Services Guide

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

Throughout this Services Guide, references to "Client," "you," or "your" mean the entity who has accepted a Quote, proposal, service order, statement of work, Master Services Agreement or similar document (electronic or otherwise) from us.

This Services Guide is our "owner's manual" that generally describes all managed services provided or facilitated by Zanacore Technologies ("Zanacore," "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.

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

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

TABLE OF CONTENTS

GENERAL SERVICES

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 you or previous IT service providers.
- Compile an 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 and management 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.

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. The start date for each of the following services will be dependent upon completion of one or more Onboarding Services above and may not be provided until the dependent tasks are completed or scheduled with you. Please direct any questions about start or "go live" dates to your account manager.

MANAGED SERVICES

SERVER MONITORING & MAINTENANCE:

As part of our RMM service, we will monitor and maintain managed servers as follows:

- Software agents installed on 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 and alerting for detected security vulnerabilities
- Secure remote connectivity to the server and collaborative screen sharing
- Monitoring of updates and patches for Windows and supported software
- Asset inventory and server information collection

Event	Server
Hardware Failures	Yes
Device Offline	Yes
Failed/Missing Backup	Yes
Failed/Missing Updates	Yes
Low Disk Space	Yes
Agent missing/misconfigured	Yes

*** Please see Service Level Descriptions sections below for important details.**

WORKSTATION MONITORING & MAINTENANCE:

As part of our RMM service, we will monitor and maintain managed servers as follows:

- 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 and alerting for detected security vulnerabilities
- Secure remote connectivity to the workstation and collaborative screen sharing.
- Monitoring of updates and patches for Windows and supported software.
- Asset inventory and workstation information collection.

Event	Workstation
Hardware Failures	No
Device Offline	No
Failed/Missing Backup	No
Failed/Missing Updates	Yes
Low Disk Space	Yes
Agent missing/misconfigured	Yes

*** Please see Service Level Descriptions sections below for important details.**

WINDOWS SERVER BACKUP MANAGEMENT:

Windows server backup is a basic backup and recovery solution.

- Monitoring backup status, such as successful completion of backup, failure errors, and destination free space restrictions/limitations.
- Full Daily Image Backups
- Yearly Test Restores
- Server recovery from backup is included unless the failure or data loss is caused by a security related event, 1st party error, or any request not related to data loss.
- Limited to Physical Windows Servers and virtual machines running on the Physical Servers
- No offsite replication included

Note: Full Recovery of backups using Windows Server Backups could take up to 48 hours. Other backup solutions are available for enhanced features, including offsite replication, non-windows servers, faster recovery time, etc.

REMOTE HELPDESK:

- Remote Helpdesk support is available 24/7 for covered devices.
- Users can request Helpdesk support via chat session or phone. E-Mail requests are also available but should only be used for low priority requests, due to slower response time.
- A tiered support structure and escalation process ensures effective resolution of issues.
- Support is limited to Tier 1 and basic Tier 2 issues as determined by the Help Desk team. All other requests will be out of scope and escalated to our Tier 2 support team.
- The Helpdesk will not perform actions that would result in billable charges, such as purchasing software licenses.
- Support for critical networking equipment to mitigate network outages is not provided by the Helpdesk. Such requests will be escalated accordingly.

REACTIVE SUPPORT:

- Remote and onsite support is provided during normal business hours for managed devices.
- Onsite support is scheduled and provided at the sole discretion of Zanacore.
- Reactive support is limited to addressing issues for existing systems that were previously functioning and making minor changes to existing systems, such as adjusting user permissions.

AFTER-HOURS EMERGENCY SUPPORT:

- After-hours emergency support is provided exclusively for managed devices.
- This support is only available for issues that prevent multiple users from performing their job functions, or a critical user from performing a job function that affects most users (i.e. running payroll).

- For critical service outages, the Client must notify Zanacore through the after-hours emergency voicemail service at 678-822-5818. Notifications received through any other means may result in a delayed response.
- Critical alerts from Zanacore Monitoring systems will be addressed the following morning unless Zanacore determines that emergency after-hours support is warranted.

SMALL PROJECT LABOR:

We understand that small needs arise. Projects estimated to require two (2) hours or less will normally be handled as 'Small Projects' without separate project fees, providing you with efficient and cost-effective support.

- Small Project labor is defined as any work not directly related to resolving an issue with existing covered components of the system.
- Small Project labor generally includes basic tasks such as installing new software or hardware devices and performing minor version upgrades.
- Small Projects typically involve work requiring less than 2 hours of labor. We retain sole discretion to determine what qualifies as a Small Project.
- Total labor for all Small Projects are limited to 4 hours per month.

Note: New User or Computer setups are not included under Small Projects.

FLAT-FEE SETUP FOR NEW USERS OR WORKSTATIONS:

Setting up a computer for an employee can take 2-4 hours on average. We have a fixed charge for setting up computers, and for new users, with or without a computer. Repurposing an existing computer for a different user is also considered a computer setup and incurs the fixed setup charge.

The following restrictions apply:

- Setup of computers are limited to two (2) devices per month unless otherwise approved in advance by us.
- This service is not available for used or remanufactured computers.
- New/replacement computers must be business-grade machines (not home) from a major manufacturer like Dell, HPE, Lenovo, or other approved vendor.

The current flat rate for PC Setups is: $150/each

Note: New User and Computer setups need to be scheduled. We require that you give us at least 3 business days' notice before the user or computer is needed.

STANDARD LABOR RATES:

Client will be charged at the hourly labor rates below for projects and any requested support which is otherwise excluded from the Services. These rates are subject to change without notice.

Contract Type	Remote	Onsite
Standard Rates	$200	$250
NetWatch	$200	$250
NetShield	$175	$200
NetGuard	$150	$175

Note: After hours will be billed at 1.25x the Standard Labor Rate

ENDPOINT ANTIVIRUS & MALWARE PROTECTION:

We provide Antivirus and malware protection for managed devices such as laptops, desktops, and servers from our designated Third Party Providers.

Software agents are installed on covered devices to protect against malware and intruder access. These are used in coordination with other endpoint security layers and security solutions to form a comprehensive defense strategy.

Typical functions of Endpoint Protection include:

- Detection of unauthorized behaviors of users or applications.
- Blocking of suspicious actions before execution.
- Protection against file-based and fileless scripts, as well as malicious JavaScript, VBScript, PowerShell, macros and more.
- Whitelisting for legitimate scripts.

*** Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**

ENDPOINT DETECTION & RESPONSE (EDR):

EDR tools for managed devices such as laptops, desktops, and servers from our designated Third Party Provider offer deep visibility into endpoint activities, helping to detect and respond to threats more effectively than traditional antivirus software.

- Detects threats such as malware, ransomware, and other malicious activities.
- EDR can automatically respond to threats by isolating infected devices, terminating malicious processes, and quarantining harmful files mitigating threats before they spread.
- Collects and analyzes data from endpoints to identify patterns and indicators of compromise.
- Continuously monitor endpoint activities, including user behavior, system logs, and network traffic, to detect any suspicious actions.
- Advanced analytics and intelligence to identify both known and novel threats in real-time

*** Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**

ADVANCE SECURITY SOLUTION (XDR / MDR / SOC):

Implementation and facilitation of top-tier XDR / MDR solutions from our designated Third Party Providers.

- Real time and continuous (24x7) monitoring and threat hunting by live team of security engineers (SOC).
- Automated correlation of data across multiple system logs including but not limited to Office 365, EDR, Antivirus, and others (SIEM), to provide insights into potential threats.
- Security team (SOC) can quickly launch response protocols, reducing the impact of security incidents.
- Provides extended malware sweeping, hunting, and investigation including on-demand endpoint isolation, and advanced threat intelligence.

*** Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**

ENDPOINT PRIVILEGE MANAGEMENT:

Endpoint Privilege Management improves security by managing and controlling administrative privileges on endpoints, ensuring that users operate with the least privilege necessary. It helps meet compliance goals and is essential for most cyber insurance coverage, as removing admin rights can avoid or limit the impact of many system vulnerabilities.

- Automates the elevation of approved applications and other administrative tasks reducing the need for users to have constant administrative rights
- Enhances User Account Control (UAC) settings, making it easier to audit and remediate machines with improper UAC configurations.

END USER SECURITY AWARENESS TRAINING:

Implementation and facilitation of a security awareness training solution from an industry-leading third party solution provider.

- Online training videos are sent via monthly email to all employees. Includes quizzes to verify employee retention of training content.
- Simulated phishing email campaigns, designed to test and educate employees about security threats, are sent monthly by e-mail.

Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.

WINDOWS UPDATES & 3RD PARTY PATCHING:

We will keep all managed Windows devices and approved 3rd party software applications current with critical patches and updates ("Patches") as per our Patch Policy.

- Deploy, manage, and monitor the installation of approved Windows service packs, and security updates as deemed necessary on all applicable managed devices.
- Deploy, manage, and monitor the installation of approved updates for approved 3rd Party applications including tools provided by us.
- Major Version upgrades for Windows and 3rd party applications are out of scope.
- Updates and patching for any applications not on our Approved 3rd party application list are out of scope

Please note: 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.

Zanacore Patch Policy: (for Windows Desktops/Laptops)

- Windows patches are typically approved for installation 2 weeks after being released by Microsoft.
- Windows device drivers, Preview Patches, and Patches for Preview versions of Windows are not approved automatically.
- Included 3rd party patches are approved for installation as soon as our patching tools detect update availability from the vendor.
- Patches are downloaded and installed on a daily basis.

Approved 3rd Party Applications for Patching:

- 7-zip
- Adobe Acrobat Reader DC
- Adobe Air
- FileZilla Client
- Foxit PDF Reader
- Google Chrome
- Java Runtime Environment
- Microsoft .NET Desktop Runtime
- Microsoft Office (Click-to-run)
- Mozilla Firefox
- Notepad ++
- PuTTY
- Zoom

Please Note: Additional 3rd party apps may be included in our patching services if approved by Zanacore. Specific patching may be excluded if requested by you.

DARK WEB MONITORING:

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

Domains requested by you will be continuously monitored by human and machine-powered tools to determine if any credentials using those domain names are located on the dark web. If compromised credentials are found, they are reported to us, and we 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. Client acknowledges this service is provided by Zanacore only as an aid to reduce the risk of damage caused by breached credentials, and further acknowledges that responsibility for management and security of website logon credentials resides solely with you and your employees.

EMAIL SECURITY AND SPAM FILTERING SERVICES:

Implementation and facilitation of an email spam protection solution from our designated Third Party Provider.

- Identification and blocking of spam, viruses, phishing attempts, and other malicious content.
- Intelligent message handling to reduce false positives and ensure delivery of legitimate emails.
- Implementation of customizable filtering policies to align with your security and compliance requirements.
- Access to detailed analytics for transparency and monitoring of filtered emails.
- Secure quarantine of potentially harmful or suspicious emails for user review.
- Safe previewing tools for quarantined emails to mitigate risks without compromising security.
- Seamless integration with existing email platforms, including Microsoft 365 and Google Workspace, for an added layer of email protection.

Please note: From time to time the service may filter email that is not SPAM or junk mail, or may block email from legitimate sources. You are advised to periodically search the filtered email folder to ensure that relevant emails are not being filtered improperly, and notify us if the SPAM filter settings require adjustment.

Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.

FIREWALL SOLUTION:

- We will provide a firewall configured for your organization's specific bandwidth, remote access, and required licenses.
- Monitor, update (software/firmware), and support firewall appliance.
- Firewall appliance is subject to "Hardware as a Service" terms and conditions located in this Guide.
- Firewall appliance must be returned to Zanacore upon the termination of service. Client will be responsible for missing or damaged (normal wear and tear excepted) appliance.

Note: This service only applies to Zanacore provided Firewall solution. If you elect to use your own firewall solution, then the services above are out of scope.

WI-FI SOLUTION:

We provide our approved Wireless Solution on your premises to provide bandwidth in all areas requiring wireless network coverage, as agreed upon with you.

- We will Monitor, Update, and Support the wireless solution.
- You understand and acknowledge that some end-user devices may not connect or perform well on the wireless network. In those cases, we will provide support on a best effort basis only.

Note: This service only applies to Zanacore approved Wi-Fi solution. If you elect to use your own Wi-Fi solution, then the services above are out of scope.

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.
- Provide recommendations for business technologies.
- Participate in scheduled technology review meetings.
- Make recommendations for improving technology usage and services.

NETWORK TECHNOLOGY ALIGNMENT:

Each client is assigned a Technology Alignment Manager (TAM) to maintain alignment of client systems with our best practices.

- The TAM is the primary point of contact for Technical Questions, major changes to the environment, or Issues related to Security.
- Maintain technology documentation.
- Create company-specific standards and best practices.
- Run periodic alignment scans to identify gaps and correct identified issues.

SOFTWARE PASSTHROUGH LICENSING:

We provide Software Passthrough Licensing services to facilitate the acquisition and management of software licenses on your behalf. This service streamlines the license procurement process.

1. License Procurement

We purchase software licenses from third-party vendors, including but not limited to Adobe, Microsoft Office 365, and Veeam, on your behalf. These licenses are provided under the terms established by the respective software vendors.

2. Billing and Terms of Service

Billing and terms of service for passthrough licenses are governed by the vendor's policies and may differ from our internal billing structure. For example, some products may be billed in arrears while others may be billed in advance of the service term. You acknowledge and agree that payments, renewal terms, and other financial obligations related to software licenses are determined by the vendor.

3. Quantity and Pricing

- Our billing is based on the actual licenses on record with the vendor. You are responsible for notifying us of any discrepancies for license usage.

- Pricing is subject to change based on the software vendor pricing, policies, market conditions, or licensing agreements.

4. Additional Vendor Products & Services

From time to time you may receive additional products or services from a vendor included in the original quote. These additions do not require a new quote from us, as they already fall under the direct engagement between you and that vendor.

5. Refunds and Credits

Any requests for refunds or credits related to software licenses are subject to the vendor's policies. We do not issue refunds or credits for passthrough licensing.

*** Please see Software Licensing / EULA**

DOMAIN NAME REGISTRATION SERVICES:

We may provide Domain Name Registration services to facilitate the acquisition and management of Domain Names on your behalf. This service streamlines the domain registration process.

If you register, renew or transfer a domain name through us, we will submit the request to our third party domain name service provider (the "Registrar") on your behalf. Our sole responsibility is to submit the request to the Registrar. We are not responsible for any errors, omissions or failures of the Registrar. Your use of domain name services is subject to the applicable legal terms of the Registrar. You are responsible for closing any account with any prior reseller or registrar for the requested domain name, and you are responsible for responding to any inquiries sent to you by the Registrar.

*** Please see Offboarding**

OFFICE 365 BACKUP:

Implementation and facilitation of an Office 365 Backup solution from our designated Third Party Provider. This service includes:

- Monitoring backup status, such as successful completion of backup or failure errors.
- Perform daily automated backups to capture relevant changes across Microsoft 365 applications, including Exchange, OneDrive, and SharePoint.
- Recovery from backup is included unless the failure or data loss is caused by a security related event, 1st party error, or any request not related to data loss.
- Yearly Test restores

Billing for this service is based on the number of licensed O365 users. By default, all licensed users are backed up, including new users that are added.

Note: Speed of data recovery is limited by backup vendor and Microsoft. Large restores can take multiple days to complete.

POLICIES AND CONDITIONS

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 only include technology assets (such as computers, servers, and networking equipment) owned by the Client's organization. As an accommodation, Zanacore 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.

All of Zanacore's managed service tools will be fully supported, regardless of who acquired the license. However, for line-of-business tools or applications (e.g. QuickBooks), support will be provided on a best-effort basis, offering only Level 1 support, which includes basic troubleshooting and guidance. More complex issues may require further escalation or vendor-specific support.

If we are unable to remediate an issue with a line-of-business tool, 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 line-of-business tools ("Service Contract"). If you request that we facilitate technical support for line-of-business tools and if you have a Service Contract in place, our facilitation services will be provided at no additional cost to you.

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

PHYSICAL LOCATIONS COVERED BY SERVICES

Services will be provided remotely unless, in our discretion, we determine that an onsite visit is required. Zanacore 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 "Professional" versions of such software and have all the latest Microsoft service packs and critical updates installed.
- 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 servers must be connected to working UPS devices.
- Data Recovery activity 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 Zanacore. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by Zanacore in writing:

- Customization of third party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Equipment which, in the judgement of Zanacore, has exceeded its normal life expectancy for reliable service. Such equipment may be excluded from the Services.
- Data/voice wiring or cabling services of any kind.
- Replacement of battery backup devices and batteries.
- Equipment relocation.
- The cost to bring the managed environment up to these minimum requirements (unless otherwise noted in the Quote).
- The cost of 3rd party repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.
- Support for phone systems unless specifically included elsewhere in the Scope of Services.
- On-site service work at any location other than the Primary Business Locations.
- Repair service for failed printers, monitors, thin-clients, or any other peripheral equipment connected to computers. Zanacore responsibility for this equipment is limited to diagnostic tests, replacement purchase assistance, and coordination with manufacturers for repair services.
- Training services of any kind, other than specifically included elsewhere in this agreement.

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 M-F, 8:30 AM – 5:30 PM Eastern Time, excluding legal holidays and Zanacore-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 Zanacore in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; Zanacore 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	Priority	NetGuard Response Time (in hours) *	Non-NetGuard Response Time (in hours) *
Critical Service Not Available (affecting all organization users – no work around available)	Critical	Within 2 Hours	Within 8 Business Hours
Significant Degradation of Service (majority of users or business critical functions affected – workaround available)	High	Within 4 Business Hours	Within 8 Business Hours
Limited Degradation of Service (limited users or functions affected, business process can continue – workaround available)	Medium	Within 8 Business Hours	Within 8 Business Hours
Minimal Degradation of Service (business process can continue)	Low	Within 8 Business Hours	Within 8 Business Hours

* Response time is defined as: The elapsed time for Zanacore to have a live person triage the issue and open a support ticket. All issues must be reported to us by the 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 Zanacore 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 and will be billed to Client at the hourly rates specified in the Quote.

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.

ZANACORE-OBSERVED HOLIDAYS:

Zanacore observes the following holidays:

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

SERVICE CREDITS:

Our service level target is 90% as measured over a calendar month ("Target Service Level"). If we fail to adhere to the Target Service Level and Client timely brings that failure to our attention in writing (as per the requirements of our Master Services Agreement), then Client will be entitled to receive a pro-rated service credit equal to 1/30 of that calendar month's recurring service fees (excluding hard costs, licenses, etc.) for each day on which the Target Service Level is missed. Under no circumstances shall credits exceed 30% of the total monthly recurring service fees under an applicable Quote.

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, time spent traveling one-way will be billed to you at the hourly onsite rates specified in the Quote. 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 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.

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 our 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, 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 Zanacore "as a service." If you fail to timely return all such equipment to us, or if the equipment is returned to us damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

OFFBOARDING

Subject to the requirements in the MSA, we may begin off-boarding our tools and services before the end the term of the services agreement. We encourage you to transition to replacement tools and services during this offboarding period to minimize negative impact to your operations or security protection. We will make a best effort to cooperate with any new service provider you specify to help make a smooth transition to their services.

Services and tools we will offboard from your system include one or more of the following:

- Removal / disabling of monitoring and management agents in the Environment.
- Removal / disabling of endpoint protection software and 3rd party security management tools from the Environment.
- Removal of any 3rd party licenses (i.e. Microsoft 365, SPLA, Adobe, etc.) provided by Zanacore (unless the licenses are being transferred to your incoming provider or your direct billing)
- Removal of our management credentials from the Environment.
- Removal of our backup software from the Environment.
- Removal of Zanacore provided HaaS equipment (firewall, servers, backup appliances, WiFi access points, etc.) from the Environment

Offboarding Domain Services:

If you have domains registered with our domain registration vendor, then you acknowledge that you are solely responsible for managing your account, including configuration of domain auto-renewals and billing payment methods. We recommend you transfer your domain registration to another registrar as soon as possible. If you request our support to assist with any issues related to your account or domain names (i.e. lost credentials, expired domain names, expired payment methods, etc.), you will be billed at our standard hourly rates.

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 Zanacore, 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

You understand and agree that no security solution is one hundred percent effective, and any security paradigm may be circumvented and/or rendered ineffective by certain Viruses or malware, such as ransomware or rootkits, that were previously unknown to the manufacturers of the software solution, and/or which are purposely or intentionally downloaded or installed onto your System. You are strongly advised to refrain from downloading files that are sent by unknown users, and/or users or files whose origination cannot be verified. We do not warrant or guarantee that all Viruses and malware will be capable of being avoided or removed, or that all forms of Viruses and malware will be timely detected or removed, or that any data corrupted or encrypted by Viruses or malware will be recoverable. 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.

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 Zanacore 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. Zanacore 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 Zanacore 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 Zanacore 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. Zanacore cannot and does not warrant that data corruption or loss will be avoided, and

Client agrees that Zanacore shall be held harmless if such data corruption or loss occurs. **Client is strongly advised to keep a local backup of all stored data to mitigate against the unintentional loss of data.**

PROCUREMENT

Equipment and software procured by Zanacore on Client's behalf ("Procured Equipment") must be paid in full at the time of order placement. 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, Zanacore 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. Zanacore is not a warranty service or repair center. Zanacore 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 Zanacore will be held harmless, and (ii) Zanacore 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.

ADVICE & INSTRUCTIONS

Suggestions and advice rendered to Client are provided in accordance with relevant industry practices and based on Client's specific needs. By suggesting a particular service or solution, Zanacore is not endorsing any manufacturer or service provider. Zanacore is not a warranty service or repair center, and does not warrant or guaranty the performance of any third party service or solution.

VCTO OR VCIO SERVICES

The advice and suggestions provided by us in our capacity as a virtual chief technology or information officer (if applicable) will be for your informational and/or educational purposes only. Zanacore 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 Zanacore 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.

UNSUPPORTED CONFIGURATION ELEMENTS OR SERVICES

If You request a configuration element (hardware or software) or hosting service in a manner that is not customary for Us to support, We may designate the element or service as "unsupported," "non-standard," "best efforts," "reasonable endeavor," "one-off," "EOL," "end of support," or with like term in the service description (an "Unsupported Service"). We make no representation or warranty whatsoever regarding any Unsupported Service, and You agree that We will not be liable to You for any loss or damage arising from the provision of an Unsupported Service. Deployment and service level guarantees shall not apply to any Unsupported Service.

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.

SOFTWARE LICENSING / EULA

All software provided to you by or through Zanacore ("Software"), is licensed, not sold, to you. In addition to any Software-related requirements described in Zanacore's Master Services Agreement, Software may also be subject to Third Party Provider end user license agreements (EULAs), acceptable use policies (AUPs), and other restrictions. **You should assume that all Software has an applicable EULA and/or AUP to which your authorized users and you must adhere.**

If the acceptance of an End User Agreement is required for you to receive any Services, then you hereby grant us permission to accept the applicable agreement(s) on your behalf. End User Agreements may contain service levels, warranties and/or liability limitations different from those contained in this Agreement. You agree to be bound by the terms of all applicable End User Agreements.

For your convenience the Third Party Providers typically used by Zanacore for delivery of our services, along with their governing terms and conditions, are listed on the Schedule of Third-Party Services. This list is not intended to be a complete list of all 3rd party services, and there will be 3rd party services with EULAs accepted on your behalf which are not on the list. If you have any questions or require a copy of a specific EULA or AUP, please contact us.

You can find the Schedule of Third-Party Services on our website:

https://www.zanacore.com/terms

SCHEDULED MAINTENANCE

Zanacore's routine maintenance, which includes tasks such as restarting servers and workstations to ensure optimal performance and security, will take place daily between 10 PM and 5 AM. During this time, you may experience brief periods of downtime.

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 may be charged a non-refundable and non-disputable fee from the VoIP provider.**

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").

Zanacore 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**: Zanacore has a zero tolerance policy for the sending of unsolicited commercial email ("SPAM"). Use of a Hosted Service to transmit any unsolicited commercial or unsolicited bulk e-mail is prohibited. You are not permitted to host, or permit the hosting of, sites or information that is advertised by SPAM from other networks. To prevent unnecessary blacklisting due to SPAM, we reserve the right to drop the section of IP space identified by SPAM or denial-of-service complaints if it is clear that the offending activity is causing harm to parties on the Internet, if open relays are on the hosted network, or if denial of service attacks are originated from the hosted network.
- **Internet Relay Chat (IRC)**: The use of IRC on a hosted server is prohibited.
- **Open or "anonymous" proxy**: Use of open or anonymous proxy servers is prohibited.
- **Crypto mining:** Using any portion of the Hosted Services for mining cryptocurrency or using any bandwidth or processing power made available by or through a Hosted Services for mining cryptocurrency, is prohibited.
- **Hosting spammers**: The hosting of websites or services using a hosted server that supports spammers, or which causes (or is likely to cause) our IP space or any IP space allocated to us or our customers to be listed in any of the various SPAM databases, is prohibited. Customers violating this policy will have their server immediately removed from our network and the server will not be reconnected until such time that the customer agrees to remove all traces of the offending material immediately upon reconnection and agree to allow Zanacore 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, Zanacore security measures or the security measures of another entity's network or electronic communications system, whether or not the intrusion results in the corruption or loss of data, is prohibited. This includes but is not limited to accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other networks, as well as the use or distribution of tools designed for compromising security such as password guessing programs, cracking tools, or network probing tools.
- **IP infringement**: Use of a Hosted Service to transmit any materials that infringe any copyright, trademark, patent, trade secret or other proprietary rights of any third party, is prohibited.
- **Collection of personal data**: Use of a Hosted Service to collect, or attempt to collect, personal information about third parties without their knowledge or consent is prohibited.
- **Disruptive Activity:** Use of the Hosted Services for any activity which affects the ability of other people or systems to use the Hosted Services or the internet is prohibited. This includes "denial of service" (DOS) attacks against another network host or individual, "flooding" of networks, deliberate attempts to overload a service, and attempts to "crash" a host.
- **Distribution of malware**: Intentional distribution of software or code that attempts to and/or causes damage, harassment, or annoyance to persons, data, and/or computer systems is prohibited.
- **Excessive use or abuse of shared resources**: The Hosted Services depend on shared resources. Excessive use or abuse of these shared network resources by one customer may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network performance is prohibited. You are prohibited from excessive consumption of resources, including CPU time, memory, and session time. You may not use resource-intensive programs which negatively impact other customers or the 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, 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.