic or otherwise), of the security system, protocols, processes, or solutions that we implement in the managed environment ("Testing Activity"). Any services required to diagnose or remediate errors, issues, or problems arising from unauthorized Testing Activity are not covered under the Quote, and if you request us (and we elect) to perform those services, those services will be billed to you at our then-current hourly rates.

Obsolescence

If at any time any portion of the managed environment becomes outdated, obsolete, reaches the end of its useful life, or acquires "end of support" status from the applicable device's or software's manufacturer ("Obsolete Element"), then we may designate the device or software as "unsupported" or "non-standard" and require you to update the Obsolete Element within a reasonable time period. If you do not replace the Obsolete Element reasonably promptly, then in our discretion we may (i) continue to provide the Services to the Obsolete Element using our "best efforts" only with no warranty or requirement of remediation whatsoever regarding the operability or functionality of the Obsolete Element,

or (ii) eliminate the Obsolete Element from the scope of the Services by providing written notice to you (email is sufficient for this purpose). In any event, we make no representation or warranty whatsoever regarding any Obsolete Element or the deployment, service level guarantees, or remediation activities for any Obsolete Element.

Licenses

If we are required to re-install or replicate any software provided by you as part of the Services, then it is your responsibility to verify that all such software is properly licensed. We reserve the right, but not the obligation, to require proof of licensing before installing, re-installing, or replicating software into the managed environment. The cost of acquiring licenses is not included in the scope of the Quote unless otherwise expressly stated therein.

The following additional policies ("Policies") apply to Services that we provide or facilitate under a Quote. By accepting a Service for which one or more of the Policies apply, you agree to the applicable Policy.

Shipping & Storage Policy

You are required to take the following steps in the order listed below when shipping equipment to Framework.

1. Notify Framework IT via a ticket that you have equipment to ship to our Chicago office. Include the complete contents of the package, the reason for the shipment, and the long-term intent of the equipment when Framework IT receives it.

   Example: "I need to ship Framework IT a laptop for a user no longer with our company. We plan to repurpose it for a new user we are presently interviewing to hire."
2. Framework IT's ticketing system will auto-reply with an email including the ticket number associated with the shipment.
3. At this time, order or create a shipping label for your shipment and send it to Framework IT at the following address:

   Framework IT
   ATTN: <**Your Ticket Number Here**>
   700 N Sacramento Blvd. Ste 101
   Chicago, IL 60612
4. Once ordered or shipped, respond to the ticket with the tracking number and ETA of the package.

General Policies Applicable to Shipping/Storage:

- Framework IT has limited storage space. As such, we do not offer long-term storage. Any equipment stored at the Framework IT office must have an intended use and be distributed within 90 days or 30 days for bulk items.
- Equipment held beyond 90 days with no intended purpose for the client will either be shipped back to the client or recycled. All costs incurred will be billed to Client.
- Framework IT reserves the right to charge for storing equipment at its sole discretion by providing advance notice of such costs to Client.
- Framework IT is not responsible for lost or stolen packages during shipment, while in transit, or after signature (unless signed for by a Framework IT employee).
- Client will be solely responsible for all communications with the shipping provider and any costs involved.
- Client must provide its shipping labels for equipment sent to Framework IT. We recommend insuring your package for the appropriate amount to cover the items in your shipment and requiring a signature upon delivery.
- Framework IT will provide the shipping label with appropriate shipment insurance for equipment shipped from Framework IT. All packages insured for over $500 will require a signature upon delivery. Framework IT will bill Client for shipping costs.
- Items shipped to Framework IT intended to be recycled will be done at cost to Client.
- Framework IT does not ship internationally.

VOIP – Dialing 911 (Emergency) Services

The following terms and conditions apply to your use of any VoIP service that we facilitate for you or that is provided to you by a third party provider of such service. Please note, by using VoIP services you agree to the provisions of the waiver at the end of this section. If you do not understand or do not agree with any of the terms below, you must not subscribe to, use, or rely upon any VoIP service and, instead, you must contact us immediately.

There is an important difference in how 9-1-1 (*i.e.*, emergency) services can be dialed using a VoIP service as compared to a traditional telephone line. Calling emergency services using a VoIP service is referred to as "E911."

Location: The address you provide to us for use with VoIP services is the location to which emergency services (such as the fire department, the police department, etc.) will respond. For this reason, it is important that you correctly notify us of the location at which you are using the VoIP services. PO boxes are not proper addresses for registration and must not be used as your registered address. Please note, even if your account is properly registered with a correct physical address, (i) there may be a problem automatically transmitting a caller's physical location to the emergency responders, even if the caller can reach the 911 call center, and (ii) a VoIP 911 call may go to an unstaffed call center administrative line or be routed to a call center in the wrong location. These issues are inherent to all VoIP systems and services. **We will not be responsible for, and you agree to hold us harmless from, any issues, problems, incidents, damages (both bodily- and property-related), costs, expenses, and fees arising from or related to any failure of emergency services to respond to locations to which they are requested.**

In addition to the above, you understand that calling 911 from a mobile or desktop application might result in a mismatch between your registered VoIP location and the location of the mobile or desktop device from which your call emanates. For that reason, if you are using a mobile or desktop application to call 911, you must provide emergency services with the address to which you need those services to respond. Do not assume that mobile or desktop applications will correctly convey the applicable location to emergency services.

Address Change(s): If you change the address used for E911 calling, the E911 services may not be available and/or may operate differently than expected. Moreover, if you do notify us of a change of address, then emergency services may be directed to the location where your services are registered and not where the emergency may be occurring. **For that reason, you must notify us of a change of address no less than three (3) business days prior to your anticipated move/address change**. Address changes that are provided to us with less than three (3) business days' notice may cause incorrect/outdated information to be conveyed to emergency service personnel. If you are unable to provide us with at least three (3) business days' notice of an address change, then you should not rely on the E911 service to provide correct physical location information to emergency service personnel. Under those circumstances, you **must** provide your correct physical location to emergency service dispatchers if you call them using the VoIP services.

Power Loss: If you lose power or there is a disruption to power at the location where the VoIP services are used, then the E911 calling service will not function until power is restored. You should also be aware that after a power failure or disruption, you may need to reset or reconfigure the device prior to utilizing the service, including E911 dialing.

Internet Disruption: If your internet connection or broadband service is lost, suspended, terminated, or disrupted, E911 calling will not function until the internet connection and/or broadband service is restored.

Account Suspension: If your account is suspended or terminated, then all E911 dialing services will not function.

Network Congestion: There may be a greater possibility of network congestion and/or reduced speed in the routing of E911 calls as compared to 911 dialing over traditional public telephone networks.

WAIVER: You hereby agree to release, indemnify, defend, and hold us and our officers, directors, representatives, agents, and any third party service provider that furnishes VoIP-related services to you, harmless from any and all claims, damages, losses, suits or actions, fines, penalties, costs and expenses (including, but not limited to, attorneys' fees), whether suffered, made, instituted or asserted by you or by any other party or person (collectively, "Claims") arising from or related to the VoIP services, including but not limited to any failure or outage of the VoIP services, incorrect routing or use of, or any inability to use, E911 dialing features. The foregoing waiver and release shall not apply to Claims arising from our gross negligence, recklessness, or willful misconduct.

Acceptable Use Policy

The following policy applies to all Services, including but not limited to (and as applicable) hosted applications, hosted websites, hosted email services, managed internet services, VoIP solutions, and hosted infrastructure services.

Framework IT does not routinely monitor the activity of hosted accounts except to measure service utilization and/or service uptime, security-related purposes and billing-related purposes, and as necessary for us to provide or facilitate our managed services to you; however, we reserve the right to monitor the Services at any time to ensure your compliance with the terms of this Acceptable Use Policy (this "AUP") and our master services agreement, and to help monitor and ensure the safety, integrity, reliability, or security of the Services.

Similarly, we do not exercise editorial control over the content of any information or data created on or accessible over or through the Services. Instead, we prefer to advise our customers of inappropriate behavior and any necessary corrective action. If, however, the Services are used in violation of this AUP, then we reserve the right to suspend your access to part or all of the Services without prior notice.

Violations of this AUP: The following constitute violations of this AUP:

- **Harmful or illegal uses**: Use of a Service for illegal purposes or in support of illegal activities, to cause harm to minors or attempt to contact minors for illicit purposes, to transmit any material that threatens or encourages bodily harm or destruction of property or to transmit any material that harasses another is prohibited.
- **Fraudulent activity**: Use of a Service to conduct any fraudulent activity or to engage in any unfair or deceptive practices, including but not limited to fraudulent offers to sell or buy products, items, or services, or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters" is prohibited.
- **Forgery or impersonation**: Adding, removing, or modifying identifying network header information to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous remailers or nicknames does not constitute impersonation.
- **SPAM**: Framework IT has a zero-tolerance policy for the sending of unsolicited commercial email ("SPAM"). Use of a Hosted Service to transmit any unsolicited commercial or unsolicited bulk e-mail is prohibited. You are not permitted to host, or permit the hosting of, sites or information that is advertised by SPAM from other networks. To prevent unnecessary blacklisting due to SPAM, we reserve the right to drop the section of IP space identified by SPAM or denial-of-service complaints if it is clear that the offending activity is causing harm to parties on the Internet, if open relays are on the hosted network, or if denial of service attacks are originated from the hosted network.
- **Internet Relay Chat (IRC)**: The use of IRC on a hosted server is prohibited.
- **Open or "anonymous" proxy**: Use of open or anonymous proxy servers is prohibited.
- **Crypto mining:** Using any portion of the Hosted Services for mining cryptocurrency or using any bandwidth or processing power made available by or through a Hosted Services for mining cryptocurrency, is prohibited.
- **Hosting spammers**: The hosting of websites or services using a hosted server that supports spammers, or which causes (or is likely to cause) our IP space or any IP space allocated to us or our customers to be listed in any of the various SPAM databases, is prohibited. Customers violating this policy will have their server immediately removed from our network and the server will not be reconnected until such time that the customer agrees to remove all traces of the offending material immediately upon reconnection and agree to allow Framework IT to access the server to confirm that all material has been completely removed. Any subscriber guilty of a second violation may be immediately and permanently removed from the hosted network for cause and without prior notice.
- **Email/message forging**: Forging any email message header, in part or whole, is prohibited.
- **Unauthorized access**: Use of the Hosted Services to access, or to attempt to access, the accounts of others or to penetrate, or attempt to penetrate, Framework IT's security measures or the security measures of another entity's network or electronic communications system, whether or not the intrusion results in the corruption or loss of data, is prohibited. This includes but is not limited to accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other networks, as well as the use or distribution of tools designed for compromising security such as password guessing programs, cracking tools, or network probing tools.

- **IP infringement**: Use of a Hosted Service to transmit any materials that infringe any copyright, trademark, patent, trade secret or other proprietary rights of any third party, is prohibited.
- **Collection of personal data**: Use of a Hosted Service to collect, or attempt to collect, personal information about third parties without their knowledge or consent is prohibited.
- **Disruptive Activity:** Use of the Hosted Services for any activity which affects the ability of other people or systems to use the Hosted Services or the internet is prohibited. This includes “denial of service” (DOS) attacks against another network host or individual, “flooding” of networks, deliberate attempts to overload a service, and attempts to “crash” a host.
- **Distribution of malware**: Intentional distribution of software or code that attempts to and/or causes damage, harassment, or annoyance to persons, data, and/or computer systems is prohibited.
- **Excessive use or abuse of shared resources**: The Hosted Services depend on shared resources. Excessive use or abuse of these shared network resources by one customer may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network performance is prohibited. You are prohibited from excessive consumption of resources, including CPU time, memory, and session time. You may not use resource-intensive programs which negatively impact other customers or the performance of our systems or networks.
- **Allowing the misuse of your account**: You are responsible for any misuse of your account, even if the inappropriate activity was committed by an employee or independent contractor. You shall not permit your hosted network, through action or inaction, to be configured in such a way that gives a third party the capability to use your hosted network in an illegal or inappropriate manner. You must take adequate security measures to prevent or minimize unauthorized use of your account. It is your responsibility to keep your account credentials secure.

To maintain the security and integrity of the hosted environment, we reserve the right, but not the obligation, to filter content, Framework IT requests, or website access for any web requests made from within the hosted environment.

Revisions to this AUP: We reserve the right to revise or modify this AUP at any time. Changes to this AUP shall not be grounds for early contract termination or non-payment.

Last Updated: September 2025

APPENDIX A

Service Levels for Network Availability

Appendix A ONLY applies to Managed Fiber Internet Service provided by Framework IT. The terms of Appendix A only apply to the Managed Fiber Internet Service and they shall apply to no other Services provided by Framework IT.

Framework IT's target Network Availability and performance objectives for the duration of each calendar month in a year shall be as follows:

Network Unavailability. The performance objective for the Managed Internet Service (MIS) Site Availability/Time to Restore SLA is for the MIS Site Availability to be 100%. If Framework IT does not meet this performance objective in any given calendar month, Client will be eligible for an MIS Site Availability/Time to Restore SLA credit for each Outage equal to the product of Client's total discounted Covered MIS Monthly Charges for the affected MIS Ports by a percentage based on the duration of (Time to Restore) the Outage, as set forth in the MIS Site Availability/Time to Restore SLA Credit Table below ("Service Credit"). Network Unavailability shall be deemed to begin upon the earlier of Framework IT's actual knowledge of the Network Unavailability or Framework IT's receipt of notice from Client of the Network Unavailability, and end when the Service is operational such that the Service is again able to transmit and receive packets to/from the Network and Access Port or Ports, as documented by Framework IT's records. Network unavailability does not apply to outages due to a power failure; due to failure of Client's local network; due to the failure or malfunction of non-Framework IT services, equipment, facilities, or systems; due to circumstances or causes (i.e. force majeure or act of God) beyond the control of Framework IT or its agents; caused in whole or in part by the negligence or acts or omissions of Client or its end users or its agents; or due to the failure or malfunction of services, equipment, facilities, or systems outside the Framework IT network past the point of minimum point of entry at the Client's site. Where Client provides its own local access circuits, any periods of Network Unavailability caused by failure of such local access circuits shall be further excluded from any calculation of Network Unavailability. Notwithstanding anything to the contrary in this SLA, in the Agreement or in any SOW, in no event shall any Network Unavailability or failure to meet any objectives or parameters under this SLA be deemed to be or constitute a breach by Framework IT of this SLA, the Agreement or any SOW.

- "Outage" means an occurrence within the Framework IT Network and/or the Framework IT-provided dedicated access (and in the case of MIS with Managed Router, the Framework IT CPE) that is unrelated to the normal functioning of MIS and that results in the inability of Client to transmit IP packets for more than one minute. Measurement of Time to Restore begins when a trouble ticket is opened by Framework IT Client Care and Client releases the affected Service Component(s) to Framework IT and ends when Framework IT Client Care makes its first attempt to notify Client that the problem has been resolved and the Service Component(s) are restored and available for Client to use. Time to Restore excludes Outage time that is outside of the standard operating hours of the local access provider used by Framework IT for the affected MIS Port and any delay caused by Client.

The MIS Site Availability/Time to Restore SLA does not apply for MIS with Managed Router installations if the dedicated POTS line is not provided by the Client and if it is determined the outage is related to the Managed Router.

MIS Site Availability/Time to Restore SLA Credit Table – Single Link / Single Router		
Time to Restore		**Country Group**
1 Minute	1 Hour	3.3%
1 Hour	2 Hours	3.3%
2 Hours	3 Hours	10.0%
3 Hours	4 Hours	10.0%
4 Hours	5 Hours	25.0%
5 Hours	6 Hours	25.0%
6 Hours	7 Hours	25.0%

7 Hours	8 Hours	25.0%
8 Hours	9 Hours	50.0%
9 Hours	10 Hours	50.0%
10 Hours	11 Hours	50.0%
11 Hours	12 Hours	50.0%
12 Hours	13 Hours	50.0%
13 Hours	14 Hours	50.0%
14 Hours	15 Hours	50.0%
15 Hours	16 Hours	50.0%
16 Hours	17 Hours	100.0%
17 Hours	18 Hours	100.0%
18 Hours	19 Hours	100.0%
19 Hours	20 Hours	100.0%
20 Hours	21 Hours	100.0%
21 Hours	22 Hours	100.0%
22 Hours	23 Hours	100.0%
23 Hours	24 Hours	100.0%
24 Hours	36 Hours	100.0%
36 Hours	Over 36 Hours	100.0%

MIS Site Availability/Time to Restore SLA Credit Table – Dual Link / Single Router		
Time to Restore		**Country Group**
Equal to or Greater than:	to Less than:	Group 1 Dual Link Single Router
1 Minute	1 Hour	3.3%
1 Hour	2 Hours	25.0%
2 Hours	3 Hours	25.0%
3 Hours	4 Hours	50.0%
4 Hours	5 Hours	50.0%
5 Hours	6 Hours	50.0%
6 Hours	7 Hours	50.0%
7 Hours	8 Hours	50.0%
8 Hours	9 Hours	100.0%
9 Hours	10 Hours	100.0%
10 Hours	11 Hours	100.0%
11 Hours	12 Hours	100.0%
12 Hours	13 Hours	100.0%
13 Hours	14 Hours	100.0%

14 Hours	15 Hours	100.0%
15 Hours	16 Hours	100.0%
16 Hours	17 Hours	100.0%
17 Hours	18 Hours	100.0%
18 Hours	19 Hours	100.0%
19 Hours	20 Hours	100.0%
20 Hours	21Hours	100.0%
21Hours	22 Hours	100.0%
22 Hours	23 Hours	100.0%
23 Hours	24 Hours	100.0%
24 Hours	36 Hours	100.0%
36 Hours	Over 36 Hours	100.0%

MIS Site Availability/Time to Restore SLA Credit Table – Dual Link / Dual Router		
Time to Restore		**Country Group**
Equal to or Greater than:	to Less than:	Group 1 Dual Link Dual Router
1 Minute	1 Hour	3.3%
1 Hour	2 Hours	50.0%
2 Hours	3 Hours	50.0%
3 Hours	4 Hours	50.0%
4 Hours	5 Hours	50.0%
5 Hours	6 Hours	50.0%
6 Hours	7 Hours	50.0%
7 Hours	8 Hours	50.0%
8 Hours	9 Hours	100.0%
9 Hours	10 Hours	100.0%
10 Hours	11 Hours	100.0%
11 Hours	12 Hours	100.0%
12 Hours	13 Hours	100.0%
13 Hours	14 Hours	100.0%
14 Hours	15 Hours	100.0%
15 Hours	16 Hours	100.0%
16 Hours	17 Hours	100.0%
17 Hours	18 Hours	100.0%
18 Hours	19 Hours	100.0%
19 Hours	20 Hours	100.0%

20 Hours	21Hours	100.0%
21Hours	22 Hours	100.0%
22 Hours	23 Hours	100.0%
23 Hours	24 Hours	100.0%
24 Hours	36 Hours	100.0%
36 Hours	Over 36 Hours	100.0%

Latency.

- Parameter. Framework IT shall use commercially reasonable efforts to maintain a monthly average Latency less than 37 milliseconds.
- Measurement. Latency is a monthly measure of the network-wide delay within the region or between regions, which is the average interval of time it takes during the applicable calendar month for test packets of data to travel between all selected pairs of Network Backbone Nodes in the region(s).
- Definitions. "Network Backbone Nodes" are the core routing nodes in the Network.
- Service Credit. If Framework IT does not meet its latency performance objective set forth herein in a given calendar month, Client will be eligible for MIS Latency SLA credit equal to 1/30th of Client's total MIS Monthly Charges for all MIS ports in the affected region for that month.

Data Delivery.

- Parameter. Framework IT shall use commercially reasonable efforts to maintain a monthly average Data Delivery of no less than 99.95%.
- Measurement: MIS data delivery percentage for a region or between regions is the average data delivery percentage for that month for all selected pairs of IP Backbone Nodes in the region(s) calculated by dividing data received by data delivered and multiplying by 100.
- Definitions. For purposes of this Section, "Data Delivered" is the number of test packets of data delivered in a month to an ingress router at a Network Backbone Node for delivery to an egress router at the other specific Network Backbone Node. "Data Received" is the number of such test packets of data that are actually received by the egress router at the other Network Backbone Node.
- Service Credit. If monthly average Data Delivery fails to meet the parameters set forth herein, Client shall be entitled to a SLA Credit equal to 1/30th of Client's total MIS Monthly Charges for all MIS ports in the affected region for that month.

MIS Jitter.

- Parameter. Framework IT shall use commercially reasonable efforts to maintain a monthly average Jitter of no more than 1.0 milliseconds.
- Measurement. The difference in time it takes a selected pair of test packets in a data stream to travel from one Network Backbone Node in a pair to another is measured for all selected pairs of Network backbone Nodes in the region(s) over the month. One of the test packets in the selected pair will always be a packet in the data stream that takes the least time to travel from one Network Backbone Node in a pair to another.
- Definitions. "MIS Jitter" is a monthly measure of the network-wide IP packet delay variation within or between the applicable region(s), which is the average difference in the interval of time it takes during the applicable calendar month for selected pairs of test packets of data in data streams to travel between selected pairs of Network Backbone Nodes in the regions(s).
- Service Credit. If monthly average Jitter fails to meet the parameters set forth herein, Client shall be entitled to a SLA Credit equal to 1/30th of Client's total MIS Monthly Charges for all MIS ports in the affected region for that month.

VoIP on MIS Site Availability SLA.

The performance objective for the VoIP on MIS Site Availability SLA is that no problem occurring within the IP Network, the Framework IT CPE or, if provided by Framework IT at the Site, the dedicated access will prevent Client from completing all attempted IP telephone calls for a period that lasts two consecutive hours or more. If Framework IT does not meet this performance objective, Client will be entitled to a VoIP on MIS Site Availability SLA credit equal to 1/30th of Client's total monthly Concurrent Call charges for IP voice channels at the affected Client VoIP Site for each such incident. The VoIP on MIS Site Availability SLA does not apply for MIS with Managed Router installations if the dedicated POTS line is not provided by the Client and if it is determined the outage is related to the Managed Router.

MIS VoIP Call Quality SLA.

The performance objective for the MIS VoIP Call Quality SLA is a VoIP R-Factor Percentage of at least 95%. If Framework IT does not meet this performance objective for a Client VoIP Site in a given calendar month, Client will be eligible for an MIS VoIP Call Quality SLA credit equal to the monthly charges for IP voice channels at the affected Client VoIP Site times 5%, times the number of consecutive months Framework IT does not meet the SLA, up to five months.

"VoIP R-Factor Percentage" is the percentage of qualifying On-Net Calls made from a Client site in the 48 contiguous United States in a given month that meet or exceed an R-Factor of 70. Calls lasting 10 seconds or less are not included when calculating the VoIP R-Factor Percentage.

The VoIP Call Quality SLA only applies to Client sites with access speeds greater than or equal to 128Kbs. Client sites with cascaded router or IP PBX configurations do not qualify for the VoIP Call Quality SLA.

The MIS VoIP Call Quality SLA does not apply for MIS with Managed Router installations if the dedicated POTS line is not provided by the Client and if it is determined the outage is related to the Managed Router.

MIS SERVICE COMPONENTS/CAPABILITIES

MIS Port. An MIS Port provides the connection to the Network. The Port speed is the maximum rate for transmission of data through the Port.

Domain Name System (DNS) Administration. FWC will host Client's IP addresses or domain names for up to 15 primary and/or secondary (the same domain counts as both primary and secondary) DNS zones (15 domain names per circuit or per each NxT1 circuit bundle). If Client establishes its own primary DNS, FWC will host secondary DNS only. Client must pay to the registrar all domain registration fees related to registration and use of domain names. FWC will not host domains that are not owned by Client. Once Client's DNS is established, Client must self-administer its DNS for all existing zones using FWC's web-based DNS Provisioning Tool, which permits Client to view, add, delete or update its DNS records and add new domains. (Client may not use the DNS Provisioning Tool to obtain IP block assignments.) FWC also operates "resolving" or "caching" DNS servers that Client may use for domain name look-ups by Client's in-house systems (PCs, mail servers, etc.) connected to the Service. This domain name look-up service is only available if FWC is providing primary DNS or primary and secondary DNS to Client and if Client does not have its own DNS server(s), and it may not be used by Client's spam detection software for querying spam block lists. For a separate charge, FWC may provide additional DNS Administration in blocks of up to 15 additional primary or secondary DNS zones. Clients may not make more than 500 DNS queries per second. FWC will only provide DNS Administration, including domain name look-ups, directly to Client and not to downstream providers (including Internet Service Providers, Internet Access Providers, Application Service Providers and resellers) or to any third parties given access to Service by Client. Clients running their own DNS Servers or relying on third parties to host their forward domain names must use their or the third party's DNS Servers for this purpose, and those Servers may not be configured to forward DNS queries to FWC DNS Servers. Clients running their own DNS Servers or relying on third Parties to run DNS Servers must ensure that the servers are configured to only answer queries from local, known and/or trusted sources ("Permitted Sources"). If FWC determines that a Client is operating what is commonly known as an Open DNS Resolver or open DNS Proxy which is one that answers queries from sources other than Permitted Sources, FWC reserves the right to block at any time the affected traffic without any notice to the Client. Client will be required to reconfigure the DNS Servers to only answer queries from Permitted Sources.

Additional DNS. Provides Clients with administration of up to 15 additional DNS zones. Clients may select primary DNS or secondary DNS. An additional monthly charge applies. Multiple orders of Additional DNS, for the corresponding monthly charge, are available.

Network Usage Reports. Client will have access to traffic summary reports that track access line utilization as a percentage of the available bandwidth. Daily graphical reports display the inbound and outbound traffic profile in 15-minute increments (except for usage-based circuits, for which 5-minute increments are displayed) and peak and average traffic statistics of the day. Weekly and monthly graphical reports display the inbound and outbound traffic profile, and peak and average traffic statistics, for the selected reporting period.

Network Practices. FWC's underlying carrier engineers its dedicated Internet access services to provide a high-quality Internet experience for its Clients. FWC does not favor certain Internet applications by blocking, throttling or modifying particular protocols, protocol ports, or protocol fields in ways not prescribed by the protocol standards. However, FWC and its carrier(s) proactively monitor the network to guard against a wide range of security threats, including viruses, botnets, worms, SPAM, distributed denial of service attacks and other malicious or harmful activity. In the event a security threat is detected, FWC will typically attempt to isolate that threat and prevent it from spreading across its network or to other networks. We may use a variety of security measures to prevent the spread of a threat, which may include temporarily limiting the flow of traffic over some portions of its network or taking other actions to address the threat. FWC attempts to limit those actions to the specific portions of its network or Client base impacted by the security threat and for only as long as necessary to mitigate the threat.

MIS FEATURES

Class of Service. The Class of Service (CoS) feature enables Client to prioritize traffic among four classes: real-time, high-grade data, medium-grade data, and low-grade data. Each CoS has a specific amount of bandwidth allocation so that all classes can transmit data during congestion. However, if any class does not use its entire bandwidth allocation, packets of other classes can share the unused bandwidth. Client may select from a number of "profiles" that have predetermined bandwidth allocations for each CoS.The CoS feature is required when IP Flex is used with MIS Services. Some restrictions apply with the MIS Access Redundancy Options.

Inbound Mail Relay. Inbound Mail Relay includes use of a hosted Simple Mail Transfer Protocol (SMTP) Internet mail relay server dedicated to routing, and temporarily storing, incoming (to Client's Site) Internet e-mail, if needed. When incoming mail for Users in the Client's domain cannot be delivered to the Client's mail servers designated in the domain MX record, it is redirected to the FWC mail relay server, which will store incoming mail data and will retry and attempt delivery for a maximum of 5 days. Mail data exceeding the 5-day period will be deleted. Mail storage capacity limits apply.

MIS with MPLS Private Network Transport (PNT). With the MPLS PNT feature, FWC segregates Client data traffic transmitted over the FWC IP Network using MPLS to create a network-based IP Virtual Private Network (VPN). FWC segregates Client's PNT traffic from other traffic on the network with separate routing tables in FWC network/provider edge (PE) routers. Unique VPN ID labels are added to Client's data packets as they enter the FWC IP Network and are removed as the data packets reach their destination so that the Client's router may read the data. PNT does not permit access to the Internet, so Clients must order separate MIS ports if they also want Internet access and DNS Administration at an MIS with PNT Site. The MPLS PNT feature is available for use at Sites with Local Channel access (Full/Fractional DS-1, MLPPP 3 Mbps through 12 Mbps, and Full/Fractional DS-3) and Ethernet access from 10 Mbps to 100 Mbps. MPLS PNT Ports using Ethernet access may be configured as a single VLAN or up to ten (10) VLANS. MIS with MPLS PNT is not available with the Dual Stack.

MPLS PNT Service Types

MPLS PNT IP Transport. With MPLS PNT IP Transport, MPLS label stacking starts at the FWC's MPLS-enabled Provider Edge (PE) routers, and MPLS and other enabling technologies are used within the FWC IP Network to join Client's MPLS PNT Sites into a VPN. Client traffic sent between the Client edge (CE) router at the Client Site and the FWC PE router over the local access circuit is not segregated using MPLS labels, but FWC supports static routing or BGP 4 between the CE router and the FWC PE router.

MPLS PNT Label Transport. With MPLS PNT Label Transport, Client CE routers and FWC PE routers are configured for IP static routing and Label Distribution Protocol (LDP) to allow the exchange of MPLS labeled traffic between Client CE router and the FWC PE router over the local access circuit. MPLS label stacking starts at the Client's router, so Client network information associated with Client's end user is not visible to FWC. MPLS PNT Label Transport also enables Clients to offer MPLS VPN capabilities to their end-user Clients.

MPLS PNT Unilink. MPLS PNT Unilink allows Clients to maintain up to one hundred twenty (120) logical channels on an MPLS PNT Port. The aggregate bandwidth of all logical channels may not exceed the bandwidth of the Port. Router limitations may limit the bandwidth of the Port. CoS is not available.

FWC Private Network Transport – FWC VPN Interoperability Feature. FWC Private Network Transport (PNT) - FWC VPN (AVPN) Interoperability Feature ("AVPN Interoperability Feature") allows Client Sites using FWC VPN MPLS VPN and FWC Private Network Transport VPN to be interconnected, and permits communication on an any-to-any basis. The AVPN Interoperability Feature may not be compatible with all FWC VPN features or capabilities, or with all MPLS PNT features or capabilities. Service Components interconnected using the AVPN Interoperability Feature only qualify for SLAs that are expressly applicable to the respective Service. Implementation of the AVPN Interoperability Feature does not change the testing or measurement of performance obligations applicable to or reporting available for a Service Component. For example, and without limiting the forgoing, when Client's FWC VPN and MPLS PNT VPN are interconnected by the AVPN Interoperability Feature, the PNT Port will not be included in the measurement of the FWC VPN MPLS Port-to-MPLS Port Latency and FWC VPN MPLS Port Data Delivery SLAs, and a failure by FWC to meet the performance objective for these SLAs shall not make Client's AVPN Ports eligible for service credits under the PNT SLAs. When making a claim for a service credit, Client must follow the SLA credit request process applicable to the respective Service for which the credit is claimed.

MIS with IP Flex. IP Flex service is available in conjunction with MIS to permit Clients to transmit voice telephone calls in IP format over the FWC IP Network. To be eligible for MIS with IP Flex, Client must order MIS Plus (FWC Managed/Provided CPE) and the CoS feature via the MIS Pricing Schedule.

IP Version Option. Three IP Version options are available with MIS; IPv4 ("IPv4").

Internet Protocol version 4 (IPv4). Internet Protocol version 4 (IPv4) is the current standard communication protocol in place for Internet communication. IPv4 has been the default IP version supported by MIS. IPv4 uses 32-bit (four-byte) addresses, usually written in dot-decimal notation, which consists of the four octets of the address expressed in decimal and separated by periods. (Example: 192.168.255.255).

COVERED ACCESS ARRANGEMENTS AND DUE DATES. The MIS On-Time Provisioning SLA applies to MIS Sites located in the continental United States with respect to Covered Access Arrangements, as defined in the following table, and based on the availability dates provided by the local access provider, which may change at any time and without notice to Client, in which case the SLA start date will be automatically reset to the latest date provided to FWC by the local access provider. The On-Time Provisioning SLA does not apply with respect to any access arrangement ordered for, and/or associated with, any type of Client collocation arrangement on FWC's premises.

Covered Access Arrangement	**Due Date**
Access of any speed that is provisioned as part of a T1 Access Channel, including multiple T1 configurations	30 calendar days after the date when FWC issued CCD to Client
Access of any speed which is provisioned as part of a T3 Access Channel	42 calendar days after the date when FWC issued CCD to Client

SERVICE CREDITS . Service Credits hereunder are calculated as a percentage of the monthly recurring charges ("MRC") and may not be applied to usage charges, government fees, taxes, or surcharges, or any third party charges passed through to Client by FWC. Service Credits hereunder may be paid only once per any given billing cycle. Service Credits issued to Client hereunder shall be Client's sole and exclusive remedy at law or in equity on account of any Network Unavailability and/or failure to meet any objectives or parameters set forth in this SLA. FWC agrees to pass through a credit equal to the credit received by FWC from its underlying FWC(s) for such Network Unavailability, in lieu of the above-stated Service Credits. In no event shall FWC's total liability for any and all interruptions, disruptions, failures, and/or degradations in Service (including, without limitation, any Network Unavailability or failure to meet any objectives or parameters set forth in this Supplement) exceed one hundred percent (100%) of the MRC for the affected Service.

Service Credit Request. Client must submit a written request to claim a Service Credit no later than thirty (30) days following the event which gives rise to Client's right to request the Service Credit. Failure to request an allowance within such period shall constitute a waiver of any claim for a Service Credit.

Multiple Applicable Service Standards. If an incident affects the performance of the Service and results in a period or periods of interruption, disruption, failure or degradation in Service, entitling Client to one or more credits under multiple service level standards, only the single highest credit with respect to that incident will be applied, and Client shall not be entitled to credits under multiple service level standards for the same incident.

Events Excluded From Service Credit. Notwithstanding the foregoing, Client shall not receive any Service Credit for any Network Unavailability, failure to meet any objectives or parameters hereunder, or delay in performing repairs, arising from or caused, in whole or in part, by any of the following events:

a. the conduct of Client or users of MIS Service

b. the failure or deficient performance of power, equipment, services or systems not provided by FWC

c. delay caused or requested by Client

d. service interruptions, deficiencies, degradations or delays due to access lines or CPE when provided by third parties (except as specifically provided in a particular SLA)

e. service interruptions, deficiencies, degradations or delays during any period in which FWC or its agents are not afforded access to the premises where access lines associated with MIS Service are terminated or FWC CPE is located

f. service interruptions, deficiencies, degradations or delays during any period when a Service Component is removed from service for maintenance, replacement, or rearrangement purposes or for the implementation of a Client order

g. Client's election to not release a Service Component for testing and/or repair and to continue using the Service Component

h. force majeure conditions

i. service interruptions or delays in investigating and/or fixing a trouble affecting a non-US Service Component due to the hours of operation of the local access provider in the country for which Client is reporting a trouble

j. service interruptions, deficiencies, degradations or delays during routine network maintenance. Routine maintenance is scheduled between 12 am and 6 am - local time - Monday through Friday.

k. In addition, the SLA does not apply (a) if Client is entitled to other available credits, compensation or remedies for the same service interruption, deficiency, degradation or delay, (b) for service interruptions, deficiencies, degradations or delays not reported by Client to FWC, (c) where Client reports an SLA failure, but FWC does not find any SLA failure, and (d) to sites that are not directly connected to the FWC Network, such as sites connected in a cascaded fashion to a directly connected site.

Use of Alternate Service If Client elects to use another means of communications during the period of interruption, Client must pay the charges for the alternative service used.

SERVICE CALL FEES. Client has the right to request FWC visit Client's premises to attend to service issues. FWC has the right to refuse such request if it deems a site visit is unnecessary. In such an instance, Client may overrule FWC's refusal and demand FWC make a service call. If it is subsequently determined, in FWC's sole discretion, that the service call request was unnecessary and Client's demand was in error, FWC has the right to bill Client for the service call at its hourly rate set forth in the Rate Table.

RELOCATION. If Client moves during the term of this Agreement and would like to relocate the Service, Client shall file a relocation request within FWC forty-five (45) days prior to scheduled relocation. This request must contain at least the requested date of Service termination, the address and phone number of the new location, the prospective move-in date, and the requested transfer of Service date. Relocation does not release Client from its obligations under this Agreement or any SOW. FWC shall use its best efforts to provide Client with the Services in the event Client relocates within the FWC service area but has the sole discretion to refuse to relocate the Service. If FWC is unable or chooses not to provide Service to Client's new location, this Agreement shall terminate and Client shall be responsible for early termination fees.

Limitations. Client acknowledges that Service performance may vary according to geographic location and there is no assurance that Client will receive the same level of Service or pricing with relocation. If Client terminates or moves Service, any service level and price guarantees are void. FWC assumes no liability whatsoever for any claims, damages, losses or expenses arising out of or otherwise relating to the unavailability of the Service in Client's geographical area, for any reason, even where such unavailability occurs after installation of the Service.

Relocation Fee. FWC may charge Client a relocation fee. In addition, in the event relocation or early termination of Service results in FWC incurring fees or penalties from its underlying carrier, such fees or penalties shall be passed on to Client and Client agrees to assume all responsibility for paying such fees or penalties.

DISCLAIMER OF THIRD PARTY ACTIONS. At times, actions or inactions caused by third parties (e.g. denial of service attacks) can produce situations in which Client connections to the Internet (or portions thereof) may be impaired or disrupted. FWC cannot guarantee that such situations will not occur, and accordingly FWC disclaims any and all liability resulting from or related to such events. In the event that Client's use of the Service or such third parties is causing harm to the Network or its operations, FWC shall have the right to suspend the Service. FWC shall restore the Service at such time as it reasonably deems that there is no further harm or threat to the FWC network or its operations.

MAINTENANCE AND MODIFICATIONS TO SERVICE. FWC may at any time and without liability modify, expand, improve, maintain, or repair the FWC network even if such activity might result in temporary suspension(s) of the operation of the Service. FWC will use commercially reasonable efforts to minimize any disruption to the Service to Client and shall use its best efforts to give Client commercially reasonable notice of a maintenance period prior to the disruption by telephone (real-time or voicemail), facsimile, or e-mail. Credits will not be issued with respect to such Service interruptions if FWC has used commercially reasonable efforts to so notify Client in accordance with this paragraph.

NIST 2.0 Framework Assessment Service

Our NIST 2.0 Framework Assessment Service aligns with the NIST Cybersecurity Framework (CSF) 2.0, which provides guidance to manage cybersecurity risks. Following the CSF's core functions of **GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, AND RECOVER** (each, a "Function"), the Assessment is designed to probe and disclose deficiencies in an organization's cybersecurity processes so they can be corrected. **Please note: This is a diagnostic and assessment service only, and unless additional services are purchased (such as those required for the PROTECT, DETECT, RESPOND, AND RECOVER Functions described below), this service will be limited to assessing and notifying you of cybersecurity-related deficiencies discovered in your managed IT environment**.

- **GOVERN**. In this Function, Client's cybersecurity risk management strategies, expectations, and policies will be examined and evaluated for effectiveness. The GOVERN function addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.
- **IDENTIFY**. In this Function, Client's current cybersecurity risks are identified and examined, which enables Client to prioritize its efforts consistent with its risk management and cybersecurity strategies identified under GOVERN. This stage also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.
- **PROTECT.** (*If purchased*): Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function may include identity management, authentication, and access control; awareness and training; data security; platform security *(i.e.*, securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure. **Areas that are identified as needing protection will be discussed with you; however, depending on the areas identified, remediation services related to the PROTECT Function will require a separate Quote or an amendment to an existing Quote to implement.**
- **DETECT.** (*If purchased*): Possible cybersecurity attacks and compromises are found and analyzed. DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities. **Please note: To implement the DETECT Function Client must purchase our security operations center (SOC) services.**
- RESPOND. (If purchased): Actions regarding a detected cybersecurity incident are taken. RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication. **Please note: RESPOND-related services must be purchased separately.**

- RECOVER. (If purchased): Assets and operations affected by a cybersecurity incident are restored. RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts. **Please note: RECOVER-related services must be purchased separately.**