Uptime Manage Service Agreement

2026v3 | Last updated: Oct 2026

This Uptime Manage Service Agreement ("Uptime Manage SLA") is incorporated into and subject to the Master Service Agreement (the "Agreement") between Uptime and the undersigned Client ("Client") (collectively, the "Parties" or individually, a "Party"). If Client's Agreement is with Uptime Systems, LLC, then "Uptime" refers to Uptime Systems, LLC, a limited liability company organized in the state of Minnesota; or if Client's Agreement is with Uptime Systems Canada, ULC, then "Uptime" refers to Uptime Systems Canada, ULC, an unlimited liability company incorporated in Alberta, Canada, and registered in Ontario, Canada. This Uptime Manage SLA is effective and binding as of the date a signed copy from Client is returned to Uptime, without any changes hereto, or upon the continued use of the Services following notice by Uptime of any changes to this Uptime Manage SLA. This Uptime Manage SLA and the corresponding Agreement contain the terms and conditions that govern the relationship between the Parties, and may only be amended as provided for in the Agreement. If there is any conflict between this Uptime Manage SLA and the Agreement, the terms of the Agreement shall control. The Parties hereby mutually agree to be bound by the following terms and conditions.

1. **Description of Services.** Uptime Manage is an MSP service including hosted business solutions, remote IT monitoring, and IT support ("MSP Services"). Client may use MSP Services for any legal purpose.

2. **Charges.**
   a. Unless otherwise specified in writing and agreed by Uptime, billing will commence once the MSP Services are setup and ready for Client's use, and/or data migration into Uptime's services begins, whichever occurs first. The current fees and expenses for MSP Services related to this Uptime Manage SLA are located in Client's Plan Documentation. The fees and expenses outlined in Client's Plan Documentation are subject to change if Client's migration to Uptime Manage does not start (data is not transferred to Uptime) within 6 months of the effective date of this Uptime Manage SLA.
   b. Users, computers, mailboxes, and storage (mailbox size, OneDrive, SharePoint) are subject to the Variable Storage, Usage, & Users Section (5.2) of the Master Service Agreement and will automatically increase to match usage.
   c. Some licensing is billed monthly but requires an annual commitment. Such licensing includes but is not limited to Microsoft CoPilot, and will be indicated as annual licensing on Client's Plan Document. Client is responsible for licensing fees through the licensing term, regardless of Client's overall Uptime Services term. Any remaining annual licensing at time of service cancellation will be immediately due and payable to Uptime.
   d. If Client has annual licensing assigned to their Microsoft tenant when starting MSP Services with Uptime, Client will be responsible for paying for this licensing through the end of the

licensing term. This licensing will be charged by Uptime to Client and will be separate from and in addition to any licensing or services included with the Uptime MSP Services.

3. **Software Licensing & Third-Party Software.** Client acknowledges that its use of software from Third-Party Vendors including, but not limited to, Microsoft, Clio, and LEAP, and other Third-Party Vendors (collectively, "Third-Party Vendors"), regardless of whether the software was obtained by or with the assistance of Uptime, is subject to the terms and conditions established by the Third-Party Vendor. Client hereby agrees to be bound by, and comply with, those terms and conditions as applicable.

   Software from Third-Party Vendors, regardless of whether obtained by or with the assistance of Uptime, does not include any warranties as between Uptime and Client. UPTIME EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO SOFTWARE FROM THIRD-PARTY VENDORS INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ACCURACY. Uptime makes no representations to Client with respect to any software from Third-Party Vendors including, but not limited to, that the software will meet Client's requirements, will be error-free, will be free from defects, or that any issues with the software will be corrected by Uptime. Client agrees that Uptime is not responsible for nor liable for the operation, performance, or content of any Third-Party Vendor software, or any deficiencies with respect thereto including, but not limited to, downtime, degraded performance, loss of Client's access to the software, loss of Client content or Data, or any other deficiencies or defects. Client acknowledges that the terms, limitations, and disclaimers herein also apply to software from Third-Party Vendors that Uptime may select and use for purposes of providing certain MSP Services to Client. Client agrees that its sole and exclusive claims and/or remedies, if any, for any and all issues involving, or that result from, software from a Third-Party Vendor will be against the Third-Party Vendor pursuant to its terms and conditions, and that Client does not have, or has otherwise waived, any and all claims and/or remedies against Uptime, including any and all claims and/or remedies involving, or that result from, Uptime's selection and use of software from Third-Party Vendors for purposes of providing certain MSP Services to Client. Uptime is not responsible for nor will it assist with any defects, problems, or other issues involving software from Third-Party Vendors.

4. **Microsoft Customer Agreement (MCA)**. As part of the MSP Services, Uptime will provision Microsoft 365 licensing for Client under the terms of the Agreement, this Uptime Manage SLA, and Microsoft's MCA. **Client agrees to Microsoft's Customer Agreement (MCA) and authorizes Uptime to agree to the MCA on Client's behalf when provisioning or otherwise managing Microsoft licensing for Client.** Microsoft's MCA can be viewed at https://www.microsoft.com/licensing/docs/customeragreement.

5. **Uptime Intellectual Property.** Client acknowledges that the Uptime Manage Platform and all components associated with the Uptime Manage Platform are the sole and exclusive intellectual property of Uptime. All intellectual property rights associated with the Uptime Manage Platform, including any patent, copyright, trademark, or trade secrets, are and shall remain the intellectual property of Uptime as between Uptime and Client. Client shall be permitted a limited right and license to use the Uptime Manage Platform and intellectual property only as necessary for Client's internal business purposes in connection with use of the MSP Services pursuant to this Uptime Manage SLA.

6. **Ownership of Data.**
   a. Client retains sole ownership of all content and Data that Client imports to Uptime's MSP Services and stores and/or backs up using Uptime's MSP Services ("Data"). Client acknowledges that Uptime does not own or control the software that will ultimately hold Client's Data, and thus the treatment and storage of Client's Data is subject to the terms and conditions of the applicable Third-Party Vendor.

      As between Uptime and Client, the individual person entering into the Agreement, or other agreement as may be applicable, on behalf of Client shall be considered the "Client" for purposes of the ownership of Data and making decisions regarding the treatment of Data, unless that individual provides Uptime with written authorization designating a different individual person as the representative of Client for purposes of ownership of Data and making decisions regarding the treatment of Data, specifically via Uptime's Master Service Form. If the individual person who entered into this Agreement, or other agreement as may be applicable, is no longer associated with Client, and a successor representative has not been designated as set forth above, or if Uptime otherwise cannot identify the appropriate representative after reasonable inquiry, Client agrees that Uptime may, in Uptime's sole discretion, determine which individual shall be considered the representative of Client for purposes of the ownership of Data and making decisions regarding the treatment of Data.

   b. Uptime owns or controls the management accounts, licenses (including Microsoft licenses), and platform(s) to facilitate MSP Services on behalf of Client. These accounts, licenses, and platforms are non-transferrable to Client.

7. **Data Sovereignty.** Data Sovereignty is defined in Client's Plan Document.

   If the Plan Document identifies Data Sovereignty in the United States, then the Microsoft 365 Tenant and primary backups will be located in the United States. "Cloud File Server" storage, an optional add-on, data will be saved and all backups located in the United States.

   If the Plan Document identifies Data Sovereignty in Canada, then the Microsoft 365 Tenant and

primary backups will be located in Canada. "Cloud File Server" storage, an optional add-on, has primary data saved in Canada while backups are saved in the United States. Data is not stored outside of Canada and the United States.

8. **Backup Systems & Data Retention**. The standard backup for Microsoft 365 is Microsoft's native feature. The MSP Services Availability Section of Microsoft's Service Agreement (as of August 13, 2021):

> "We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you have stored. **We recommend that you regularly backup Your Content and Data** that you store on the Services or store using Third-Party Apps and Services." [emphasis added]

Uptime Manage includes an *additional (third-party) backup* to 1) meet Microsoft's recommendation of an additional, regular backup, and 2) to close common Microsoft 365 data protection gaps. All Microsoft 365 data and files (Email, OneDrive, SharePoint, Teams, Groups, Calendars, Tasks) will be backed up a minimum of once per day. See additional backup details below, based on your service package.

No backup system is without faults, flaws, or problems such as a missed file or failed backup during one of the scheduled backup jobs. Uptime will use commercially reasonable efforts to maintain the additional backup of Microsoft 365 files through a third-party software backup service (and subject to the Third-Party Backup section of this Agreement). Client acknowledges that Uptime cannot guarantee the integrity of each individual day or increment of the backup file.

9. **Help Desk Hours.** Uptime's Normal Help Desk Hours and Emergency Help Desk Hours are posted at www.uptimelegal.com/service-hours. During Emergency Help Desk Hours, Uptime support staff are available on an on-call basis. To receive Support Services during Emergency Help Desk Hours, Client must request Support Services via phone and voicemail. Uptime will not respond to email or online requests during Emergency Help Desk Hours. All requests for Support Services during Emergency Help Desk Hours, including Support Services scheduled in advance but that occur during Emergency Help Desk Hours, will be subject to Uptime's Extended Service Fees. Extended Service Fees are subject to change without notice and are posted at www.uptimelegal.com/extended-service-fees. Uptime reserves the right, in its sole discretion, to determine whether Client's request is subject to Uptime's After Hours Support or Uptime's After Hours Project/Weekend Project rates. During No Help Desk Hours, Uptime staff is unavailable to provide Support Services. If Client calls during No Help Desk Hours, Client may leave a voicemail,

and Uptime will call Client back as soon as reasonably possible during Uptime's Normal Help Desk Hours.

10. **Covered Services.** Uptime agrees to provide the covered Services outlined below as part of this Uptime Manage SLA (based on the service options selected in the Plan Documentation). Some covered Services will incur additional or extended service fees (see uptimelegal.com/extended-service-fees for additional information).

    All covered Services are provided via remote support only, onsite (boots on the ground) service is available for an additional fee. Uptime may, in its sole discretion, deem that a task is outside the scope of standard covered Service and may quote the task as a fixed-fee project.

    a. **User Support Policy**
    With regard to covered support and services, Uptime will only assist and support users identified in the Master Service Form as Owners or Admins, or who have a named user account in Uptime's services (Microsoft 365 account).
    b. Covered Service(s) (based on elections in your Plan Document):

Included Elements, Support Scope & Covered Services by Service Level	**Starter**	**Core**	**Advanced**
Microsoft 365 Licensing	Business Standard	Business Premium	Business Premium
OneDrive/SharePoint: Uptime will support permissions on top-level folders. Nuanced permissions on subfolders or individual files are not recommended and unsupported by Uptime. Clients requiring permissions to manage subfolder permission waive Uptime's support of top-level permissions. For a fee, Uptime can repair or restore top-level permissions. Assist with restoration of deleted items (may incur an Extended Service Fee) Restore or assist with deleted webparts	✔	✔	✔
Email Support: Add/Remove users, including adding to distribution groups. Add/Remove email aliases. Creation of distribution groups (outside of initial onboarding, this will incur an Extended Service Fee). Add additional domain(s) (outside of initial onboarding this may incur an additional or Extended Service Fee). External Email Tagging - emails from outside your domain will be tagged as "External". Support (installation, basic troubleshooting) of Outlook add-ins and Exchange integrations (i.e. Groupware) User Mailboxes are limited to 50GB, with an archive mailbox capacity of 50GB. User Mailbox capacity can be expanded to 100GB with unlimited archive mailbox capacity (for additional fee – see Expand User 365 License to 100GB Capacity add-on option). Mailbox size, and plan fees, will be adjusted by Uptime as necessary. Exchange server-side support (excluding extended services) Support Public Folder creation, permissions, email send-to-folder. Public Folders are limited to 25 GB	✔	✔	✔

per folder, with a total size for all public folders 100 GB. This capacity cannot be extended and exceeding these limits will cause performance issues and possible data loss			
Teams Support: Support (installation, basic support) of Microsoft integrations (i.e. OneNote, SharePoint, OneDrive). Creation of groups and channels.	✔	✔	✔
Entra ID Basic setup and join computers to domain for ease of access Self-service password changes SSO support. Uptime work with vendors/apps to configure SSO where available.		✔	✔
Intune MDM & conditional access (details in Security & Compliance section (below))		✔	✔
Setup of Microsoft 365 email and apps on mobile devices	✔	✔	✔
Training for all included Microsoft 365 services	✔	✔	✔

Local Computers, Printers & Network

Computer Requirements for Supported Computers <u>Starter:</u> Company-owned computers with an Operating Systems that is within vendor support. Windows Home licenses are not recommended but will I be supported at this service level. <u>Core & Advanced:</u> Company-owned computers with an Operating Systems that is within vendor support. Windows Home licenses are not supported in these service levels to align to best practices and additional security elements included in selected service Level. Uptime's ability to provide support will be limited if the device(s) does not have an active support contract. Windows operating system is required to take advantage of the full security suite. MacOS is supported with limitations.			
Computer Support (support limited to computers with Uptime's monitoring agent installed) Installation and monitoring of local RMM agent (supplied / supported by Uptime). Hardware monitoring and support for hardware under warranty. Monitoring of computer disk space and working with users to resolve low-disk space alerts. Monitoring of critical services including Windows Updates and Windows Firewall. Working with Client to resolve any issues to the operation of these services. Support includes troubleshooting to determine issue and best effort to resolve the issue.	✔	✔	✔
Support for *unmanaged* computers (computers without Uptime's monitoring agent) – i.e. BOYD or personal (non-Company) computers. BYOD or personal computers are not recommended as they require exceptions to conditional access policies among other security settings and they don't have Uptime's monitoring agent or security stack (antivirus and MDR). You're only as secure as your weakest link, and unmanaged computers will become your weakest link. Starter and Core plans: personal computers can be used if the Firm Owner or Account Admin approves the exception to the conditional access policy. Support is limited to getting the user logged into Office.com for Company email, OneDrive, and SharePoint access and work. Advanced plans: Personal computers are not allowed due to security compliance requirements of this service level	*	*	

Uptime to work with hardware vendor (for HP, Lenovo, and Dell equipment with Pro or Enterprise warranty)		✓	✓
Reformatting computers	*	✓	✓
Purchase Advisory – as requested Including providing Client recommendations on PC's, software, devices, ISPs, and other devices and services All Packages: Purchase Advisory included on as-needed, ad-hoc basis.	✓	✓	✓
Purchase Advisory – proactive Core and Advanced Packages will also receive proactive purchase recommendations based on Client's upcoming equipment lifecycles and Client goals.		✓	✓
Operating System Patch Management (Windows devices only)	✓	✓	✓
Operating System Upgrades		✓	✓
Computer Refresh & New Computer Setup Consulting, advisement, and recommendations on new computer via Client's assigned IT Manager is included with Core and Advanced Packages. Incremental computer setups, including new computers associated with a new user (added to Plan) is included. A material number of new computers or computer setups are subject to project fees.	*	✓	✓
Network Equipment Requirements for Supported Network – Supported Network equipment stacks Firewalls: WatchGuard and Ubiquity Access Points: WatchGuard and Ubiquity Switches: Ubiquity, Aruba Support is limited to devices with an active vendor support contract. Ubiquity devices must be joined to Uptime's Ubiquity controller for support Uptime's ability to provide support will be limited if the device(s) does not have an active support contract.			
Network Support Monitoring: Network availability and general performance information Patching: WatchGuard and Ubiquity devices (with active support contracts) will be patched by Uptime on a semi-annual basis, unless an emergency or critical patch is released, in which case Uptime will work with the Client to patch the equipment as soon as practically possible Support - WatchGuard & Aruba: Uptime will troubleshoot and work with vendor (with active support contracts) Firewall Configuration Management: support limited to supporting configurations and policies that are already in-place (after initial onboarding to Uptime). Changing configurations or policies (such as implementing web-blocking) is a project and subject to project fees.	✓	✓	✓
Network Refresh Consulting, advisement, and recommendations on updated networking equipment and setup via Client's assigned IT Manager is included with Core and Advanced Packages. Any resulting project is an additional fee and limited to Uptime's supported equipment.	*	✓	✓

Equipment Life Cycle Management – Reactive Uptime will alert client to renewals or warranty/support expiration of supported computers and network equipment.	✓	✓	✓
Equipment Life Cycle Management – Proactive Client's assigned IT Manager will proactively work with the client on life cycle renewals.		✓	✓
Printer & Scanner Support Devices need to be on vendor-supported firmware. Scan-to-email requires TLS support. Scan-to-folder requires SMB3 on both the printer and the computer. Uptime strongly recommends Clients maintain an active support contract on large multi-function printer/scanner/copiers. Lack of support contract may limit Uptime's ability to troubleshoot or resolve issues.	✓	✓	✓
Serverless Print-from-Anywhere – provided by Uptime Cloud Print Server, Uptime will assist with managing and deploying network based printers. Print anywhere requires a device to be online on the same network as the printer or requires a VPN client on the endpoint.	✓	✓	✓
Onsite IT Support Onsite Support is provided on billable hour basis. All billing will be direct from Uptime to Client and is in addition to Client's monthly Plan Charges Onsite support to be scheduled and confirmed with Uptime's Help Desk 2-hour minimum (not including travel time), plus travel time After 2-hour minimum, hours are billed in 30-minute increments Onsite technician is contracted by Uptime but is not an Uptime employee Availability and timing for onsite support is location dependent; Not available in all locations Any onsite jobs cancelled within 48 hours are billed at the estimated work time.		Available*	

Egnyte Cloud File Server

Egnyte Cloud File Server Alternative to SharePoint for document storage. Similar to a cloud-based Windows File Explorer. Egnyte Cloud Storage is a third-party tool resold and supported by Uptime. In electing Egnyte services, Client is agreeing to Egnyte's terms and conditions found here: www.egnyte.com/MSP-end-customer-tos Egnyte service is an annual commit (paid monthly). The annual renewal date for all Clients is May 10. Billing for users and storage can be increased throughout the annual term but cannot be reduced. Biling reductions must be requested 30-days in advance of the annual renewal. Should the Client cancel services mid-term, the Client must pay through the term before admin credentials or offboarding services will be provided by Uptime. Support includes: All support is provided by Uptime. Client has no direct access to support with Egnyte. Uptime will escalate to Egnyte directly and as needed. Desktop support for currently supported Windows or Mac OS Web Browser support for Chrome or Edge only User creation/deletion, group changes, SSO administration. Permissions management: Uptime will assist Client with best practices and will support group-based permissions for top-level folders. Nuanced permissions on subfolders or individual files are not recommended and unsupported by Uptime. Clients requiring permissions to manage		✓	✓

subfolder permission waive Uptime's support of top-level permissions. For a fee, Uptime can repair or restore top-level permissions. Backup & Recovery: Uptime will assist with file version recovery and global recycling bin restoration (up to 10 files per month, additional recovery may incur fees). Recovery from snapshots or bulk changes and restoration may incur additional fees.			

Application Support & Management

Installation (executables and instructions provided by firm): any app or add-in supported by the computer OS and approved by the firm. Automated / proactive Upgrade, Update: Adobe, Chrome, Edge, Firefox, Office 365, FoxIt,	✔	✔	✔
Automated / proactive Upgrade, Update: any application that can be automated via Uptime's tools. Specific apps to be discussed during initial onboarding discovery and setup.		✔	✔
Software & Apps Provided by Uptime include: How-to Support, Microsoft 365 integration, and Troubleshooting	✔	✔	✔
System Tools provided by Uptime (such as for 365 Account Backups, and Spam Filtering): Uptime will provide training and guidance on how to use system tools to best meet user and Firm needs		✔	✔
Software & Apps Not Provided by Uptime: Customizations, workflows, how-to's are not included (would need an Application Support plan)			

Security & Compliance

Compliant Email Archive & 365 Account Backup All emails into/out of Client's domain will be saved in the compliant archive. Uptime will provide training and grant access to the full archive to users indicated by Client owners. Daily backup of Microsoft 365 accounts (Email, OneDrive, SharePoint, Teams, Groups, Calendars, Tasks) via third-party service provider. Email will be backed-up continuously via journaling. All other items will be backed up a minimum of once per day. Default backup retention period is indefinite but can be modified based on Client compliance needs and at Client's request (reduced to 7-years or 10-years, etc.). Data restoration fees may apply (Extended Service Fee).		✔	✔
365 Account Backup Restoration Starter: Client has no direct access to backups. backup restoration subject to Extended Service Fees Core: Client can access the Compliant Archive. Users identified by client as Admin can search across all users' 365 Accounts. Users can restore files without Uptime's assistance at no additional cost. Requesting Uptime's assistance in restoring files is subject to Extended Service Fees. Advanced: Same as Core Package except that Uptime's assistance is at no additional cost.	*	✔*	✔
Antivirus & MDR Installation and monitoring of local Antivirus and MDR (managed detection & response) software (supplied / supported by Uptime) Uptime's scope is limited to virus remediation. Uptime does not conduct digital forensic evaluations or malware analysis (i.e. Uptime cannot confirm whether data was compromised or exfiltrated).	✔	✔	✔

Cases of confirmed compromise/breach should be evaluated by client's insurance carrier for additional guidance on remediation and/or evaluation (whether forensic evaluation is needed).			
Data restoration and/or computer reformatting. Engagement with 3rd Party Auditors or Insurance Carriers (due to virus or related issue) Starter: Not included. Available as an Extended Service. Core: Up to .5 hours / user (per year) is included. Hours beyond this are billable. Advanced: Up to 1 hour / user (per year) is included. Hours beyond this are billable.	*	✔*	✔*
Upgrade local antivirus to include Windows Defender Premium		✔	✔
Identity Threat Detention Response (ITDR) for Microsoft 365 Analyze and detect malicious logins to Microsoft 365 account, such as an email account compromise (Sometimes referred to as BEC - business email compromise). If compromise is detected the user account is isolated and remediation plan is enacted. The ITDR/EDR agent will monitor and protect 365 accounts 24/7 - based on the severity of the alert, a user's 365 account could be suspended until the alert is reviewed and remediated by Uptime's security and support team Uptime will act on alerts during Uptime's standard help desk hours.	✔	✔	✔
Third-Party (non-Microsoft 365) Spam Filtering, Spam filtering, phishing filtering, anti-spam, known malware prevention, reputation-based URL protection, scanning of OneDrive and Teams as well. Does not include URL sandboxing Basic spam filtering and support including whitelisting/blacklisting domains.	✔	✔	✔
Malware sandboxing (email protection) Malware sandboxing, file sanitization (removes suspected malicious code from attachments), URL sandboxing, Support includes configuring file sanitation per Client's needs, whitelisting/blacklisting domains.		✔	✔
Email Encryption Data loss prevention: can be configured to force encryption or prevent sending emails when including certain things such as SSN or credit card number). Uptime will assist client in configuring or modifying encryption triggers and/or policy-based encryption triggers. Uptime will provide user training and how-to support.		*	✔
Conditional Access (via Intune) (Mobile Device Management) Uptime will work with client to define conditional access policies. Only Windows devices are supported at this time. Core: Conditional Access policies can be bypassed with a signed waiver. Advanced: This package is intended to put security first and foremost and therefore no exceptions to conditional access policies are allowed.		✔	✔
SASE (Secure Access Server Edge) with always on-VPN and zero trust networking. Uptime will provide consultation and support on implementation. Device must be company owned to access the agent. Supported devices include Windows, Mac OS, or Android. Windows with ARM processors are not supported. Available as an add-on to Core and Advanced Packages		*	*

Managed SIEM (Security Information & Event Management) Uptime will ingest logs from Windows Devices and WatchGuard firewalls. Uptime will provide best effort support setting up third party applications that have SIEM support. Uptime will provide an on-premise device to gather logs.			✔
Managed Security Awareness Training & Phishing Simulation Available as an add-on. Security is only as strong as the weakest link. For Security Awareness Training to be meaningful, it must be provided to all members of your firm. Uptime's Security Awareness training is enabled on a firm-level and applies to all Uptime Manage users. Can add additional users above and beyond Uptime Manager users as well. Options Uptime will work with you to enable: Training can be monthly or quarterly. A custom cadence can be evaluated as well (additional fees may apply for the setup and configuration of custom cadence). Training can be automatically assigned post-security incident (if there is an email compromise, the compromised user will automatically receive additional training) Phishing Simulation is monthly. Additional Phishing training can be automated if a user interacts with a phishing threat. Automated reminders will be send to end-users. Uptime will work with Client to determine who at the firm will receive training completion and compliance reports, and have access to the dashboard to see completion rates. Uptime enables and manages the training and tech, Client is responsible for end-user completion and compliance.	*	*	*
Auto-elevate Uptime will provide support for creating rules and approving one off requests for tasks requiring admin privilege's. Requires Windows 10 or newer.		✔	✔
DNS Protection Actively monitor DNS traffic for malicious websites, provides content filtering and adblocking. Uptime will assist/advise on tailoring this application to the Firm's needs. Uptime will monitor local devices to ensure installation. Supported devices: Windows and MacOS. Supported web browsers: Edge, Firefox, Chrome, Brave, Vivaldi browsers		✔	✔
Secure Web Browsing Actively monitor DNS traffic for malicious websites, provides content filtering, adblocking, remote browser isolation for high risk or unknown websites, and credential filtering. Uptime will assist/advise on tailoring this application to the Firm's needs. Uptime will monitor local devices to ensure installation. Supported devices: Windows and MacOS. Supported web browsers: Edge, Firefox, Chrome, Brave, Vivaldi browsers			✔
DMARC Publish DMARC record and ingest reports to provide customer with insights into mail deliverability. Will consult on ensuring DKIM/SPF alignment for outbound mail servers and configure DMARC with a reject policy to improve deliverability.	*	*	✔

Vulnerability Management Continuous vulnerability monitoring of Windows and Mac devices. Weekly scans of supported networking equipment. Vulnerabilities are addressed alongside device patching Windows. Only Windows devices are currently supported.			✔
Security, Compliance, and Insurance Questionnaires or Assessments Basis: Limited to 2 hours annually. Hours beyond this are billable. Includes a general review of the assessment, advisement on which technology measures are met, and advisement on services needed to meet the assessment's requirements. Core: Up to 5 hours annually. Hours beyond this are billable. Includes reviewing the assessment, advisement on which technology measures are met, setup automations for reporting based on future needs (such as automated inventory updates) as outlined in the assessment (if any), and advisement on needed to meet the assessment's requirements. Advanced: Up to 10 hours annually. Hours beyond this are billable. Includes reviewing the assessment, advisement on which technology measures are met, setup automations for reporting based on future needs (such as automated inventory updates) as outlined in the assessment (if any), and advisement on needed to meet the assessment's requirements. Also includes compiling documentation or evidence to support the answers provided or as required by the assessment. Uptime reserves the right to not answer all questions or to withhold certain information it deems confidential. Uptime cannot create client policies or policy documentation. Uptime cannot conduct pen testing though can work with client's vendor at client's request. Uptime can work with client's cyber security vendor to run 3rd party scans (outside of the tools Uptime Manage already includes). Uptime will also provide documentation to aid Client in answering security questionnaires.	✔*	✔*	✔*

General Support & Projects

IT Manager Core and Advanced: include an assigned IT Manager. Client's assigned IT Manager will be the lead IT Engineer regarding Client's Uptime Services. They will maintain documentation of Client's setup, configuration, and processes related to Client's Uptime Services. The IT Manager will provide consulting and advisement on any significant change to Client's Services, network configuration or settings, or other IT projects. IT Managers will proactively review Client's services and support history on a quarterly basis to ensure consistency and advise on any issues or suggested changes. IT Managers will meet with Client's annually to review service and support history, upcoming Firm changes and technology goals, and create a technology roadmap for the coming year. IT Manager will review the roadmap during their quarterly account reviews to align their recommendations.		✔	✔
Office Move / New Office Location Consulting and advisement to roadmap the technology aspects of an office move project, as well as the actual work of an office move project (technology aspects only) are available as an Extended Service Fee.	*	*	*
Add / Remove users Incremental user additions or removals from the Service Plan are included.	✔*	✔*	✔*

Material user adds/removes are subject to project fees and Section 5.8 (Changes) of the Master Service Agreement.			
**Firm Growth	Acquisition/Merge** Data import / migration after the initial onboarding is subject to project fees. Additional material users or office locations (see sections above).	*	*	*

*Included as an Extended Service or package add-on, subject to Extended Service Fees or additional monthly service fees.

Uptime WatchGuard Firewall & Access Point Rental Service

Through the WatchGuard Rental Program, Uptime will provide the initial physical device(s) and licensing (such as firewall live security). Support for firewall and access points is covered separately under the Network Support section of this Manage SLA.

Physical Device Terms:

- WatchGuard hardware, firmware, software, security services, warranties, replacements, and related vendor services are subject to availability and the applicable terms and service levels provided by WatchGuard. Uptime does not separately warrant WatchGuard products or guarantee WatchGuard's replacement, update, repair, support, or service timelines. Temporary hardware failure, warranty replacement, vendor support activity, software or firmware issues, or other WatchGuard product issues do not suspend or eliminate Client's recurring service charges.
- Licensing/hardware are non-transferable.
- Client is responsible for disposing of devices upon termination of services or change of firewall.

Uptime Phone (VoIP) Support Service Plan

Available for clients with Intermedia Elevate VoIP Plans Only

VoIP Service is provided and billed direct from Intermedia. Uptime is not responsible for phone service (including availability, reliability, and third-party vendor billing and fees). All terms, conditions, restrictions and fair use policies of the VoIP vendor apply. Uptime's Phone Support Plan provides a managed VoIP experience where Uptime will aid your firm in provisioning new users, new handsets (physical phones), making changes to call routing and other phone system features, and day-to-day support of the VoIP service. Uptime's support requires administrative access to the Intermedia account. In the event Client removes or reduces Uptime's access, Uptime's support may be limited.

E911: Uptime will assist with the initial setup of E911 location services. Client is responsible for ensuring E911 location is setup accurately and updated. E911 can be updated from the softphone or via a tick to Uptime support.

Covered Phone Support Services:

- User creation/provisioning and removal
  - Account downgrades (removing users, phone numbers, etc) may take 2-3 business days to full process. Uptime is not responsible for VoIP vendor billing or when billing changes are reflected.
- Device provisioning (soft phones and desk phones / handsets). Physical phones or conference room phones must be supported by VoIP vendor in order for Uptime to provide support.
- Number porting coordination. Uptime cannot guarantee numbers are portable. Client may need to assist if porting needs additional information or is rejected.
  - Number porting outside of initial onboarding will incur an Extended Service Fee.
- VoIP tenant management including user configuration, auto-attendant and hunt group provisioning and changes, call routing provisioning and changes.

- Significant or bulk changes, such as reconfiguring the entire auto-attendant, increasing users by 20% or more, or updating all physical phones, are subject to additional fees.
- Uptime will assist in uploading recordings for auto-attendant or other features. Client is responsible for generating the actual voice recording. Uptime will make referrals to third-party options including AI options at client's request.
- SSO configuration
- Uptime will escalate support issue to the VoIP vendor and manage communications and troubleshooting. Client end-users may still be required to assist with troubleshooting efforts.
- Performance (handsets, call quality) on Uptime Managed Devices on an Uptime Managed Network.
- Uptime will configure and support Intermedia's Microsoft Teams phone integration.
- Fair Use Policy: Uptime will provide support up to a maximum of 2 hours + 15 minutes per user, per month. Support in excess of this is subject to account review and additional fees.
- Client owns the VoIP account with the VoIP vendor. Changes to the setup, configuration, or provisioning within the account made independent from Uptime maybe subject to additional Uptime support fees. Uptime will charge time and materials (or an Extended Service Fee) to re-provision services or fix changes and errors made by client, end-users, or other third-parties.

11. Services Not Covered. Services not listed herein as a covered Service will not be provided as part of this Uptime Manage SLA. Services that are not provided include, but are not limited to:

- Local / on-premise server support
- Email delivery / receipt issues from non-clients (Uptime will support email sending/receipt from Client's domain and Microsoft 365 account but cannot work with non-clients to troubleshoot deliver/receipt issues on their end).
- Data Conversion between applications
- Personal / Home networks (routers, wireless devices, etc., not owned and operated by the Client (company))
- Migration away from Uptime's Services, including data copies or exports
- Maintaining Client's Data after Client's account is 40 days past-due
- Any third-party, non-Uptime phone system
- Any operating system or device using an operating system that is not under maintenance or support by its publisher
- Third-Party Services not provided by Uptime (Dropbox, Google Drive, Amazon, etc.)
- Third-Party backup solutions not provided by Uptime (Iron Mountain, Carbonite, etc.)
- Shipping fees outside of migration
- WatchGuard Firewall & AP Rental Service, Services Not Covered:
    - Upgrading or replacing firewalls. Firewall upgrade or replacement may be necessary if the physical device reaches end of vendor support, or depending on firm size and office configuration. Any upgrade or replacement may incur a project or Extended Service Fee.
- Uptime Phone (VoIP) Support Service Plan, Services Not Covered:
    - Intermedia Contact Center service options
    - Uptime will not generate voice recordings
    - Performance issues on unmanaged devices or unmanaged networks, including but not limited to phones that are unsupported by the VoIP vendor, home networks, third-party wifi, and company networks on unsupported or unrecommended configurations.
    - Intermedia outages
    - Outbound Caller-ID issues with third-parties. Outbound Caller-ID will be setup as Client's request. Uptime cannot guarantee downstream carriers will update their systems in a timely manner. Uptime cannot work with third parties or other carriers if the Outbound Caller-ID is displaying different from how it's configured within Intermedia's system.

12. **Termination.** Upon termination (pursuant to the terms outlined in the Agreement), timely request from Client in writing, and payment in-full of Services through the termination date, Uptime can provide the following to Client (considered an extended service):
    - **Microsoft 365 Account:** Client's Microsoft 365 tenant can be released to a different Microsoft Partner. Annual Microsoft licensing may be transferrable to another third-party provider. Subject to Section 10.3 of the Agreement, Uptime will accept and approve the transfer request. Uptime is unable to assist with account transfer issues outside of approving the request.
    - **Network monitoring boxes** (physical devices) deployed or provided by Uptime are owned by Uptime. The device can be transferred to the client upon termination (subject to Extended Service Fee). Client will received a credit of $150 upon Uptime's receipt of the returned device.
    - **Remote Monitoring Agent and Local Antivirus:** These services cannot be released or transferred to Client and the licensing and service is only valid while an Uptime Client. Upon termination, Uptime will deactivate these services. It is possible that Client will need to remove these items from their computer(s).
    - **Other Third-Party Tools & Services:** Other services and their related licensing and tools, including but not limited to: spam filtering / advanced spam filtering, anti-phishing technology, Microsoft 365 backup, compliant email archive, and email encryption, cannot be released or transferred to Client and the licensing and service is only valid while an Uptime Client. Upon termination, Uptime will deactivate these services and any stored data (backups, archive, etc.) will be deleted.

13. **Assignment.** Client may not assign this Uptime Manage SLA without the prior written consent of Uptime. Uptime may assign this Uptime Manage SLA in whole or in part without the prior consent of Client. This Uptime Manage SLA will inure to the benefit of, and be binding upon, the Parties hereto, and their successors and assigns.

Signature

I agree to all terms in the above Uptime Manage SLA and associated Master Service Agreement.

Firm Name ("Client")	
Signed By	
Signature	
Title	
Date	