MyPCFriends Cybersecurity — Services Guide

Version control	
Document	Services Guide (SG)
Document ID	MPF-SG-2026.1
Version	2026.1
Effective date	November 1, 2026
Applies to	Quotes accepted on or after the effective date, including existing clients who accept a new Quote for a Service Plan
Does not apply to	Quotes accepted before the effective date, which remain governed by the version in place when they were accepted (Version 2024.1 or Version 2025.1)
Companion document	Master Services Agreement, Version 2026.1 (MPF-MSA-2026.1)
Owner	MyPCFriends Cybersecurity (Desysca, Inc.)

Version 2026.1. This version applies to every Quote accepted on or after November 1, 2026. Quotes accepted before that date remain governed by the Services Guide that accompanied them, until the Quote expires, is terminated, or is replaced by a new Quote.

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 MyPCFriends Cybersecurity ("MyPCFriends Cybersecurity," "we," "us," or "our"); however, only those services specifically described in the Quote, including the services included in any Service Plan named 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, or included in the Service Plan named 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.

Service Plans

We offer three Service Plans. Each Service Plan is priced per user, per month, and includes everything in the Service Plan before it. The Quote states the Service Plan, the number of users, the term, whether the Microsoft 365 license is included, and any services billed separately.

	Tier 1 – Essential IT & Security	Tier 2 – Advanced Security	Tier 3 – Compliance for Regulated Businesses
Best for	Small offices that need a full IT department without hiring one	Businesses that handle personal or financial data of their customers, including tax, accounting, and insurance offices	Any business subject to a security or privacy law or standard, or asked by its insurer or customers for proof of its security program
Includes	The services listed under Tier 1 below	Everything in Tier 1, plus the services listed under Tier 2 below	Everything in Tier 2, plus the services listed under Tier 3 below

Per-user coverage. Each user covered by a Service Plan includes one (1) named user account and one (1) Business Device (computer) used primarily by that user, as described in "Covered Environment," below. Additional computers, servers, network sites, and other items are billed separately as described in the Quote and in "Rates for Services Billed Separately," below.

Microsoft 365 license. Each Service Plan is offered (a) with a Microsoft 365 Business Premium license included for each covered user, or (b) without the license, in which case we resell the Microsoft 365 Business Premium license to you as a separate line item. Microsoft licenses for covered users are purchased through us; we do not manage users with licenses purchased elsewhere unless the Quote states otherwise. Microsoft licenses are Access Licenses under the MSA.

Tier 1 – Essential IT & Security

- Microsoft 365 management: configuration and administration of your Microsoft 365 tenant, with multifactor authentication enforced for every covered user.
- Microsoft 365 backup: backup of Exchange Online mailboxes, OneDrive, SharePoint, and Teams data.
- Email threat protection: filtering of spam, phishing, impersonation, and email-based malware.
- Endpoint protection: next-generation antivirus with endpoint detection and response (EDR) on each covered computer.
- Updates and patching of the operating system and supported third-party applications.
- DNS filtering to block access to known malicious and unwanted websites.
- Security awareness training: short monthly lessons and a simulated phishing campaign every month, with results by user.
- Remote help desk during business hours, and on-site visits within the Service Area at no additional charge (see "Physical Locations Covered by Services").
- User adds and removes (new and departing employees), subject to the Rule of 3.
- Support for your line-of-business applications on a best-effort basis, and coordination with your technology vendors.
- Remote monitoring and maintenance of covered computers.
- Monthly service report and monthly productivity report (see "Usage and Productivity Reporting").
- Technology review every six (6) months, and an annual equipment replacement plan and technology budget.
- Basic containment of security incidents during business hours. Additional incident response work is billed at the incident response rate.

Tier 2 – Advanced Security

Everything in Tier 1, plus:

- Managed detection and response (MDR): 24x7x365 monitoring of covered computers by a security operations center (SOC), which can isolate a device or stop a threat at any time of day.
- Incident containment included, 24x7, for Security Incidents detected in covered systems, and a written incident summary with the cause and the actions taken (see "Incident Response," below).
- Application control: only approved applications and scripts can run on covered computers.
- Identity threat detection and response (ITDR) for Microsoft 365 accounts, including alerts on suspicious sign-ins and mailbox rules.
- Role-based access, conditional access, and device management through Microsoft Entra ID and Intune.
- Password manager with an individual vault for each covered user.
- Dark web monitoring of your company domain(s).
- Monthly security report, Microsoft 365 adoption by user, unused licenses, and a security score for each employee.
- Access review every three (3) months, a security review meeting every six (6) months, and an annual security report.

Minimum plan for certain businesses. If your business is a "financial institution" under the FTC Standards for Safeguarding Customer Information (16 C.F.R. Part 314), which includes most tax preparers, accountants, and insurance agencies, Tier 2 is the minimum Service Plan we offer, and we recommend Tier 3.

Tier 3 – Compliance for Regulated Businesses

Everything in Tier 2, plus:

- Security information and event management (SIEM): central collection of logs from Microsoft 365, firewalls, and servers covered by the Quote, monitored 24x7x365 and retained for fourteen (14) months unless the Quote states a different period.

- A managed compliance program for the law(s) or standard(s) named in the Quote (each, an "Applicable Framework"), as described in "Managed Compliance Program," below. Applicable Frameworks may include the FTC Safeguards Rule (including the written information security plan expected by the IRS for tax professionals), the HIPAA Security Rule, PCI DSS for the systems we manage, state insurance data security laws, and the written security requirements of your cyber insurance policy. CMMC Level 2 and other certification programs are not included and are quoted as Projects.
- Designated Security Role: we serve in or support the security role required by the Applicable Framework, such as the Qualified Individual under the FTC Safeguards Rule or the security official under HIPAA, as described in the MSA.
- Written risk assessment, written information security program (WISP), and written policies (including an acceptable use policy for artificial intelligence tools), delivered within sixty (60) days after the Commencement Date and updated each year, aligned with the NIST Cybersecurity Framework 2.0.
- Internal and external vulnerability scans every six (6) months, with a report and a remediation plan.
- Written incident response plan and one (1) tabletop exercise per year.
- Virtual Chief Information Security Officer (vCISO) meeting with your leadership every three (3) months, with a one-page dashboard of productivity, risk, and compliance.
- Annual written report to your governing body or senior officer on the status of your security program.
- Audit evidence collection and support with cyber insurance and customer security questionnaires.
- Incident investigation using SIEM logs, an incident record for compliance purposes, and assistance preparing the regulatory notifications that your Applicable Framework requires. You remain responsible for deciding whether, and for making, any notification.

Penetration testing is not included in any Service Plan and is available as a separately billed service.

Cyber insurance. Tier 3 requires you to maintain cyber liability insurance as described in the "Client Insurance" paragraph of the MSA. For Tier 1 and Tier 2, cyber liability insurance is strongly recommended.

Service Plan Deliverables

Each Service Plan delivers the items below, in addition to everything in the Service Plan before it.

When	Tier 1	Tier 2 (adds)	Tier 3 (adds)
First 30 days	Inventory of devices, users, and licenses; software agents installed; Microsoft 365 secured with MFA; documentation of the Environment; list of risks found (for example, unsupported operating systems); training and first phishing simulation started; productivity baseline	MDR, application control, ITDR, and password manager active; password vault for each user; baseline of Microsoft 365 adoption and licenses	SIEM connected; Applicable Framework(s) confirmed; written risk assessment; first vulnerability scan; written designation of the Designated Security Role; WISP and policies within 60 days
Every month	Service report (tickets, response times, patches, protection status, verified backups, devices not checking in); simulated phishing campaign, with training and phishing results; productivity report (time lost per person, slow or failing devices, repeat issues)	Security report (SOC alerts and actions, suspicious sign-ins, dark web findings, application approvals); Microsoft 365 adoption by user; unused licenses; security score by employee	Compliance report (status of controls under the Applicable Framework, SIEM events reviewed, evidence recorded, open items)
Every 3 months	—	Access review (who has access to what)	vCISO meeting and one-page leadership dashboard
Every 6 months	Technology review (30 minutes): devices to replace, warranties, and licenses	Security review meeting	Internal and external vulnerability scans with report and remediation plan
Every year	Equipment replacement plan and technology budget	Annual security report	WISP and risk assessment update; written report to

When	Tier 1	Tier 2 (adds)	Tier 3 (adds)
			leadership; incident response tabletop exercise; letter describing your security program for your insurer
When an incident occurs	Basic containment during business hours; further work billed at the incident response rate	24x7 containment included; written incident summary	Investigation with SIEM logs; incident record; assistance with notifications required by the Applicable Framework

Deliverables that depend on your participation (for example, meetings, attestations, or information we request) are considered delivered when we offer them on a reasonable schedule, even if you decline or do not respond. Reports may be delivered through a portal or by email.

Changing Your Service Plan

You may move to a higher Service Plan at any time; the new price starts on the next billing cycle. You may move to a lower Service Plan only at the end of the then-current term, unless we agree otherwise in writing. Moving to a different Service Plan requires a new or amended Quote. If we recommend a higher Service Plan because of a law or standard that applies to your business and you choose not to follow that recommendation, you accept the risks of that decision, as described in the "Advice; Instructions" paragraph of the MSA.

Projects: The Rule of 3

Support requests are included in your Service Plan. A request is a **Project** when it meets any one of these three conditions:

1. **3 or more computers:** the work touches three (3) or more devices.
2. **3 or more users:** the work affects three (3) or more users.
3. **3 or more hours:** the work is expected to take three (3) hours or more.

Projects are out of scope of the Service Plan. They are billed at the project rate, with a one (1) hour minimum, or at a fixed price based on a written scope. We will give you a Quote or a written estimate (email is sufficient) before any Project starts, and Project work starts only after you approve it. Examples:

Request	Project?	Why
Install a printer on 2 computers	No	2 devices, less than 3 hours
Install a new program on 5 computers	Yes	5 devices
Add 1 new employee	No	1 user
Add 4 employees for a new branch	Yes	4 users
Set up 1 new computer	Billed per computer	New computers are billed per computer, outside the Rule of 3 (see "Labor for New / Replacement Workstations")
Onboarding of a new client	Yes	Onboarding is always a Project
Change internet provider or move the office	Yes	Affects all users
A user cannot print	No	Normal support

The following are not Projects, even when they touch three (3) or more computers or users: (a) maintenance that we decide to perform, such as patching, changes to our security tools, and agent updates; (b) fixing a failure that affects several users at the same time, such as an email or internet outage within the Environment; and (c) incident containment included in Tier 2 and Tier 3. Setup of new or replacement computers is billed per computer, as described in "Labor for New / Replacement Workstations," and onboarding is always a Project.

If a request turns out to meet the Rule of 3 after work has started, we will tell you before continuing, and the remaining work will be handled as a Project once you approve it. We decide in good faith whether a request meets the Rule of 3.

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 of 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
- Basic security vulnerability check
- Basic backup and file recovery solution audit
- Speed test and ISP audit
- Print output audit
- Office telephone vendor service audit
- Asset inventory
- Email and website 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 monthly 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.
- Uninstall unsafe applications or applications that are no longer necessary.
- 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.
- Stabilize network and assure that all devices can securely access the file server.
- 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.

Onboarding fee. Onboarding is a Project. It is quoted separately, based on the number of users, devices, and locations and on the condition of your Environment, and is billed as stated in the Quote. Onboarding is not included in any Service Plan, and it is not waived by selecting a longer term.

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. Remediation of Issues, such as replacing unsupported computers or upgrading operating system editions, is quoted separately.

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.

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.

The descriptions below apply to each service when it is included in your Service Plan or listed in your Quote. We may provide a service through the Third Party Provider of our choice, as described in the MSA. Our current principal Third Party Providers, including the AI Tools we use with Client Data and the tools with Built-In AI Features, are listed in the Schedule of Third-Party Services at www.mypcfriends.com/vendors.

Application Control

Implementation and facilitation of an application allow-listing and ringfencing solution from our designated Third Party Provider.

- Only applications, scripts, and libraries approved for your Environment can run on covered computers.
- Ringfencing limits what approved applications can access, such as files, the registry, the network, and other applications.
- Requests to approve new software are reviewed during business hours in accordance with the Service Levels. Urgent requests are handled as Priority 2.

Note: Application control may block software that you or your users install without our knowledge. Blocking unapproved software is the intended function of the service and is not a service failure.

Artificial Intelligence Readiness (Project)

AI assistants such as Microsoft 365 Copilot can find and summarize any file, email, or chat that a user has permission to open. Before you turn them on, we recommend a readiness Project, which may include:

- Review of sharing and permissions in SharePoint, OneDrive, and Teams, and correction of files that are shared too broadly.
- Sensitivity labels and data loss prevention policies for confidential information.
- Configuration of the AI assistant licenses and settings that you choose.
- An acceptable use policy for AI tools and a short training session for your users.

AI readiness, deployment, and training are Projects and are quoted separately. AI services are Third Party Services; please see the "Artificial Intelligence" paragraph of the MSA. Tier 3 includes an acceptable use policy for AI tools as part of the written policies.

Azure Server and Azure Virtual Desktop Management

Management of servers and virtual desktops that we host for you in Microsoft Azure.

- Azure servers: monitoring, patching, endpoint protection, backup configuration, and administration of each server listed in the Quote.
- Azure Virtual Desktop (AVD): management of host pools, session hosts, user profiles, application images, and user access for each AVD user listed in the Quote.
- Cost monitoring and budget alerts, and recommendations to reduce consumption (for example, right-sizing and scheduled shutdowns).

Billing. Azure and AVD are Usage-Based Services under the MSA. Each Azure server is billed at the actual Azure consumption for that server, plus fifteen percent (15%), plus a monthly management fee per server. Each AVD user is billed at that user's share of the actual Azure consumption of the AVD environment, plus fifteen percent (15%), plus a monthly management fee per user. Consumption is billed in arrears based on the Microsoft invoice for the prior month.

Shared AVD consumption (such as session hosts and storage) is divided equally among the AVD users of the same environment unless the Quote states otherwise.

Backup and File Recovery

Implementation and facilitation of a backup and file recovery solution from our designated Third Party Provider.

- 24/7 monitoring of backup system, including offsite backup, offsite replication, and an onsite backup appliance ("Backup Appliance").
- Troubleshooting and remediation of failed backup disks.
- 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 recovery verification.

Backup Data Security: All backed up data is encrypted in transit and at rest in 256-bit AES encryption. 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. This includes both on-premise and cloud backups.

- 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 thirty (30) day 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 business hours.
- Request Method: Requests to restore backed up data should be made through one of the following methods: any approved support channel described in "Service Levels" (MyPCFriends app, desktop support icon, email to help@mypcfriends.com, or telephone at +1 (321) 300-1442).
- 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.

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 platform from our designated Third Party Provider. When included in Tier 3, CaaS is part of the Managed Compliance Program described below.

- Enable Client to monitor its compliance across the regulation(s) named in the Quote, such as the FTC Safeguards Rule, HIPAA Security, HIPAA Privacy, PCI DSS, and SOC 2.
- Access to training videos, recommended processes, and templates relevant to Client's specific compliance needs.
- Enable Client to schedule and assign compliance training, log employee attestations, and identify overdue training.

- Enable Client to create automated reminders for upcoming and past due compliance-related dates.
- Provision of personalized certificates auto-generated upon completion.

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 training or of a program milestone is valid as of the date on which it 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 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

Implementation and facilitation of a Dark Web Monitoring solution from our designated Third Party Provider.

Credentials and domains 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.

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.

DNS Filtering

Implementation and facilitation of a DNS filtering solution from our designated Third Party Provider on covered computers.

- Blocks access to known malicious, phishing, and newly registered domains.
- Optional blocking of website categories that you choose.

Note: DNS filtering reduces, but does not eliminate, the risk of visiting malicious websites, and may occasionally block legitimate websites. Requests to unblock a website are handled as Priority 3, or Priority 2 if business operations are affected.

Email Threat Protection

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 the 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 (including EDR)

Implementation and facilitation of an endpoint malware protection solution, with endpoint detection and response (EDR), 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 such as laptops, desktops, and servers.
- Protection against file-based and fileless scripts, as well as malicious JavaScript, VBScript, PowerShell, macros and more.
- Allow-listing for legitimate scripts.

- Blocking of unwanted web content.
- Detection of advanced phishing attacks.
- Detection/prevention of content from IP addresses with low reputation.

Please see the 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 lessons (multi-lingual), assigned each month.
- 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.
- Results by user, included in your monthly reports.

You are responsible for requiring your personnel to complete the assigned training.

Extended Detection & Response (XDR)

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* (email, endpoint, server, cloud workload, and the managed network), enabling faster threat detection.
- Provides extended malware sweeping, hunting, and investigation.
- Allows allow-listing 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).

Firewall as a Service (firewall appliance provided by MyPCFriends Cybersecurity)

- 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 the "Hardware as a Service" terms and conditions located in this Guide.
- Firewall appliance must be returned to MyPCFriends Cybersecurity upon the termination of service. Client will be responsible for missing or damaged (normal wear and tear excepted) appliance.

Firewall Solution / Managed Network (firewall appliance provided or purchased by Client)

- Monitors, updates (software/firmware), and supports Client-supplied firewall appliance, and the switches and wireless access points listed in the Quote.
- 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.
- Client must keep the manufacturer's security subscription and support for the firewall active.

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. MyPCFriends Cybersecurity 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, MyPCFriends Cybersecurity and has been determined by MyPCFriends Cybersecurity 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 MyPCFriends Cybersecurity 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.

Identity Threat Detection and Response (ITDR)

Implementation and facilitation of an identity threat detection and response solution from our designated Third Party Provider for covered Microsoft 365 accounts.

- 24x7 monitoring of sign-ins, mailbox rules, and account changes for signs of account takeover, such as sign-ins from unusual locations or suspicious forwarding rules.
- Automated or analyst-driven response, such as disabling a compromised account or revoking its sessions.
- Notification to your Authorized Contact, and recovery of the account during business hours.

Incident Response

Security Incident has the meaning given in "Breach/Cyber Security Incident Recovery," below.

- **Containment** means the actions needed to stop an active Security Incident from spreading or continuing, such as isolating devices, disabling or resetting compromised accounts, blocking malicious senders or sites, removing malicious mailbox rules, and confirming that the threat is no longer active. Containment also includes a written incident summary.

- **Recovery** means restoring systems and data after the threat is contained, such as rebuilding or reimaging devices, restoring data from backup, rebuilding servers, and returning the Environment to normal operation. Recovery is included only to the extent it can be completed within the Rule of 3; otherwise it is a Project.
- **Investigation** means determining the cause and extent of a Security Incident. Tier 3 includes investigation using the logs collected by the SIEM. Forensic investigation intended for use in litigation, insurance claims, or law enforcement, and the services of an incident response firm required by your insurer, are not included in any Service Plan.

	Tier 1	**Tier 2**	**Tier 3**
Containment	Basic containment during business hours; additional work at the incident response rate	Included, 24x7	Included, 24x7
Recovery	Incident response rate	Included within the Rule of 3; Projects beyond that	Included within the Rule of 3; Projects beyond that
Investigation	Incident response rate	Cause and actions in the incident summary	SIEM-based investigation, incident record, and help preparing required notifications

Containment included in a Service Plan applies to Security Incidents in the covered Environment. It does not apply to devices, accounts, or systems that are not covered by the Quote, or that were not protected because you declined, removed, or disabled a security service we recommended or installed. Please see the Incident Mitigation Coverage paragraph of the MSA before requesting services for an incident covered by your insurance.

Labor for New / Replacement Workstations

Setup of new or replacement computers is not included in your Service Plan and does not follow the Rule of 3. Each computer is billed separately, per computer, at the rate stated in the Quote, whether you set up one computer or several at the same time. Setup includes enrolling the computer in our management and security tools, installing your standard business software, and moving the user's data and profile from the computer it replaces. Large deployments, such as computers for a new location or an office move, may be quoted as a Project at a fixed price.

The following restrictions apply:

- This service is not available for used or remanufactured computers; and,
- New/replacement computers must be business-grade machines (not home editions) from a major manufacturer such as Dell, HP, or Lenovo, running a then-currently supported business edition of Windows (for example, Windows 11 Pro) or macOS.

Managed Compliance Program (Tier 3)

A managed program that helps you meet the administrative and technical safeguards of each Applicable Framework named in the Quote.

- Identification of the Applicable Framework(s) and the systems and data in scope.
- Written risk assessment, updated each year and after a significant change in your business or a Security Incident.
- Written information security program (WISP) and written policies aligned with the NIST Cybersecurity Framework 2.0 and mapped to the Applicable Framework(s).
- Implementation and operation of the technical safeguards included in your Service Plan, such as MFA, encryption, logging and monitoring, access reviews, and vulnerability scans.
- Collection of evidence of the safeguards in operation, and a compliance report each month.
- Designated Security Role, including the written reports that the Applicable Framework requires (for example, the annual report to the board of directors or senior officer required by 16 C.F.R. § 314.4(i)).
- Support with insurance questionnaires, customer security questionnaires, and the information requested by an auditor or examiner.

Note: The Managed Compliance Program covers the systems we manage. Paper records, physical security, your vendors other than MyPCFriends Cybersecurity, and business processes we do not manage remain your responsibility, although

our policies and risk assessment will address them. Please see the "Compliance; No Legal Advice" and "Designated Security Roles" paragraphs of the MSA.

Managed Detection & Response (MDR)

Implementation and facilitation of a top-tier MDR solution from our designated Third Party Provider.

- 24x7 managed endpoint detection and response by a security operations center (SOC).
- Real time and continuous (24x7) monitoring and threat hunting.
- Real time threat response, including isolation of affected devices.
- Alerts handled in accordance with our Service Levels, below.
- Security reports, such as privileged activities, security events, and network reports, are available upon request and summarized in your monthly security report.
- 24x7x365 access to a security team for incident response.*

* Containment is included in Tier 2 and Tier 3 as described in "Incident Response." Other incident response services are provided on a time and materials basis. Please see the Anti-Virus; Anti-Malware and Breach/Cyber Security Incident Recovery sections below for important details.

Microsoft 365 Management and Licensing

- Administration of your Microsoft 365 tenant, including users, groups, licenses, shared mailboxes, Teams, OneDrive, and SharePoint.
- Security baseline, including multifactor authentication for every covered user, blocking of legacy authentication, and secure default settings.
- License management, including monthly review of unused or unassigned licenses.
- Resale of Microsoft 365 Business Premium and other Microsoft licenses. Microsoft licenses are Access Licenses under the MSA and are subject to Microsoft's commitment terms, which may not allow reductions until the end of the license term.

Note: The availability of Microsoft 365 is controlled by Microsoft and is subject to Microsoft's own service level agreement. If Microsoft issues a service credit to us for an outage that affected you, we will pass the corresponding credit through to you.

Microsoft 365 Backup

Implementation and facilitation of a cloud-to-cloud backup solution from our designated Third Party Provider for Exchange Online, OneDrive, SharePoint, and Teams data of covered users.

- Backups performed automatically several times per day.
- Retention as stated by the Third Party Provider for the plan we provide (unlimited retention for active covered users unless the Quote states otherwise).
- Restores of individual items, mailboxes, or sites upon request, in accordance with the Service Levels.

Data of users who are no longer covered (for example, former employees whose licenses were removed) is retained only if the user is converted to an archived or shared account listed in the Quote.

NIST Risk Assessment

Perform a cybersecurity assessment under the NIST Cybersecurity Framework (CSF) 2.0, using the NIST Risk Management Framework and NIST SP 800-53 as references.

- Identifies how Client currently assesses, mitigates, and tracks its cybersecurity requirements.
- Identifies authorized and unauthorized devices in the managed network.
- Identifies gaps or deficiencies in the Client's operations that would prevent alignment with NIST CSF.

The assessment will cover the six core functions of NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover. The results of the assessment will be provided in a report that will identify detected risks and your organization's current maturity levels (i.e., indicators that represent the level of capabilities within your organization's security program) and will propose actionable activities to help increase relevant maturity levels and augment your organization's security posture.

Please Note: This service is limited to an assessment/audit only. Remediation of issues discovered during the assessment, as well as additional solutions required to bring your managed environment into compliance, are not part of this service. After the audit is complete, we will discuss the results with you to determine what steps, if any, are needed to bring your organization into full compliance. For Tier 3 clients, the annual risk assessment is included in the Managed Compliance Program.

Password Manager

Implementation and facilitation of a password management 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.
- Contact Information Vault: Store private addresses and personal contact information within your vault.
- Browser App: Browser extension permits easy access to your information, including the vaults 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.

Note: Each user is responsible for keeping the master password and recovery method of their vault. We cannot recover a vault's contents if both are lost.

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.

Pen testing is not included in any Service Plan. Please see additional terms for Penetration Testing below.

Remote Helpdesk

- Remote support provided during business hours for covered users, Business Devices, and Supported Software.
- Tiered-level support provides a smooth escalation process and helps to ensure effective solutions.
- Support requests may be submitted through the approved channels described in "Service Levels."

Remote Infrastructure Maintenance & Support; Remote Monitoring and Management

- Configuration, monitoring, and preventative maintenance services provided for the managed IT infrastructure.
- If remote efforts are unsuccessful, then MyPCFriends Cybersecurity will dispatch a technician to the Client's premises to resolve covered incidents, as described in "Physical Locations Covered by Services" (timing of onsite support is subject to technician availability and scheduling).
- 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 and SSD 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.

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

Event	Server	Workstation
Hardware failures	Yes	No
Device offline	Yes	No
Failed/missing backup	Yes	No
Failed/missing updates	Yes	Yes
Low disk space	Yes	Yes
Agent missing/misconfigured	Yes	Yes
Excessive uptime	Yes	No
Automatic reboots (weekly)	No	Yes

Security Information & Event Management (SIEM)

Implementation and facilitation of an industry leading SIEM solution from our designated Third Party Provider. SIEM is included in Tier 3.

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 define the log sources to be collected, such as Microsoft 365, firewalls, and servers covered by the Quote (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 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.
- Log Retention. Logs are retained for fourteen (14) months, unless the Quote states a different period. Logs from sources that are not connected to the SIEM, or that stop sending logs because of changes not made by us, are not retained.

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. Containment of Security Incidents detected by the SIEM is included in Tier 2 and Tier 3 as described in "Incident Response"; other remediation is provided on a time and materials basis.

Server Monitoring & Maintenance

As part of our RMM service, we will monitor and maintain managed servers listed in the Quote 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.

Servers are not included in the per-user price of a Service Plan and are billed per server as stated in the Quote.

Server Next-Generation Antivirus

Implementation and facilitation of a top-tier, next generation antivirus protection solution from our designated Third Party 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.

Software Licensing (applies to all software licensed by or through MyPCFriends Cybersecurity)

All software provided to you by or through MyPCFriends Cybersecurity is licensed, not sold, to you ("Software"). In addition to any Software-related requirements described in MyPCFriends Cybersecurity'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.

Two Factor (Multifactor) Authentication

Multifactor authentication (MFA) for Microsoft 365 is included in every Service Plan and is enforced for every covered user. For other applications, implementation and facilitation of a two factor authentication solution from our designated Third Party Provider is available as listed in the Quote:

- Advanced two factor authentication with advanced admin 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.

You may not ask us to disable MFA for a covered user. If you require an exception, you must request it in writing, and you accept the risk of that exception.

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 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. Upgrades between

major versions or editions of an operating system (for example, Windows 10 to Windows 11, or Home to Pro) are not patches and are quoted separately.

Usage and Productivity Reporting

Every Service Plan includes reports that show how technology helps or slows down your team, based on data from our ticketing, monitoring, Microsoft 365, and training tools.

- Tier 1: time lost per person because of IT issues, devices that slow your team down (slow, old, low on disk space, or failing often), repeat issues by person or device, and training and phishing results.
- Tier 2 adds: Microsoft 365 adoption by person (for example, use of Teams and OneDrive), licenses paid for but unused, a security score for each employee, and time to make each new employee productive.
- Tier 3 adds: a one-page leadership dashboard every three (3) months with productivity, risk, and compliance by area, and recommendations with numbers.

Reports measure the use and performance of technology. They do not include keystroke logging, screen recording, or the content of communications or files. Please see the "Usage and Productivity Reporting" paragraph of the MSA, including your responsibility to inform your personnel. Reports may be prepared with the help of AI Tools through our approved systems, as described in the "Artificial Intelligence" paragraph of the MSA, and are reviewed by our team before delivery. Some metrics require that the corresponding data source be connected (for example, Microsoft 365 usage reports); metrics without a connected source are omitted until the source is available.

Virtual Chief Information Officer (vCIO)

Act as the main point of contact for certain business-related IT issues and concerns.

- Assist in creation of information/data-related plans and budgets.
- Provide strategic guidance and consultation across different technologies.
- Create company-specific best standards and practices.
- Provide education and recommendations for business technologies.
- Participate in scheduled meetings to maintain goals.
- Maintain technology documentation.
- Assess and make recommendations for improving technology usage and services.

Virtual Chief Information Security Officer (vCISO)

Included in Tier 3. A security advisor for your leadership.

- Meeting with your leadership every three (3) months to review risks, incidents, the status of the compliance program, and decisions that require your approval.
- Prioritized security roadmap and budget recommendations.
- Review of risk acceptance decisions and exceptions to policy, for your approval.
- Annual written report to your governing body or senior officer.

Please see the "VCTO, VCIO, or VCISO Services" policy below and the "Designated Security Roles" paragraph of the MSA.

Voice Over IP (VoIP) Services

Implementation and facilitation of an industry-recognized VoIP solution from our designated Third Party Provider. Features include:

- Scalable VoIP-based telephone service with call transferring, voicemail, caller ID, call hold, conference calling, and call waiting functionalities.
- Central control panel provides access to VoIP-related configurations, including physical address registration, call routing, updating greetings, and ability to turn on/off service features.
- Ability to use mobile app dialing.

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 Scanning

Implementation and facilitation of an industry-recognized vulnerability scanning solution from our designated Third Party Provider.

Vulnerability scanning identifies holes in the managed network that could be exploited. External vulnerability scans (which pertain to the IP address assigned to each customer location through the Client's ISP) are run monthly. Internal vulnerability scans (which pertain to all systems inside the managed network) are run at least every six (6) months for Tier 3 clients, and at least annually for other clients that subscribe to this service.

Vulnerability results will be discussed during business review meetings with Client. Vulnerability reports will be made available on request, and are included in the compliance report for Tier 3 clients. Remediation of vulnerabilities on covered devices that can be fixed by patching or configuration is included; remediation that meets the Rule of 3 or requires new hardware or software is quoted separately. Please see additional terms for vulnerability scanning below.

Wi-Fi Services

MyPCFriends Cybersecurity will install at the Client's premises Wireless Access Points to provide bandwidth in all areas requiring wireless network coverage, as agreed upon by MyPCFriends Cybersecurity and Client.

- MyPCFriends Cybersecurity will maintain, supervise, and manage the wireless system listed in the Quote.
- Installed equipment, if provided by MyPCFriends Cybersecurity, will be compatible with the then-current industry standards.
- MyPCFriends Cybersecurity will provide remote support services during 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.

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.
- 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.
- Endpoint protection agent monitoring, alerting us to potential security vulnerabilities.
- Routine operating system inspection and cleansing.
- Secure remote connectivity to the workstation and collaborative screen sharing.
- Review and installation of updates and patches for Windows and supported software.
- Asset inventory and workstation information collection.

Covered Environment

Managed Services will be applied to the users and devices indicated in the Quote ("Covered Hardware"). The list of Covered Hardware may be modified by mutual consent (email is sufficient for this purpose); however, we reserve the right to modify the list of Covered Hardware at any time if we discover devices that were not previously included in the

list of Covered Hardware and which are receiving Services, or as necessary to accommodate changes to the quantity of Covered Hardware.

Unless otherwise stated in the Quote, Covered Devices will only include technology assets (such as computers, servers, and networking equipment) owned or leased by the Client's organization. As an accommodation, MyPCFriends Cybersecurity 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.

Per-user Service Plans. If the Quote indicates that the Services are billed on a "per user" basis, then each covered user includes one (1) named user account and one (1) Business Device (a desktop or laptop computer). Each additional computer used by the same user, and each computer not assigned to a covered user (for example, a shared front-desk computer), is billed as an additional computer. Each covered user may also connect one (1) mobile device (a phone or a tablet) for access to Microsoft 365, which we will enroll and configure on a best-effort basis. Additional mobile devices are supported only if stated in the Quote. Servers, network sites, shared mailboxes, and other items listed in "Rates for Services Billed Separately" are not included in the per-user price.

A "Business Device" is a device that (i) is owned or leased by Client and used primarily for business, (ii) is regularly connected to Client's managed network or to the internet, and (iii) has installed on it a software agent through which we (or our designated Third Party Providers) can monitor the device.

User changes. Adding and removing users is included, subject to the Rule of 3. Your monthly fees are adjusted on the next invoice to reflect the number of covered users and devices, subject to the Minimum Monthly Fees in the MSA. Microsoft licenses may only be reduced as permitted by Microsoft's commitment terms.

We will provide support for any software applications that are licensed through us, and for your line-of-business applications as described in your Service Plan. Such software ("Supported Software") will 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. Coverage for non-Supported Software is outside of the scope of the Quote and will be provided to you on a "best-effort" basis and a time and materials basis with no guarantee of remediation. Should our technicians provide you with advice concerning non-Supported Software, the provision of that advice should be viewed as an accommodation, not an obligation, to you.

If we are unable to remediate an issue with non-Supported Software, 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 whenever the issue can be resolved remotely. When we determine, in our reasonable discretion, that an onsite visit is required to resolve a covered issue, the onsite visit is included in your Service Plan at no additional charge for locations within the Service Area. Onsite 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 the Client location(s) listed in the Quote.

Service Area. The Service Area includes locations within forty-five (45) minutes of one-way driving time from our nearest office. Travel beyond the Service Area is billed as described in "Travel Time," below. Onsite visits that you request when we have determined that the issue can be resolved remotely, and onsite work that is part of a Project, are billed at the applicable rate.

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 computers must run an operating system edition and version that is currently supported by its manufacturer and suitable for business management (for example, Windows 11 Pro or Enterprise; Windows Home editions are not supported), and must have all the latest service packs and critical updates installed.

Computers that do not meet this requirement are Legacy Devices under the MSA until they are upgraded or replaced.

- 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.
- Firewalls must be supported by their manufacturer and have an active security subscription.
- 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 or included in your Service Plan will be out of scope and will not be provided to Client unless otherwise agreed, in writing, by MyPCFriends Cybersecurity. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by MyPCFriends Cybersecurity in writing:

- Projects, as defined by the Rule of 3.
- Customization of third party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- Battery backup replacement.
- Equipment relocation.
- The cost to bring the managed environment up to these minimum requirements (unless otherwise noted in the Quote).
- 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.

Service Levels

Business hours. Automated monitoring is provided on an ongoing (i.e., 24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided during our business hours, which are Monday through Friday, 9:00 AM to 5:00 PM Eastern Time, excluding the MyPCFriends Cybersecurity-observed holidays listed below ("Business Hours"), unless otherwise specifically stated in the Quote or as otherwise described below. For Tier 2 and Tier 3, Security Incidents are also handled outside of Business Hours as described in "After-Hours Security Response."

How to request support. Requests must be submitted through one of the following approved channels: (a) a ticket in the MyPCFriends app; (b) a ticket from the MyPCFriends support icon on your computer's desktop; (c) email to help@mypcfriends.com; or (d) telephone at +1 (321) 300-1442. **Priority 1 (Critical) issues must be reported by telephone.** A Priority 1 issue reported only by ticket or email is treated as Priority 2 until it is reported by telephone. Outside of Business Hours, Emergencies must be reported to the Emergency Line described in "Support During Off-Hours/Non-Business Hours." Other requests received outside of Business Hours are received at the start of the next Business Hour, except as described in "After-Hours Security Response."

Channels that are not approved. Microsoft Teams, WhatsApp, text messages, social media, and messages to the personal phone or account of any of our personnel are not approved channels. Requests sent through them are not received as support requests and do not start a response time. These channels may be used only for general questions, and our personnel use them only from devices and accounts provided by MyPCFriends. Never send passwords or other sensitive information through a messaging channel.

Priority. We assign the priority of each request based on its business impact and urgency, after consulting with the Client when needed. We may change the priority if the impact changes.

Priority	Description	Examples	Tier 1 response	Tier 2 response	Tier 3 response
P1 – Critical	Your business cannot operate, or there is an active Security Incident	Most users cannot work; server or internet down for the office; ransomware; a compromised account sending fraudulent email	1 Business Hour	30 minutes	30 minutes
P2 – High	Several users or a business-critical function are affected and there is no reasonable workaround	A department cannot use a key application; a shared printer for a team is down	4 Business Hours	2 Business Hours	1 Business Hour
P3 – Medium	One user cannot work normally, or a limited number of users or functions are affected	One computer will not start; one user cannot access email	8 Business Hours	4 Business Hours	4 Business Hours
P4 – Low	A request, question, or issue with a workaround	A new shortcut; a software install for one user; a question	2 business days	1 business day	1 business day
Scheduled work and Projects	Planned work	Approved Projects; scheduled changes	Proposed schedule within 3 business days of approval	Same	Same

What "response" means. A response is the first contact by a MyPCFriends Cybersecurity technician (by telephone, email, ticket update, or remote session) that acknowledges the request and begins work on it, or that schedules the work at a time agreed with you. Automated acknowledgments do not count as a response. Response times are measured from the time the request is received through an approved channel, counting only Business Hours.

Updates and resolution. For P1 issues, we will provide status updates at least every one (1) Business Hour until the issue is resolved or a workaround is in place. For P2 issues, we will provide updates at least once per business day. We will work diligently to resolve every issue, but resolution times depend on the nature of the issue and on Third Party Providers, and are not guaranteed.

After-Hours Security Response (Tier 2 and Tier 3). Outside of Business Hours, the security operations center monitors covered computers and Microsoft 365 accounts and may contain threats directly (for example, by isolating a device or disabling an account). When the security operations center escalates a Security Incident to us outside of Business Hours, our on-call technician's target is to begin response within two (2) hours. This after-hours target is an objective and is not eligible for service credits.

Third party availability. We do not guarantee the availability (uptime) of Third Party Services such as Microsoft 365, Microsoft Azure, internet service, or telephone carriers. Their availability is governed by their own service level agreements. If a Third Party Provider issues a service credit to us for an outage that affected you, we will pass the corresponding credit through to you.

Measurement and Service Credits

Target. Our target is to meet the response times above for at least ninety percent (90%) of the eligible P1, P2, and P3 requests of each Client in each calendar quarter (the "Target Service Level"). If a Client has fewer than ten (10) eligible requests in a quarter, the Target Service Level is met when no more than one (1) eligible request misses its response time. Response attainment is included in your monthly service report and is measured from our ticketing system records, which we will share with you upon request.

Service credits. If we miss the Target Service Level in a calendar quarter, and you request a credit in writing within thirty (30) days after the end of that quarter, you will receive a credit on a future invoice equal to:

Quarterly response attainment	Credit
75% to less than 90%	5% of one month of the Managed Services Fee
Less than 75%	10% of one month of the Managed Services Fee

The "Managed Services Fee" is the monthly recurring fee for your Service Plan and other managed services under the Quote, excluding Microsoft and other licenses, Usage-Based Services, hardware, Projects, and other pass-through or one-time charges. Credits will not exceed ten percent (10%) of one month of the Managed Services Fee in any calendar quarter. Credits are applied only to future invoices, have no cash value, are not available while any undisputed amount is past due, and are forfeited if the Services end before they are applied.

Exclusions. Requests are not eligible, and time does not count against a response time, to the extent that a delay is caused by: (a) the Transition Exception, Scheduled Downtime, Client-Side Downtime, or Vendor-Side Downtime described in the MSA; (b) a force majeure event; (c) requests not submitted through an approved channel, or P1 issues not reported by telephone; (d) waiting for your response, access, approval, or information; (e) devices, software, or locations that are not covered by the Quote, Legacy Devices, or Obsolete Elements; (f) suspension of the Services for nonpayment or under the MSA; (g) changes to the Environment made without our authorization; (h) a widespread event that affects many of our clients at the same time (for example, a global Microsoft outage or a mass cyberattack), during which we will prioritize by severity; or (i) requests marked with a priority higher than the one we assign under this section.

Chronic Service Level Failure. If our quarterly response attainment is less than seventy-five percent (75%) in two (2) consecutive calendar quarters, or less than ninety percent (90%) in three (3) consecutive calendar quarters, you may terminate the affected Quote by written notice given within thirty (30) days after the end of the last such quarter, effective thirty (30) days after we receive the notice, without paying a Termination Fee. You remain responsible for all fees accrued through the termination date and for Access Licenses as described in the MSA.

Sole remedy. The service credits and the termination right described in this section are your sole and exclusive remedies for any failure to meet a response time or the Target Service Level.

Support During Off-Hours/Non-Business Hours

Emergency Line. Outside of Business Hours, call the MyPCFriends Emergency Line at **+1 (321) 348-6616** to report an Emergency. An "Emergency" is an issue that meets the definition of P1 – Critical in the priority table in "Service Levels": your business cannot operate, or there is an active Security Incident. A suspected Security Incident reported in good faith is treated as an Emergency, even if it turns out not to be one, and the call is never billed as a non-Emergency call. Use the Emergency Line only for Emergencies. Send other requests through the MyPCFriends app, the desktop support icon, or email, and we will handle them during the next Business Hours.

How Emergency Line calls are billed. In Tier 2 and Tier 3, response to Emergencies outside of Business Hours is included in your Service Plan, both for Security Incidents and for other Emergencies; our on-call technician's target is to begin response within two (2) hours, and this after-hours target is an objective that is not eligible for service credits. In Tier 1, and for clients without a Service Plan, Emergency work outside of Business Hours is handled subject to technician availability and is billed as Non-Business Hour Support, or at the incident response rate for Security Incidents, unless your Quote states otherwise. In every Service Plan, a call about a suspected Security Incident made in good faith is not billed, even if it turns out not to be one. If the issue reported to the Emergency Line is not an Emergency as defined above, the call and any work performed are billed as Non-Business Hour Support, with a one (1) hour minimum.

Other technical support provided outside of Business Hours is offered on a case-by-case basis and is subject to technician availability. If MyPCFriends Cybersecurity agrees to provide off-hours/non-business hours support ("Non-Business Hour Support"), then that support will be billed to Client at the Non-Business Hour Support rate stated in the Quote. All hourly services are billed in fifteen (15) minute increments, and partial increments are rounded to the next highest increment. A one (1) hour minimum applies to all Non-Business Hour Support.

The following are not billed as Non-Business Hour Support: (a) incident containment and Emergency response included in Tier 2 and Tier 3; (b) maintenance that we schedule outside of Business Hours for our own convenience; and (c) work that we schedule outside of Business Hours to avoid disrupting your business, when we have agreed in advance that it is included.

MyPCFriends Cybersecurity-Observed Holidays: MyPCFriends Cybersecurity observes the following holidays:

- New Year's Day
- Martin Luther King Jr. Day
- Presidents' Day

- Good Friday (half day)
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- The day following Thanksgiving Day
- Christmas Eve
- Christmas Day
- New Year's Eve (half day)

Fees

The fees for the Services, including the rates for the services billed separately listed below, are stated in the Quote. If the Quote does not state a rate for a service that you request, we will tell you the rate in writing (email is sufficient) before the work starts.

Rates for Services Billed Separately

Service	How it is billed
Additional computer (more than one per covered user, or not assigned to a covered user)	Per computer, per month
Shared mailbox under management (no Microsoft 365 license required)	Per mailbox, per month
Physical server at your premises	Per server, per month
Azure server management	Per server, per month, plus Azure consumption and a management percentage
Azure Virtual Desktop (AVD) management	Per AVD user, per month, plus a share of AVD consumption and a management percentage
Setup of new or replacement computers	Per computer, one time
Onboarding	Project, one time
Projects (Rule of 3)	Per hour, with a one (1) hour minimum, or fixed price per written scope
Non-Business Hour Support	Per hour, with a one (1) hour minimum
Incident response (Tier 1, and clients without a Service Plan)	Per hour
Microsoft licenses and other third party licenses	Per license
Network sites, VoIP, BCDR, penetration testing, compliance assessments, hardware, and other services	As quoted

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, we will travel up to forty-five (45) minutes one-way from our nearest office to your location at no charge. Time spent traveling beyond 45 minutes (e.g., locations that are beyond 45 minutes from our office, occasions on which traffic conditions extend our drive time beyond 45 minutes one-way, etc.) will be billed to

you at our then-current project rate. In addition, you will be billed for all tolls, parking fees, and related expenses that we incur if we provide onsite services to you.

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 project rate (or Non-Business Hour Support rate, whichever is appropriate).

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.

Term; Termination

The Services will commence, and billing will begin, on the date indicated in the Quote ("Commencement Date") and will continue through the initial term listed in the Quote ("Initial Term"). Service Plans are offered with an Initial Term of twelve (12), twenty-four (24), or thirty-six (36) months. 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 MyPCFriends Cybersecurity's satisfaction.

The Services will continue through the Initial Term until terminated as provided in the Agreement, the Quote, or as indicated in this Services Guide (the "Service Term"), and will renew automatically as described in the "Auto-Renewal" paragraph of the MSA.

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 MyPCFriends Cybersecurity "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.

Compliance records at termination. For Tier 3 clients, upon termination and payment of all fees due, we will deliver to you, upon request made within thirty (30) days after termination, an electronic copy of your WISP, policies, risk assessments, and the compliance evidence we collected. SIEM logs can be exported as a transition service under the MSA.

Offboarding

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

- Removal/disabling of monitoring agents in the Environment.
- Removal/disabling of endpoint software from the Environment.
- Removal/disabling of Microsoft 365 from the Environment (unless the licenses for Microsoft 365 are being transferred to your incoming provider; please speak to your technician for details).
- Termination of SQL or Remote Desktop licenses provided by MyPCFriends Cybersecurity.

- Removal of credentials from the Environment.
- Removal of backup software from the Environment.

Additional Policies

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.

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 MyPCFriends Cybersecurity, 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 MyPCFriends Cybersecurity 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

Except for the containment, recovery, and investigation services included in your Service Plan as described in "Incident Response," and 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 at our then-current incident response rate. 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 MyPCFriends Cybersecurity 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. MyPCFriends Cybersecurity 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 MyPCFriends Cybersecurity 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 MyPCFriends Cybersecurity 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. MyPCFriends Cybersecurity cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that MyPCFriends Cybersecurity shall be held harmless if such data corruption or loss occurs. Client is strongly advised to keep a local backup of all of stored data to mitigate against the unintentional loss of data.

Procurement

Equipment and software procured by MyPCFriends Cybersecurity 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, MyPCFriends Cybersecurity 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. MyPCFriends Cybersecurity is not a warranty service or repair center. MyPCFriends Cybersecurity 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 MyPCFriends Cybersecurity will be held harmless, and (ii) MyPCFriends Cybersecurity 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, VCIO, or VCISO Services

The advice and suggestions provided by us in our capacity as a virtual chief technology, information, or information security officer (if applicable) will be for your informational and/or educational purposes only. MyPCFriends Cybersecurity 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 MyPCFriends Cybersecurity on Client's corporate records or accounts, except that Client may identify MyPCFriends Cybersecurity, as its service provider, in its written information security program and compliance records as performing a Designated Security Role under the MSA. Decisions about your business, including the acceptance of risk, remain yours.

Sample Policies and 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.

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." Registration: You are responsible for activating the E911 dialing feature by registering the address where you will use the VoIP service. This will not be done for you, and you must take this step on your own initiative. To do this, you must log into your VoIP control panel and provide a valid physical address. If you do not take this step, then E911 services may not work correctly, or at all, using the VoIP service. Emergency service dispatchers will only send emergency personnel to a properly registered E911 service address. Location: The address you provide in the control panel 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 enter 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 your failure to register timely and correctly your physical location information into the control panel. 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 not properly and promptly register 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 register a change of address with us through the VoIP control panel 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. If you do not register the VoIP service at your location and you dial 9-1-1, that call will be categorized as a "rogue 911 call." If you are responsible for dialing a rogue 911 call, you will be charged a non-refundable and non-disputable fee of $250/call. 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 hosted services provided to you, including but not limited to (and as applicable) hosted applications, hosted websites, hosted email services, and hosted infrastructure services ("Hosted Services"). MyPCFriends Cybersecurity 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 Hosted 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 Hosted Services. Similarly, we do not exercise editorial control over the content of any information or data created on or accessible over or through the Hosted Services. Instead, we prefer to advise our customers of inappropriate behavior and any necessary corrective action. If, however, Hosted Services are used in violation of this AUP, then we reserve the right to suspend your access to part or all of the Hosted Services without prior notice. Violations of this AUP: The following constitute violations of this AUP:

- Harmful or illegal uses: Use of a Hosted 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 Hosted 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: MyPCFriends Cybersecurity 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.
- Cryptomining: 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 MyPCFriends Cybersecurity 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, MyPCFriends Cybersecurity'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.
- Deceptive synthetic media: Use of the Hosted Services to create or distribute deceptive synthetic media (for example, "deepfake" audio, images, or video) or to impersonate any person or organization is prohibited.
- 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 performances 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, MyPCFriends Cybersecurity 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.

Revision History

Version	Date	Summary
2024.1	February 2024	Original version.
2025.1	September 2025	Word edition of Version 2024.1; layout changes only.
2026.1	November 2026	Reorganized around Service Plans (Tier 1, Tier 2, Tier 3) with deliverables; Rule of 3 for Projects; new services (application control, Azure and AVD, DNS filtering, ITDR, incident response, managed compliance program, Microsoft 365 management and backup, productivity reporting, vCISO); new service levels with quarterly measurement and capped credits; business hours of 9:00 AM to 5:00 PM ET defined in one place; on-site visits included within the Service Area; services billed separately, with rates stated only in the Quote; onboarding as a Project; new computer setup billed per computer, outside the Rule of 3; approved support channels; Emergency Line for after-hours Emergencies, included in Tier 2 and Tier 3; SIEM log retention of 14 months; 12, 24, or 36 month terms; one mobile device per user; artificial intelligence readiness Project and AI acceptable use policy in Tier 3; cyber insurance required for Tier 3.

Last Updated: November 2026 (Version 2026.1)