Services Guide

This Services Guide contains provisions that define, clarify, and govern the services described in the quote that has been provided to you (the "Quote"). 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 Allied Technology Group ("Allied," "we," "us," or "our"); however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services"). This Services Guide is governed under our Master Services Agreement ("MSA"). You may locate our MSA through the link in your Quote or, if you want, we will send you a copy of the MSA by email upon request. Capitalized terms in this Services Guide will have the same meaning as the capitalized terms in the MSA, unless otherwise indicated below.

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

This Services Guide contains important provisions pertaining to the auto-renewal of the Services in the Quote, as well as fee increases that may occur from time-to-time. Please read this Services Guide carefully and keep a copy for your records.

Initial Assessment / Diagnostic Services

In the Initial Assessment/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:

- Assessment 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 review
- ISP and Telecommunications Review
- Asset inventory
- Email and Unified Communications review
- IT support processes
- Review of Industry Best Practices

If deficiencies are discovered during the assessment process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and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, assessment 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 assessment 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, laptops and key network infrastructure.
- 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 key network infrastructure.
- 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, in our discretion, that different or additional onboarding activities are required.

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

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

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 technician.

Managed Services

SERVICES	GENERAL DESCRIPTION
Business Support Agreement	**Unlimited Remote Helpdesk** • Remote support provided during normal business hours for managed devices and covered software. • Tiered-level support provides a smooth escalation process and helps to ensure effective and fast solutions. **On-Site Dispatch Support** If remote efforts are unsuccessful, then Allied will dispatch a technician to the Client's premises to resolve covered incidents (onsite support is subject to issue, technician availability, and scheduling) **Infrastructure Optimization** As part of our Business Agreement, we will monitor and maintain managed Key Infrastructure 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 • Server 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

- Server essential service monitoring
- Server Anti-virus agent and monitoring, alerting us to potential security vulnerabilities
- Routine operating system inspection and cleansing
- Secure remote connectivity to the server and collaborative screen sharing
- Patch management during an agreed upon maintenance window (server only) and in accordance with Allied's Patch Management Policy. Patches will be automated and when necessary manually applied in accordance to Allied's Patch Management Policy.
- Remediation and Recovery from Cyber Security Incidents is included if both Backup and File Recovery AND Endpoint Detection & Response (EDR) & Active Threat Defense services are in place prior to incident in addition to this Business Support Agreement. This agreement does not cover Incident Response.

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 of processor or memory usage.
- Anti-virus agent and 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.
- Licensed Copy of Allied's preferred anti-virus

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

Event	Server	Workstation
Hardware Failures (require vendor maintenance)	Yes	No
Device Offline	Yes	No
Failed/Missing Backup	Yes	Yes
Failed/Missing Updates	Yes	Yes
Low Disk Space	Yes	Yes

Updates and 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 items.
- Perform minor software 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 managed items.

Virtual Chief Information Officer (vCIO)

Acts as the main point of contact for strategic initiatives and certain business-related IT issues:

- 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.
- Licensed copy of Allied's preferred anti-virus (server only)

	Asset Management Allied will provide asset management reports for all monitored devices as part of each Technical Business Review or upon your request. Hardware Life Cycle Reports Allied's hardware lifecycle management will include purchase date, warranty information and expected end of life dates. Software Asset Management Allied will report on all standard software packages and when applicable any line of business application in use. • Licensed software version and counts • Deployed license in use version and counts • Track software renewal dates for standard software, identify unused software license and optimize software counts during renewal.
Backup and File Recovery	Implementation and facilitation of a top-tier backup and file recovery solution from our designated Third Party Provider. Features include: • 24/7 monitoring of backup system, including offsite backup, offsite replication, and a local virtual appliance ("Backup Appliance") • Troubleshooting and remediation of failed backup • Preventive maintenance and management of imaging software • Firmware and software updates of virtual appliance • Problem analysis by the network operations team • Monitoring of backup successes and failures • Daily recovery verification • Local data snapshots taken every hour • Data is Air-gapped to provide better protection • Auto-verify is enabled on all backups to ensure restores are working properly 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 according to the specifications below:

Virtual Appliance and private cloud retention policies will follow the below:

- Retain all snapshots for 14 days.
- After 14 days, retain:
- Last snapshot of day for 30 days.
- Last snapshot of week for 10 weeks.
- Last snapshot of month for 6 months.
- Do not retain last snapshot of year.

Public Cloud and Direct-to-Cloud retention policies will follow the below:

- Backup retention method: Tiered
- Retain all snapshots for 30 days.
- After 30 days, retain:
- Last snapshot of day for 30 days.
- Last snapshot of week for 24 weeks.
- Last snapshot of month for 12 months.
- Last snapshot of year for 7 years.

Backup Alerts: Managed servers will be configured to inform Allied's NOC of any backup failures.
Recovery of Data: If a clients needs to recover data from backup, then the following procedures will apply:

- Service Hours: Backed up data can be requested during our normal business hours, which are currently 7am -7pm Monday - Saturday.
- Request Method. Requests to restore back up data should be made through one of the following methods:
    - Email: ondemand@alliedtechgroup.com
    - Telephone: 855-372-4909
- Restoration Time: We will endeavor to restore backed up data as quickly as possible following service ticket submission.

	Virtual Appliances • Local Virtual Appliance for storing backup data • 7TB Available capacity Backup & Recovery Service for Desktop • Retention policies follow same criteria as servers • Data is Air-gapped to provide better protection for backups
Managed Unified Communications (UC)	Allied provides a total managed solution combining an enterprise capable virtual PBX, utilizing Internet based SIP trunks for calling coupled with Allied's ongoing support and management services. Hosting options are available either within the client's existing infrastructure or securely hosted in Allied's cloud solution. This solution is priced based on the capacity of the virtual PBX to support an organization concurrent call peak. SIP trunks and any required on-premise hardware will be purchased separately. **UC Virtual PBX** Key features of the vPBX include: • Unlimited Extensions • Auto Attendant/Digital Receptionist • Integrations with Microsoft O365 & Teams • Call Recording • Mobile App/Softphone for Each User **Secure Cloud Hosting** Hardware and datacenter services optimized for whatever level of UC Virtual PBX is required to support the client organization. Each virtual appliance is dedicated to the client and secured with a virtual firewall specifically configured to support a properly sized Virtual PBX. Each hosting agreement includes unlimited bandwidth to and from the Virtual PBX as well as support for concurrent calls up to the included amount. Hosting agreements are an annual commitment and will be billed in full at the commencement of each cloud hosting agreement. **SIP Services** Allied does not directly sell SIP service, but as a part of this solution Allied will assist the client with selecting an appropriate SIP provider that can service all the client location and existing published phone numbers. The client will receive a separate invoice directly from the ISP/Telco for SIP services.

	Additional Add-On Services • DDos Protection for Cloud Hosted Environments • eFax Solutions
New/Replacement PC Installations	Includes labor/services charges for setup of new workstations, or replacement of existing workstations. **Labor covers:** • Initial OOBE setup • Removal of all unnecessary bloatware • Installation of all Allied tools • Joining of computer to domain • Configuration of all software needed for specified users. • Setup of all peripheral hardware (monitors, mice, printers, etc.) • Delivery and manual setup of computer and peripheral equipment • Copying of data from old computer to new computer (If applicable) • Disposal of old computer (If applicable) • Configuration of default applications • Post delivery check-in with end user to verify workstation and all applications are working as expected. • Fixed Price Based on current Allied PC Installation Pricing (Does not include travel time/expense)

Managed Security Services

SERVICES	GENERAL DESCRIPTION
Dark Web Monitoring	Implementation and facilitation of a top-tier Dark Web Monitoring solution from our designated Third Party Provider. Email address and/or public IP supplied by Client will be added into a system that continuously uses human and machine-powered monitoring to determine if the supplied information is located on the dark web. If compromised credentials are found, they are sent to client's point of contact via an automated email.

	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.
Email Security	Implementation and facilitation of a trusted email threat protection solution from our designated Third Party Provider. Features include: • Content Filtering • Anti-Virus • Spam Filtering • Outbound Filtering • Imposter Email Protection • Advanced Granular Reporting • URL Defense (Sandboxing) • Attachment Defense (Reputation) • Email Data Loss Protect (DLP) • Emergency Inbox – Access to email during service disruption. (30 days) • Email Spooling – Comprehensive, extremely low-maintenance MX management during service interruption. (30 days) • Instant Replay – Access to all email for the previous 30 days with ability to redeliver in the case of accidental deletion. **Advanced Email Security with Email Encryption:** Includes all the features of Business Email Security and adds: • Attachment Defense (Sandboxing) • Email Encryption • Social Media Account Protection
End User Security Awareness Training	Implementation and facilitation of a security awareness training solution from an industry leading third-party solution provider. Features include: • Quarterly social engineering test against the client's user base. • Online, on-demand training videos. • Baseline testing to access the phish-prone percentage of users; simulated phishing email campaigns designed to educate employees about security threats.

	• Direct reporting of each campaign and training results sent to the primary contact. **Please Breach / Cyber Security Incident Recovery sections below for important details.**
Advanced Network Security	Implementation and facilitation of secure Internet gateway and remote access. Allied will fully manage firewall to terminate Internet, LAN, DMZ, and Remote access connections. Features include: • Only allow minimum required connections to secure environments • Utilize strong encryption on all WAN connections • IPS & AV traffic inspection • Geo-location filtering • Software/firmware updates • Proactive 24 x 7 IPS & log monitoring
Endpoint Detection & Response (EDR) & Active Threat Defense	Managed EDR service is designed to provide clients a solution focused on preventing, detecting and responding to threats on endpoints. Backed by the Allied security operations team, the service provides management and monitoring 24x7x365, the service meets evolving threats, provides automatic response based on playbooks and provides actionable data. **What's Included** • Deployment of necessary agents to each endpoint • Analysis of logs with notification of suspicious activity or identified threats • Customizable security policies • Customizable playbook with desired automated response • Ongoing playbook and policy optimization based on threat data and business requirements • Monthly threat findings review • 6 month log retention **Active Threat Defense** • Actively detect, collect, analyze, report and remediate possible footholds and backdoors. • Monthly reporting of all findings and actions.

	• Ransomware Canaries • External Recon **Service Limitations** • Service does not include remediation of threats. • The service does not include incident response. *** Remediation and incident response services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Managed Detection & Response (MDR) for Microsoft 365	Continuously monitors for indications and behaviors of a BEC attack, like a user logging in from a suspicious location or a malicious email forwarding rule. The Allied Security Operations Center (SOC) reviews any detections (24x7x365), instantly isolating any compromised users and supplies a semi-automated remediation plan for further necessary actions. In addition, 365 best practices are implemented unless otherwise requested by client. Microsoft 365 Secure Score report is available if Allied manages client's Microsoft account.
Application Whitelisting/Zero Trust	Application Whitelisting Service is designed to only allow pre-approved applications to run on any managed PC or server. Any non-approved application, program, or executable will be blocked, flagged, and reported to the Allied support desk for review and manual approval if authorized by member of client's management team.
Password Manager	Implementation and facilitation of industry-leading password management protection solution from our designed Third Party Provider. Features include: • Ability to create and customize automatically generated, randomized passwords. • Ability to secure folders containing passwords for specific users, making it easy and intuitive to give access to passwords users need, and lock down passwords they don't need access to.

	• Easily create groups with permissions to access specific folders making adding new users intuitive and easy to manage. • Ability to view the portal as a specific user, making it easy to check newly created permissions to ensure users don't have access to things they do not need.
Security Incident & Event Monitoring (SIEM)	Implementation and facilitation of an industry leading SIEM from our designed Third Party Provider. The SIEM service utilizes threat intelligence to detect threats that can exploit potential vulnerabilities against your managed network. • Deployment of necessary agents and/or collectors • Analysis of logs with notification of suspicious activity or identified threats • Monthly report Compliance & regulatory reporting • 90 Day active log retention • 1 year log archive Note: The SIEM service is a monitoring and alert-based system only; remediation of detected or actual threats are not within the scope of this service and may require Client to retain Allied's professional or managed services.
Two Factor Authentication	Implementation and facilitation of a two factor authentication solution from our designed Third Party Provider. Features include: • **Verify user trust.** 2FA agent uses a second form of validation, such as a smartphone, to verify that a user is who they say they are before granting them access. • **Establish device trust.** Once access is granted, 2FA enables your organization to see every device that is connected to your network and applications and easily monitor device health and compliance. • **Enforce adaptive policies.** Ability to set access levels based on role, device, location, and other relevant factors. • **Grant secure access to users.** Get even more secure access, beyond what a VPN can provide, and verify the identities of users from wherever they choose to log in.

	• **Grant secure access to apps.** Provide users with single sign-on (SSO) for a consistently easy login experience. A user-friendly dashboard provides streamlined access to company apps. • **Advanced Reporting.** 180 days of data is kept in the cloud and easily exported for specific searches or audits on external and internal access for each user, and every login.
Mobile Device Management (MDM)	Implementation and facilitation of an MDM solution from our designated Third-Party Provider. Features include: • OS configuration management • Application inventory • Hardware inventory • Content management Admin remote actions (e.g., remote data wipe, troubleshooting, device lockout, etc.)
User Activity Monitoring	Implementation and facilitation of advanced reporting software that pulls data from Active Directory, Windows Servers, and workstation to create detailed and informative reporting. Reports include: • Activity Outside of Business Hours • Privileged Group Membership • Administrator account interactive logins • Disabled/Enabled users listing • Accounts set to never expire • User Account Changes • User Account Status Changes • Assistance finding culprit for Active Directory accounts being locked out • Alerts on privileged group modifications
Internet Content Filter with DNS Defense	Implementation and facilitation of on premises DNS servers and software installation of DNS filtering and proxy defense. This allows for filtering websites based on criteria provided by the client to block time wasting websites, non-appropriate and malicious websites at the DNS level from our designated Third-Party Provider. Features include: • DNS-layer security - Uses DNS to stop threats over all ports and protocols. Stop malware earlier and prevent callbacks to attackers if infected machines connect to your network.

	• Web security via selective proxy - Routes requests to risky domains to a selective proxy for deeper URL and file inspection. Effectively protect without delay or performance impact. • App discovery & blocking - Provides visibility into cloud apps used across your organization, so you can identify potential risk and block specific applications easily. • Ability to be utilized both on premises, and outside of the network.
Rogue Device Detection	Periodically scans the routers and subnets to detect any new systems/devices found in the network. Initially it lists all the systems/devices discovered in the network. After Allied verifies and marks all the valid systems/devices in the network, during subsequent scans, if any new device/system is detected in the network, it gets listed. This includes all types of devices like desktops/laptops (wired), mobile users (wireless), routers, switches, Etc. Features include: • Ability to mark systems/devices as trusted, guest, and rogue. • Shows the switch and port to which a system/device is connected. • Alert when a new system/device is detected or when the guest validity expires. • Supports blocking of switch ports to prevent unauthorized access.
Vulnerability Scanning	Implementation and facilitation of an industry-recognized vulnerability scanning solution from our designed Third Party Provider. Vulnerability scanning identifies holes in the managed network that could be exploited. Allied runs vulnerability scans on a quarterly basis unless otherwise stated. External scans pertain to the IP address assigned to each customer location through the Client's ISP. Internal scans look at all systems inside the managed network. Vulnerability reports will be provided to client and discussed during business review meetings with Client. • Please see additional terms for vulnerability scanning below.

Other Services

SERVICES	GENERAL DESCRIPTION
Hardware as a Service or Rental (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, IaaS, or Rental 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. • Repair/replacement of HaaS Equipment. Allied will repair or replace Rental/HaaS Equipment based on severity of issue. 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 managed Rental/HaaS Equipment in accordance with the Service Levels listed in this Services Guide. • Periodic Replacement of HaaS Equipment. From time to time and in our discretion, we may decide to swap out older HaaS Equipment for updated or newer equipment. (Generally, equipment that is five years old or older may be appropriate for replacement). If we elect to swap out HaaS Equipment due to normal, periodic replacement, then we will notify you of the situation and arrange a mutually convenient time for such activity. • 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 that we 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 Allied 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 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.
Software Licensing (applies to all software licensed by or through Allied)	All software provided to you by or through Allied is licensed, not sold, to you ("Software"). In addition to any Software-related requirements described in Allied's Master Services Agreement, Software may also be subject to end user license agreements (EULAs), acceptable use policies (AUPs), and other restrictions all of which must be strictly followed by you and any of your authorized users. When installing/implementing software licenses in the managed environment or as part of the Services, we may accept (and you agree that we may accept) any required EULAs or AUPs on your behalf. You should assume that all Software has an applicable EULA and/or AUP to which your authorized users and you must adhere. If you have any questions or require a copy of the EULA or AUP, please contact us.

Covered Environment

Managed Services will be applied to the number of 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 include technology assets (such as computers, servers, and networking equipment) owned by the Client's organization. As an accommodation, Allied may provide guidance in connecting a personal device to the Client's organization's technology, but support of personal devices is generally not included in the Scope of Services.

If the Quote indicates that the Services are billed on a "per user" basis, then the Services will be provided for up to two (2) Business Devices used by the number of users indicated in the Quote. 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, and (iii) has installed on it a software agent through which we (or our designated Third Party Providers) can monitor the device.

We will provide support for any software applications that are licensed through us. 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, then if you have a Service Contract in place, our facilitation services will be provided at no additional cost to you.

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

Physical Locations Covered by Services

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

Minimum Requirements / Exclusions

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

- Server hardware must be under current warranty coverage.
- All equipment with Microsoft Windows® operating systems

must be running then-currently supported versions of such software and have all of the latest Microsoft service packs and critical updates installed.

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

Exclusions. Services that are not expressly described in the Quote will be out of scope and will not be provided to Client unless otherwise agreed, in writing, by Allied. Without limiting the foregoing, the following

services are expressly excluded, and if required to be performed, must be agreed upon by Allied in writing:

- Support or programming changes of custom applications, or application development 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.
- 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

Automated monitoring is provided on an ongoing (*i.e.*, 24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our business hours (currently Mon-Sat, 7 AM – 7 PM Central Time, excluding legal holidays and Allied-observed holidays as listed below), unless otherwise specifically stated in the Quote or as otherwise described below.

We will respond to problems, errors, or interruptions in the provision of the Services during business hours in the timeframe(s) described below. Severity levels will be determined by Allied in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; Allied will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

Trouble / Severity	Response Time
Critical / Service Not Available (*e.g.*, all users and functions unavailable)	Response within two (2) business hours after notification.
Significant Degradation (*e.g.*, large number of users or business critical functions affected)	Response within four (4) business hours after notification.
Limited Degradation (*e.g.*, limited number of users or functions affected, business process can continue).	Response within eight (8) business hours after notification.
Small Service Degradation (e.g., business process can	Response within two (2) business days after

continue, one user affected).	notification.
Long Term Project, Preventative Maintenance	Response within four (4) business days after notification.

* All time frames are calculated as of the time that we are notified of the applicable issue / problem by Client through our designated support portal, help desk, or by telephone at the telephone number listed in the Quote. Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts.

Support During Off-Hours/Non-Business Hours: Technical support provided outside of our normal business hours is offered on a case-by-case basis and is subject to technician availability. If Allied agrees to provide off-hours/non-business hours support ("Non-Business Hour Support"), then that support will be provided on a time and materials basis (which is not covered under any Service plan), and will be billed to Client at the following increased hourly rates:

- 2x Standard Rates

All hourly services are billed in 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.

Allied Observed Holidays: Allied observes the following holidays:

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

Fees

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

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, no charge will be incurred if within Pulaski County, AR. Time spent traveling outside of Pulaski County, AR will be billed to you at our then current hourly rates. In addition, you will be billed for all tolls, parking fees, mileage, 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 normal consulting time (or

non-business hours consulting time, whichever is appropriate), calculated at our then-current hourly rates.

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

Standard Billing Rates for work performed outside of a support agreement or fixed fee project.

	Hourly Rates
Work Role	
Partner	$ 200.00
Senior Consultant	$ 200.00
Infrastructure Consultant	$ 150.00
Sr. Support Analyst	$ 125.00
Support Analyst	$ 100.00
Associate Support Analyst	$ 75.00
Minimums*	
Remote Support	6 min
Dispatch/On-site Support/Non-Business Hours	.5 hour

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"). 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 Allied's satisfaction.

The Services will continue through the Initial Term until terminated as provided in the Agreement, the Quote, or as indicated in this Service Guide (the "Service Term").

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, Client will remove, package and ship, at Client's expense and in a commercially reasonable manner, all hardware, equipment, and accessories provided to Client by Allied that were used in the provision of the Services. If you fail to timely return all 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.

Off Boarding

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

- Removal / disabling of monitoring agents 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 Allied
- Removal of credentials from the Environment
- Removal of backup software from the Environment

Unless otherwise indicated in the Quote, our Offboarding service will be billed to you at our then-current hourly rates for a minimum of 16 hours.

Additional Policies

Authenticity

Everything in the managed environment must be genuine and licensed, including all hardware, software, etc. If we ask for proof of authenticity and/or licensing, you must provide us with such proof. All minimum

hardware or software requirements as indicated in a Quote or this Services Guide ("Minimum Requirements") must be implemented and maintained as an ongoing requirement of us providing the Services to you.

Monitoring Services; Alert Services

Unless otherwise indicated in the Quote, all monitoring and alert-type services are limited to detection and notification functionalities only. Monitoring levels will be set by Allied, 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 an Order 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 Allied or its designated third party affiliate may transfer information about the results of processed files, information used for URL reputation determination, security risk tracking, and statistics for protection against spam and malware. Any information obtained in this manner does not and will not contain any personal or confidential information.

Breach/Cyber Security Incident Recovery

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

of the information or applications in, or the structure or integrity of, the managed environment, or (ii) prevents normal access to the managed environment, or impedes or disrupts the normal functions of the managed environment.

Environmental Factors

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

Fair Usage Policy

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

interfere, or may likely interfere, with our ability to provide our services to our other customers.

Hosted Email

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

Hosted Email solutions are subject to acceptable use policies ("AUPs"), and your use of Hosted Email must comply with those AUPs—including ours. In all cases, you agree to refrain from uploading, posting, transmitting or distributing (or permitting any of your authorized users of the Hosted Email to upload, post, transmit or distribute) any prohibited content, which is generally content that (i) is obscene, illegal, or intended to advocate or induce the violation of any law, rule or regulation, or (ii) violates the intellectual property rights or privacy rights of any third party, or (iii) mischaracterizes you, and/or is intended to create a false identity or to otherwise attempt to mislead any person as to the identity or origin of any communication, or (iv) interferes or disrupts the services provided by Allied 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. Allied 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 Allied believes, in its discretion, that Client's email account(s) is/are being used in an improper or illegal manner.

Patch Management

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.

Overview: In order to maintain a balance between minimizing both the risk of unpatched devices and untested software patches, Allied has developed the following process for patch management. Allied approves the patch for release, test the patch for a small group of devices for a set timeframe, then pushes the patch as a general release and finally remediates any devices missing the patch.

Approval & Testing: Allied identifies a select number of workstations for each client that represent as closely as possible the full population of devices and creates the Patch Test Group. Once a patch is released from a software publisher Allied reviews the patch, and if approved, assigns it to the Patch Test Group. The patch is then applied during the clients ordinary maintenance window and Allied will monitor for one week to insure there are no unintended consequences or issues caused by the patch.

General Release: Once testing is complete the approved patch will be scheduled to update on the remaining devices in the clients environment. The patch will be applied during the next maintenance window that the device is available to receive patches.

Remediation: If a workstation or laptop misses three (3) maintenance windows and has patches available then it will be moved into the Daytime Patching Group. On the next day that the device is online patches will be applied to that device silently and without reboot. Once

the patches are applied the device is removed from the Daytime Patch Group.

Allied also performs monthly patch reviews to identify devices that have missing approved patches. Allied then manually remediates the issue so the device can resume normal patch management. All Server patching is remediated manually and never included with the Daytime Patching Group.

Manual Server Patching: Some servers require a manual processes to be run upon reboot. These servers are excluded from normal patch management and are part of a scheduled monthly manual patching ticket. These computer are patched after business hours at a predetermined time that Allied and the client have agreed upon.

Patching Exceptions

Zero Day Patches: While not a common occurrence, software publishers do from time to time release patches for newly discovered vulnerabilities that at the time of release pose a critical threat to IT stability. These are considered zero day vulnerabilities because the threat is real and immediate. During such an occurrence Allied will use Emergency Patching Procedures to rapidly deploy the patch to all clients within as short a time period as required based on the threat of the vulnerability.

Known Issue Exceptions: Some software publishers do not have necessary resources to update their software to keep pace with the development and release schedule of the underlying software that they run on. For this reason some devices may be blocked from update until the needed line of business software is deemed compatible with the newly released components. A good example would be either Oracle Java or Adobe Flash. Both are used as a platform by other software which may not initially support the latest release from Oracle or Adobe.

Patching Update Rhythms

Microsoft: Patches are currently released by Microsoft on the second Tuesday of each month. Allied will review the patches that week and release it the following week to the Test Patching Group. If the patch has no issue in testing it is then placed in General Release the following week and two weeks after “Patch Tuesday”.

Oracle and Adobe: Both Oracle and Adobe release patches and updates on an as needed basis. Allied will review updates for these product each month and evaluates the impact and criticality of the patch. Patches are then deployed using Allied’s Patch Management Process.

Line of Business Updates: Each client works with a different set of program that may be exclusive for their particular industry or vertical market. Allied Works with both the vendor and client to insure as much testing as needed or possible occur before a major line of business release or update is rolled out.

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 Allied 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. Allied cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Allied 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 Allied 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, Allied 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. Allied is not a warranty service or repair center. Allied 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 Allied will be held harmless, and (ii) Allied is not responsible for the quantity, condition, or timely delivery of the Procured Equipment once the equipment has been tendered to the designated shipping or delivery courier.

Business Review / IT Strategic Planning Meetings

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

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

VCTO or VCIO Services

The advice and suggestions provided by us in our capacity as a virtual chief technology or information officer will be for your informational and/or educational purposes only. Allied 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 Allied on Client's corporate records or accounts.

Sample Policies, Procedures.

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

Penetration Testing; Vulnerability Scanning

You understand and agree that security devices, alarms, or other security measures, both physical and virtual, may be tripped or activated during the penetration testing and/or vulnerability scanning processes, despite our efforts to avoid such occurrences. You will be solely responsible for notifying any monitoring company and all law enforcement authorities of the potential for "false alarms" due to the provision of the penetration testing or vulnerability scanning services, and you agree to take all steps

necessary to ensure that false alarms are not reported or treated as "real alarms" or credible threats against any person, place, or property. Some alarms and advanced security measures, when activated, may cause the partial or complete shutdown of the Environment, causing substantial downtime and/or delay to your business activities. We will not be responsible for any claims, costs, fees, or expenses arising or resulting from (i) any response to the penetration testing or vulnerability scanning services by any monitoring company or law enforcement authorities, or (ii) the partial or complete shutdown of the Environment by any alarm or security monitoring device.

No Third Party Scanning

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

Obsolescence

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

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

Licenses

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

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").

Allied 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**: Allied 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 Allied 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, Allied'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.
- **Network disruptions and sundry activity**. Use of the Hosted Services for any activity which affects the ability of other people or systems to use the Hosted Services or the internet is prohibited. This includes "denial of service" (DOS) attacks against another network host or individual, "flooding" of networks, deliberate attempts to overload a service, and attempts to "crash" a host.
- **Distribution of malware**: Intentional distribution of software or code that attempts to and/or causes damage, harassment, or annoyance to persons, data, and/or computer systems is prohibited.
- **Excessive use or abuse of shared resources**: The Hosted Services depend on shared resources. Excessive use or abuse of these shared network resources by one customer may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network performance is prohibited. You are prohibited from excessive consumption of resources, including CPU

time, memory, and session time. You may not use resource-intensive programs which negatively impact other customers or the 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, Allied 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.