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, telecommunications services and other services provided or facilitated by Zella Technologies ("Zella," "we," "us," or "our"); however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "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.

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 Audit / Diagnostic Services

If an Initial Audit / Diagnostic Services are listed in the Quote, then we will audit your managed information technology environment (the "Environment") to determine the readiness for, and compatibility with, ongoing managed services. Our auditing services are comprised of, but not limited to, 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
- Security vulnerability check
- Backup and disaster recovery solution audit
- Speed test and ISP audit
- Print output audit
- Office phone 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If deficiencies are discovered during the auditing process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and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.

Managed IT Onboarding Services

If onboarding services are listed in the Quote, then one or more of the following services will be provided to you.

- Uninstall any monitoring tools or other software installed by previous IT consultants. (If the uninstall file(s) and key(s)/code(s) are provided)
- Compile a full inventory of all protected servers, workstations, and laptops.
- Uninstall any previous virus protection and install our managed antivirus application. (If the uninstall file(s) and key(s)/code(s) are provided)
- Install remote support access application on each managed device to enable remote support.
- Configure patch management application and check for missing security updates.
- Uninstall unsafe applications or applications that are no longer necessary.
- Optimize device performance including disk cleanup, antivirus, and spyware scans.
- Review firewall configuration and other network infrastructure devices.
- Review status of battery backup protection on all devices.
- Stabilize network and assure that all devices can securely access the network.
- Review and document current server configuration and status.
- Determine existing backup strategy and status; prepare backup options 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.
- Configure MFA system for the managed environment.
- Configure MDM system for the managed environment.
- Configure ESG for the managed environment.
- Configure the least privileged access system for the managed environment.
- Configure Advanced DNS Protection for the managed environment.
- Configure SaaS Alerts for the managed environment.
- Configure user awareness training for the managed environment.
- Configure backup services for the managed environment.
- Configure DMARC services for the managed environment.
- Configure network monitoring tools for 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 on an ongoing basis and, unless otherwise indicated in a Quote, are billed to you monthly. Ongoing services generally begin upon the completion of onboarding services; therefore, any delays or interruptions to the onboarding services may delay the commencement of ongoing/recurring services. If any delays exceed thirty (30) days past the acceptance date on the quote, ongoing services will begin.

Managed IT/Cyber Services

The following Services, if listed in the Quote, will be provided to you.

<table>
<tr><th>SERVICES</th><th>GENERAL DESCRIPTION</th></tr>
<tr><td>Remote Monitoring and Management</td><td>Software agents installed in Covered Equipment (defined below) report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.
Includes capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD partitions, not external devices such as USB or mapped drives)
Includes routine operating system inspection and cleansing to help ensure that disk space is increased before
Review and installation of updates and patches for supported software
In addition to the above, our remote monitoring and management service will be provided as follows:<table><tr><th>Event</th><th>Server</th><th>Workstation</th></tr><tr><td>Hardware Failures</td><td>Yes</td><td>No</td></tr><tr><td>Device Offline</td><td>Yes</td><td>No</td></tr><tr><td>Missing MSP Tools</td><td>Yes</td><td>Yes</td></tr><tr><td>Failed/Missing Backup (If covered by Zella’s Backup Solution)</td><td>Yes</td><td>No</td></tr><tr><td>Failed/Missing Updates (Per the update/patch policy below)</td><td>Yes</td><td>Yes</td></tr><tr><td>Missing Endpoint Protection/AV</td><td>Yes</td><td>Yes</td></tr><tr><td>Low Disk Space</td><td>Yes</td><td>Yes</td></tr><tr><td>Agent missing/misconfigured</td><td>Yes</td><td>Yes</td></tr><tr><td>Excessive Uptime</td><td>Yes</td><td>No</td></tr></table></td></tr>
<tr><td>Remote Helpdesk</td><td>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 solutions.</td></tr>
<tr><td>Remote Infrastructure Maintenance / Zella Support</td><td>Configuration, monitoring, and preventative maintenance services provided for the managed IT infrastructure
If remote efforts are unsuccessful then Zella will dispatch a technician to the Client’s premises to resolve covered incidents (timing of onsite support is subject to technician availability and scheduling. Onsite services are billable)</td></tr>
<tr><td>Backup Monitoring</td><td><u>Only applies for Zella’s Backup Solution and does not apply to any customer supplied backup solution.</u>
Monitors backup status for certain backup applications then-installed in the managed environment, such as successful completion of backup, failure errors, and destination free space restrictions/limitations.
Helps ensure adequate access to Client’s data in the event of loss of data or disruption of certain existing backup applications.
<u>Note</u>: Backup monitoring is limited to monitoring activities only, and is not a backup and disaster recovery solution.</td></tr>
</table>

Backup and Disaster Recovery	• 24/7 monitoring of backup system, including offsite backup, offsite replication, and an onsite backup appliance or NAS ("Backup Appliance") • Troubleshooting and remediation of failed backups • Preventive maintenance and management of imaging software • Firmware and software updates of backup appliance • Problem analysis by the network operations team • Monitoring of backup successes and failures • Annual recovery verification Backup Data Security: All backed up data is encrypted in transit and at rest in 256-bit AES encryption. All facilities housing backed up data implement physical security controls. Backup Retention: Backed up data will be retained based on the retention plan accepted by the customer. Offsite backups/replications are to a single zone. Offsite backups are not backed up or replicated to another zone. Customer can request a quote for multi-zone offsite backup/replication if needed. Backup Alerts: Backup Portal will be configured to inform of any backup failures. Recovery of Data: If you need to recover any of your backed up data, then the following procedures will apply: • Service Hours: Backed up data can be requested during our normal business hours, which are currently Monday to Friday 8 am to 5 pm CST. • Request Method. Requests to restore backed up data should be made through one of the following methods: ○ Email: support@zellatech.com ○ Web-portal: https://support.zellatech.com ○ Telephone: 985-520-4824 • Restoration Time: We will endeavor to restore backed up data as quickly as possible following our receipt of a request to do so; however, in all cases data restoration services are subject to technician availability. Generally, we can restore between 0 and 100MB of data within 4 hours of your request, and 100 MB to 500 MB within 8 hours of your request. Data restoration exceeding 500 MB will be handled in accordance with technician availability. SLA applies to all request. • At no time are we responsible for the integrity of backups, recoverability, time to recover and/or the security of the backups.
Updates & Patching	• Remotely deploy updates (e.g., x.1 to x.2), as well as bug fixes, minor enhancements, and security updates as deemed necessary on all managed hardware. • Perform minor hardware and software installations and upgrades of managed hardware. • Perform minor installations (i.e., tasks that can be performed remotely and typically take less than thirty (30) minutes to complete). • Deploy, manage, and monitor the installation of approved service packs, security updates and firmware updates as deemed necessary on all applicable managed hardware. • Updates and Patches only apply to Microsoft OS Updates/Patches and the OS must be licensed and covered by Microsoft.
Block of Hours / Allocated Consulting Hours	If you purchase one or more blocks of technical support or consulting hours from Zella, then we will provide our professional information technology consulting services to you from time to time on an ongoing, "on demand" basis ("Services"). The specific scope, timing, term, and pricing of the Services (collectively, "Specifications") will be determined between you us at the time that you request the Services from us. You and we may finalize the Specifications (i) by exchanging emails confirming the relevant terms, or (ii) by you agreeing to an invoice, purchase order, or similar document we send to you that describes the Specifications (an "Invoice"), or in some cases, (iii) by us performing the Services or delivering the applicable deliverables in conformity with the Specifications.

	If we provide you with an email from billing@zellatech.com or an Invoice that contains details or terms for the Services that are different than the terms of than the Quote, then the terms of the email or Invoice (as applicable) will control for those Services only. A Service will be deemed completed upon our final delivery of the applicable portions of Specifications unless a different completion milestone is expressly agreed upon in the Specifications ("Service Completion"). (For example, sales of hardware will be deemed completed when the hardware is delivered to you; licensing will be completed when the licenses are provided to you, etc.) Any defects or deviations from the Specifications must be pointed out to us, in writing, within ten (10) days after the date of Service Completion. After that time, any issues or remedial activities related to the Services will be billed to you at our then-current hourly rates. All hardware sales are final and non-refundable once the quote is accepted. Unless we agree otherwise in writing, Services will be provided only during our normal business hours, which are currently 8 – 5 PM Central Time. Services provided outside of our normal business hours are subject to increased fees and technician availability and require your and our mutual consent to implement. The priority given to implementing the Services will be determined our reasonable discretion, considering any milestones or deadlines expressly agreed upon in an invoice or email from Zella. If no specific milestone or deadline is agreed upon, then the Services will be performed in accordance with your needs, the specific requirements of the job(s), and technician availability.
Firewall Solution **(firewall appliance provided by Zella)**	• Provide firewall configured for your organization's specific bandwidth, remote access, and user needs. • Helps to prevent unauthorized outsiders from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access. • Firewall appliance must be returned to Zella upon the termination of Services.
Firewall Solution **(firewall appliance provided / purchased by Client)**	• Monitors, updates (software/firmware), and supports Client-supplied firewall appliance. (Customer must maintain an active support/software subscription with the manufacture and updates are subject to the support/software subscription with the manufacture.)
Email Security Gateway (ESG)	• Managed email protection from phishing, business email compromise (BEC), SPAM, and email-based malware. • Protection against social engineering attacks like whaling, CEO fraud, business email compromise or W-2 fraud. • Protects against newly registered and newly observed domains to catch the first email from a newly registered domain. • Protects against display name spoofing based on a list of "VIP" users provided by the customer. • Protects against "looks like" and "sounds like" versions of domain names. • AI learning of user's email habits. • Portal to release, white-list and black-list senders. • Licensed per Mailbox
End User Security Awareness Training	• Licensed per User. • Online, on-demand training videos. • Online, on-demand quizzes to verify employee retention of training content. • Baseline testing to assess the phish-prone percentage of users; simulated phishing email campaigns designed to educate employees about security threats. • All users are required to complete weekly micro-quizzes and annual quizzes.
Hardware as a Service (HaaS)	• Provision and deployment of designated hardware (*see* the Quote or other applicable schedule for complete hardware list – "HaaS Equipment") • Installation of HaaS Equipment. • Repair/replacement of HaaS Equipment (*see below for additional details*). • Technical support for HaaS Equipment. • Periodic replacement of HaaS Equipment (*see below for additional details*). • On-site is billable.

Two Factor Authentication/Multi-Factor Authentication (MFA)	• Advanced two factor authentication with advanced admin features. • Secures on-premises and cloud-based applications that support SAML based on customer request. • Permits custom access policies based on role, device, location. • 2FA login for workstations and servers. • Single Sign-On: Single sign-on grants authorized employees or users access to applications with a single set of login credentials, based on a user's identity and permission levels. Single sign-on relies on SAML (Security Assertion Markup Language), a secure, behind-the-scenes protocol, to authenticate users to cloud, mobile, legacy, and on-premise apps.
Password Manager	• Password Vault: Securely store and organize passwords in a secure digital location accessed through your browser or an app. • Password Generation: Generate secure passwords with editable options to meet specific criteria. • Browser App: Browser extension permits easy access to all of your passwords. • Smart-Phone App: Mobile phone app enables access to your vault and stored information on your mobile device. • *Only covers a FULL user and is not included for any other Managed Cyber Plans.

New / Replacement Workstations & or User Onboarding	Per device and/or Per User fee for setup of new workstations/users, or replacement of existing workstations/users.
	• Fee covers:
	  ○ New computers or users / additional computers or users added during the term of the Quote;
	  ○ Replacement of existing computers that are four (4) or more years old (as determined by the manufacturer's serial number records);
	  ○ Replacement of existing computers that lost/stolen or irreparably damaged and/or out of warranty but not yet four years old;
	
	The following restrictions apply:
	• If Zella's Automation is not used, customer will be billed hourly.
	• Upgrades or installs of new or replacement computers are limited to four (4) devices per month unless otherwise approved in advance by Zella;
	• This service is not available for used or remanufactured computers; and,
	• New/replacement computers must be business-grade machines (not home/consumer) from a major manufacturer like Dell, HPE, or Lenovo.
	• Additional Fees may apply if workstations are not ordered from Zella.

Wi-Fi Services	• Zella will install at the Client's premises Wireless Access Points to provide a bandwidth of at least 10Mbps (download) in all areas requiring wireless network coverage, as agreed upon by Zella and Client. • Onsite and configuration services will be billed to the customer. • Zella will provide the hardware as a rental to the customer. • Zella will maintain, supervise, and manage the wireless system, including hardware and software on a per-device monthly fee. • Installed equipment will be compatible with the then-current industry standards. • Zella will provide remote support services during normal business hours to assist with device connectivity issues. (Support services will be provided on a "best efforts" basis only, and Client understands that some end-user devices may not connect to the wireless network, or they may connect but not perform well). • Client must purchase a Wifi Survey and Design or performance, coverage and support will be a best-effort only. • Wi-Fi Services only apply to Wi-Fi access points that are rented from Zella Technologies.
	• Perform a cybersecurity assessment under NIST CSF using the NIST Risk Management Framework & NIST 800-53.

NIST Compliance Audit	• Identifies how Client currently assesses, mitigates, and tracks its cybersecurity requirements • Identifies authorized and unauthorized devices in the managed network • Identifies gaps or deficiencies in the Client's operations that would prevent compliance under NIST CSF. Please Note: This service is limited to an audit only. Remediation of issues discovered during the audit, as well as additional solutions required to bring your managed environment into compliance, are not part of this service. After the audit is complete, we will discuss the results with you to determine what steps, if any, are needed to bring your organization into full compliance.
Virtual Chief Information Officer (vCIO)	Act as the main point of contact for certain business-related IT issues and concerns on a quarterly basses. • Assist in creation of information/data-related plans and budgets. • Provide strategic guidance and consultation across different technologies. • Provide education and recommendations for business technologies. • Participate in quarterly scheduled meetings to maintain goals. • Maintain technology documentation. • Assess and make recommendations for improving technology usage and services.
Zella Support Desktop Application	• Desktop application to access the Zella Support Portal.
Zella Live Chat	• Live Chat to log a Support Ticket or Sales Ticket.
Advanced DNS Protection	• Device must have our Advanced DNS Agent. • Advanced DNS Protection and Filtering at the network and device level. • The DNS layer is protected and filtered whether the device is on the client network or at a coffee shop. • *Licensed per device or user and determined by the amount of traffic passed through the DNS Protection service.
Privileged Access Management	• Device must have our PAM agent. • Least Privilege Access Windows UAC replacement.
Email Archive	• Licensed per User • Archive each user's O365 or Google Email Account. • Provides Legal Hold and other rules. • Allows customer to specify which users have compliance access to all mailboxes.
O365 Backup User License	• Licensed per User • Includes the license to backup an O365 user and does not include the storage for backups. • Storage for backups are additional and fall under the same terms/policies as Zella's Backup Solutions. • *A single Aggregated 1TB of Cloud Backup Storage is included for a single zone that covers all backup services. • *A minimal of 1 server is required for any backup service. • *A minimal of 1 local NAS is required for any backup service. • *If customer does not have a server or local NAS, a dedicated device can be rented from Zella for a monthly rental and management fee.
Threat Remediate Endpoint Protection	• Licensed per Agent/Device • TR Agent must be running on the device. • Provides EDR protection for the licensed device. • Provides SIEM/SOC for Threat Response and Remediation. • 12 months of log storage.
Threat Remediate Office365 User	• Licensed per User • Provides SIEM/SOC for Threat Response and Remediation for O365 Users. • 12 months of log storage.
Threat Remediate Firewall	• Licensed per Firewall/Router • Provides SIEM/SOC for Threat Response and Remediation for a Firewall/Router. • 12 months of log storage.
DMARC Service	• Licensed per Domain • Email deliverability monitoring and management for SPF, DKIM, DMARC, BMI, TLS, etc.

	• Non-Managed Service. Customer is responsible for monitoring and managing their DMARC service unless the Managed DMARC Service is purchased.
Zella Zero Trust Solution	• Licensed Per User or Device, whichever is greater, and Requires a dedicated Zero Trust Server which is billed as a Managed Server. • Provides users access to the network using a Zero Trust approach and replaces legacy VPN options.
Mobile Device Management	• Licensed Per User or Device, whichever is greater. • Provides an MDM agent to run on a user's mobile device, such as iOS and Android. • Provides centralized management of Mobile Devices to push company Email Accounts, Applications and Documents. • Allows for removal of Company pushed items from lost/stolen devices and/or terminated employees. • Allows for Rules/Polices to be put in place for Mobile Devices.
ND-Scanner	• Licensed per site • Requires a server for the agent to run on • Scans the network to determine devices, configurations, misaligned configurations and more.
VulScan	• Licensed per site • Requires a dedicated server or VM for the agent to run on. • Scans the network and devices to determine any known vulnerabilities. • This service does not include any remediation of issues/vulnerabilities found and is used for reporting purposes only.
Compliance Platform	• Licensed per Site • Provides a self-managed platform for customers to manage their compliancy needs. • This platform is provided as a SaaS solution and is not managed nor supported by Zella Technologies.
Zella's Managed IT & Cyber User (FULL) Bundle	• Licensed Per User based on the amount of Users in but not limited to, the PSA, AD, AAD & O365. • The Managed IT & Cyber Security User (FULL) Bundle includes our Managed IT Services, Support Portal/App, Managed DNS Protection, Privileged Access Management (PAM), Microsoft Office 365 Business Standard, Email Security Gateway (ESG), Breach Prevention Platform for Security Awareness Training and Phishing, MFA, ThreatRemediate SIEM/SOC for the user's workstation and Office 365 account with 12 months of log storage, EDR, ZeroTrust and Mobile Device Management (MDM) Essentials. • Includes Remote Support, M-F 8 AM – 5 PM CST, for the user's workstation, MDM and O365 account. • *Each User License covers one workstation, one O365 account, and one MDM. • *Not all services will be applicable to the client. • *Customer is responsible for informing Zella when a user is no longer at the company so billing may be adjusted. If an outside email/user is added to the PSA via ticket or other means, that user will count towards the company's user license. • *A single Aggregated 1TB of Cloud Backup Storage is included for a single zone that covers all backup services. • *A minimal of 1 server is required for any backup service. • *A minimal of 1 local NAS is required for any backup service. • *If customer does not have a server or local NAS, a dedicated device can be rented from Zella for a monthly rental and management fee. • *If workstation overages exceeds 10% of the "FULL" licensed users, additional licenses will be billed as a "FULL" user.
Zella's Managed IT & Cyber User (EMAIL-ONLY) Bundle	• Licensed Per User based on the amount of Users in but not limited to, the PSA, AD, AAD & O365. • The Managed IT & Cyber Security User (EMAIL-ONLY) Bundle includes our Support Portal/App, Microsoft Exchange Only (Plan 1), Email Security Gateway (ESG), Breach Prevention Platform for Security Awareness Training and Phishing, MFA, ThreatRemediate SIEM/SOC for the user's Office 365 account with 12 months of log storage, and Mobile Device Management (MDM) Essentials. • Includes Remote Support, M-F 8 AM – 5 PM CST, for the user's MDM and O365 account. • *Each User License covers one O365 account, and one MDM. • *Email-Only support only covers the support around O365. • *Not all services will be applicable to the client.
Zella's Managed IT & Cyber User (REMOTE-ONLY) Bundle	• Licensed Per User based on the amount of Users in but not limited to, the PSA, AD, AAD & O365. • The Managed IT & Cyber Security User (REMOTE-ONLY) Bundle includes our Support Portal/App, Breach Prevention Platform for Security Awareness Training and Phishing, MFA and ZeroTrust. • Includes Remote Support, M-F 8 AM – 5 PM CST, for the user's RDP session. • *Each User License covers one RDP Session and includes one RDS License from Microsoft. • *Remote-Only requires the client to have an RDP Environment (Server, Licenses, Gateway, Etc.) • *Not all services will be applicable to the client.

	• *Client is responsible for the security of the Remote-Only user, Access, devices and any security related to the Remote-Only User.
Zella's Managed IT & Cyber Network Bundle	• Licensed per Network Device (Firewall/Router, Switch, Access Point) • The Managed IT & Cyber Security Network Bundle includes our Managed Network Services for your Firewall, Switches and Access Points, Network Scanner, Vulnerability Scanner, ThreatRemediate SIEM/SOC for your Firewall with 12 months of log storage, and an Access Point Rental. • *This license covers each switch and access point. Only a single Firewall for management and ThreatRemediate is included. Only a single Network and Vulnerability Scanner is included. Vulnerability management for 3rd party software/solutions is not included. Access Point Rental is limited to the total amount of switches covered. • Access Point Rental is limited to the amount of Access Points needed, determined by Zella Technologies. • *Not all services will be applicable to the client. • *A single Aggregated 1TB of Cloud Backup Storage is included for a single zone that covers all backup services. • *A minimal of 1 server is required for server/network monitoring, ThreatResponse, SIEM/SOC. • *If customer does not have a server, a dedicated device can be rented from Zella for a monthly rental and management fee. • *All server equipment must have a Managed PDU and Managed UPS connected and must be located in a secured Rack.
Zella's Managed IT & Cyber Server Bundle	• Licensed Per Server • The Managed IT & Cyber Security Server Bundle includes our Managed IT Services, Privileged Access Management (PAM), ThreatRemediate SIEM/SOC with 12 months of log storage, EDR, ZeroTrust Server, Image Based Backups, and Cloud Backup Storage (up to 1TB aggregated storage). • *Each License covers one server. • *A single Aggregated 1TB of Cloud Backup Storage is included for a single zone. • *A minimal of 1 server is required for any backup service. • *A minimal of 1 local NAS is required for any backup service. • *If customer does not have a server or local NAS, a dedicated device can be rented from Zella for a monthly rental and management fee. • *All server equipment must have a Managed PDU and Managed UPS connected and must be located in a secured Rack. • *Not all services will be applicable to the client.
Zella's Managed IT & Cyber Group Mailbox Bundle	• Licensed Per Shared Mailbox/Distro • The Managed IT & Cyber Security Shared Mailbox Bundle includes our Email Security Gateway (ESG) and ThreatRemediate SIEM/SOC for the shared Office 365 mailbox with 12 months of log storage. • *Not all services will be applicable to the client.
Zella's Managed IT & Cyber Location Bundle	• Licensed Per Site/Location • Includes a single Domain license for DMARC Services • Includes a single local NAS license for monitoring and managing the NAS for local backups. • *All Managed Locations/Sites must have a backup internet connection approved by Zella Technologies.

Voice Services

The following Services, if listed in the Quote, will be provided to you.

Important: There are additional terms related to the VoIP/Voice service, including your use of E911 features AUP, FUP, etc., at the following link https://www.zellatech.com/telecommunications-aup/

Please read them carefully. By signing the Quote or using the service(s), you agree that you have read and understand the additional terms in the link above and the Services Guide.

Cloud PBX (Per User)	• Scalable VoIP-based telephone service with call transferring, voicemail, caller ID, call hold, conference calling, and call waiting functionalities.

	• Central control panel provides access to VoIP-related configurations, including physical address registration, call routing, updating greetings, and ability to turn on/off service features. • Each User in the system includes 1 Extenstion, 1 SIP Endpoint and 1 Cell Phone FWD Endpoint.
DID Number (Local DID)	• Local DID (Phone Number) for inbound calling.
E911 Service	• E911 service (per DID) • Service is provisioned per DID with the 911 address of the customer and managed by the customer
Unlimited SIP Trunk	• Two-Way (Inbound/Outbound) SIP Trunk (Call Path) for USA calling • Fair-Usage terms apply.
vFax	• Virtual Fax (eFax) for a designated vFax DID for USA only. • Best-Effort service. • Customer can send/receive faxes via Email.
Analog (SBC/ATA Fax)	• Single Port to convert IP to Analog Fax for USA only. • Best-Effort service. • Zella does not support the Customer Supplied Analog Devices that connect to the SBC Analog Port nor confirms such device is compatible with service.
Analog (SBC/ATA)	• Single Port to convert IP to Analog Voice for USA only. • Best-Effort service. • Zella does not support the Customer Supplied Analog Devices that connect to the SBC Analog Port nor confirms such device is compatible with the service.
Contact Center Multi-Channel	• Licensed per Agent • Multi-Channel (Voice, Email, Chat) Contact Center
Contact Center Additional Recording Storage	• Additional Storage for Contact Center in 1TB increments.
Dimensions PBX Reporting Insights Users	• Licensed per user based on the user count in the Cloud PBX. • Required for all users for any Dimensions Function/License. • Provides In-Depth Reporting and Insights for the Cloud PBX.
Dimensions PBX Reporting Analytic Users	• Licensed per user based on the user count in the Cloud PBX but Capped at 20 users. • Required for all users for any Dimensions Function/License. • Provides Cloud PBX Analytics.
Dimensions/Cloud PBX Softphone Device	• Licensed per softphone • Requires Dimensions PBX Reporting and Analytics • Provides a softphone for either iOS, Android, Windows or MAC.
Wholesale Voice Services (Origination, Termination, Toll-Free, N11 Features, CNAM, LNP, More)	• Wholesale Voice Services based on a Rate Sheet/Deck
Wholesale Two-Way SIP Trunk Port	• Wholesale single Two-Way Call Session/Path • No Origination/Termination included
Wholesale Two-Way Burst SIP Trunk Port	• Wholesale single Two-Way Call Session/Path that allows an additional burstable call session/path in-additional to the customer's Wholesale Two-Way SIP Trunk Port. • No Origination/Termination included.
Class 5 Features	• Provides class 5 features for Wholesale customers.

Fiber Internet Services

The following Services, if listed in the Quote, will be provided to you.

Important: There are additional terms related to the Internet (telecommunications) service, including AUP, FUP, etc., at the following link https://www.zellatech.com/telecommunications-aup/

Please read them carefully. By signing the Quote or using the service(s), you agree that you have read and understand the additional terms in the link above and the Services Guide.

DIA Fiber Internet	• Dedicated Fiber Internet Connection • /30 IPv4 block included with each DIA Circuit
Additional IPv4 Block	• Customer can purchase additional blocks of IPv4 addresses
Managed Router	• Customer can purchase our Managed Router Service for all DIA Circuits.

Additional Description of Services

The following additional details further explain and define the scope of the Services.

Hardware as a Service (HaaS)

HaaS Equipment We will provide you with the HaaS Equipment described in the Quote or, if no hardware is expressly designated as HaaS Equipment in the Quote, then a complete list of HaaS Equipment will be provided to you under separate cover.

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. If you wish to delay the deployment of the HaaS Equipment, then you may do so provided that you give us written notice of your election to delay no later than five (5) days following the date you sign the Quote. Deployment shall not extend beyond two (2) months following the date on which you sign the Quote. You will be charged at the rate of fifty percent (50%) of the monthly recurring fees for the HaaS-related services during the period of delay. Following deployment, we will charge you the full monthly recurring fee (plus other usage fees as applicable) for the full term indicated in the Quote.

Equipment Hardware Repair or Replacement. Zella will repair or replace HaaS Equipment based on availability for which the applicable problem is identified by, or reported to, Zella and has been determined by Zella to be incapable of being remediated remotely.

This warranty does not include the time required to rebuild your system, such as the time required to configure a replacement device, rebuild a RAID array, reload the operating system, reload and configure applications, and/or restore from backup (if necessary).

If Zella fails to meet the warranties in this section and the failure materially and adversely affects your hosted environment ("Hosted System"), you are entitled to a credit in the amount of 5% of the monthly fee per hour of downtime (after the initial one (1) hour allocated to problem identification), up to 100% of your monthly fee for the affected HaaS Equipment. In no event shall a credit exceed 100% of the applicable month's monthly fee for the affected equipment.

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.

Return of HaaS Equipment. 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 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 Zella 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. Zella Technologies may decide to have the equipment returned via FedEx. If Zella instructs you to return the hardware via FedEx, you will return the hardware within 30 days. If the hardware is not received within 30 days, we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

Usage. You will use all Zella-hosted or Zella-supplied equipment and hardware 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 Infrastructure 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 Infrastructure is violates the terms of the Quote, this Services Guide, or the Agreement.

Covered Equipment / Hardware / Software

Managed Services will be applied to the devices on which we install software monitoring agents ("Covered Hardware"). You can view the list of Covered Hardware in the support portal once all software agents have been installed. The list of Covered Hardware may be modified by mutual consent (email ticket 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. We will provide technical support for Covered Devices; however, all Covered Devices must be covered, at all times and at your cost, under a then-current manufacturer's service plan.

We will provide support for any software applications that are licensed through us (see "Recurring Services" above). 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, if provided to you, will be provided to you on a "best effort" basis only, and will be billed to you on a time and materials basis. Should our technicians provide you with general advice concerning non-Supported Software, the provision of that advice should be viewed as an accommodation to you, and not as a continuing obligation or guarantee by Zella to continue to provide such support or advice to you.

We provide the Services on a "per user" basis. As such, our managed services will be provided for up to one (1) 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. In this Services Statement, covered Business Devices are referred to as "Covered Hardware."

Physical Locations Covered by Services

Services will be provided remotely unless, in our discretion, we determine that an onsite visit is required. Zella 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.

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 Zella's satisfaction.

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

Auto-Renewal. After the expiration of the initial Service Term, the Service Term will automatically renew for contiguous terms equal to the initial Service Term unless either party notifies the other of its intention to not renew the Services no less than ninety (90) days before the end of the then-current Service Term.

Per Seat Licensing: **Regardless of the reason for the termination of the Services, you will be required to pay for all per seat licenses (such as, if applicable, Microsoft NCE licenses) that we acquire on your behalf. Please see "Per Seat License Fees" in the Fees section below for more details.**

Removal of Software Agents; Return of Firewall, Backup Appliances & Rented Devices: 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. 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 Zella 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.

Minimum Requirements / Exclusions

The scheduling, fees and provision of the Services are based upon the following assumptions and minimum requirements:

- 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, licensed as Pro or Enterprise, 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 is provided by Zella Technologies.
- All wireless data traffic in the managed environment must be securely encrypted.
- There must be an outside static IP address assigned to a network device, allowing VPN/RDP control access.
- 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.
- All Workstations and laptops must have an SSD Hard Drive, at least 16GB of RAM, and an i5 processor with vPRO.
- All Devices must have an active Warranty.
- Client must have an active internet connection at all times.

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 Zella. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by Zella 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.
- Data/voice wiring or cabling services of any kind.
- Battery backup replacement.
- Equipment relocation.
- The cost to bring the managed environment up to these minimum requirements (unless otherwise noted in the Quote).
- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.
- Any compliance-related requests.

Service Levels

Automated monitoring is provided on an ongoing (24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our business hours (currently M-F, 8 AM – 5 PM Central Time, excluding legal holidays and Zella-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 Zella in our discretion. All remediation services will initially be attempted remotely; Zella 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
Priority 1 (*Emergency incidents affecting the entire company*)	Response within One (1) business hours after notification.
Priority 2 (*Critical incidents affecting a single site*)	Response within two (2) business hours/NBD after notification.

Priority 3 (*Major incidents affecting a single department or multiple users*).	Response within four (4) business hours/NBD after notification.
Priority 4 (Normal incidents affecting a single user).	Response within eight (8) business hours/NDB after notification.
Priority 5 (Requests or nuisance issues).	Response within sixteen (16) business hours/2ndBD after notification.

* All time frames are calculated as of the time that Zella is notified of the applicable issue / problem by Client through Zella's 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 Zella 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:

- Project Professional Level 1: 1.5x normal rate
- Project Professional Advanced: 2x normal rate
- Support Technician, Level 1: 1.5x normal rate
- Support Technician, Senior: 2x normal rate

All hourly services are billed in 30 minute increments, and partial increments are rounded to the next highest increment. A one (1) hour minimum applies to all Non-Business Hour Support.

Zella-Observed Holidays: Zella observes the following holidays:

- New Year's Day
- Martin Luther King Jr. Day
- President's Day
- Good Friday – Half Day
- Memorial Day
- Juneteenth Day
- Independence Day
- Labor Day
- Columbus Day
- Veterans Day
- Thanksgiving Day
- The day following Thanksgiving Day
- Christmas Eve
- Christmas Day
- New Year's Eve – Half 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 the MSA), 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.

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, or the number of DIDs, PBX Users, Trunks, or other Voice Services QTY changes, then you agree that the fees will be automatically and immediately modified to accommodate those changes.

Minimum Monthly Fees. The initial Fees indicated in the Quote represent the minimum monthly fees ("MMF") that will be charged to you during the term. You agree that the amounts paid under the Quote will not drop below the MMF regardless of the number of users, devices, trunks, or any other services to which the Services are directed or applied. Additionally, the monthly fee for hardware, devices, authorized users, per-device, per-user, per-trunk, or any other service will be subject to a minimum of 90% of the highest quantity billed at any point during the term. Customers may add additional users, devices, or services as needed, with charges adjusting accordingly.

Increases. In addition, we reserve the right to increase our monthly recurring fees and, if applicable, our data recovery-related fees; provided, however, if an increase is more than five percent (5%) of the fees charged for the Services in the prior calendar year, then you will be provided with a thirty (30) day opportunity to terminate the Services by providing us with written notice of termination. You will be responsible for the payment of all fees that accrue up to the termination date and all pre-approved, non-mitigatable expenses that we incurred in our provision of the Services through the date of termination. Your continued acceptance or use of the Services after this thirty (30) day period will indicate your acceptance of the increased fees.

In addition to the foregoing, we reserve the right to pass through to you any increases in the costs and/or fees charged by third party providers for the third party services ("Pass Through Increases"). Since we do not control third party providers, we cannot predict whether such price increases will occur, however, should they occur, we will endeavor to provide you with as much advance notice as reasonably possible.

Pass Through Increases are independent of any increases to our monthly recurring fees and will not be included in the five percent calculation described in the paragraph above.

Travel Time. If onsite services are provided or required, we will travel up to 15 minutes from our office to your location at no charge. Time spent traveling beyond 15 minutes (*e.g.,* locations that are beyond 15 minutes from our office, occasions on which traffic conditions extend our drive time beyond 15 minutes one-way, etc.) will be billed to you at our then current hourly rates. 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.

Automated Payment. You may pay your invoices by credit card and/or by ACH, as described below. If you authorize payment by credit card and ACH, then the ACH payment method will be attempted first. If that attempt fails for any reason, then we will process payment using your designated credit card.

- **ACH**. When enrolled in an ACH payment processing method, you authorize us to electronically debit your designated checking or savings account, as defined and configured by you in our payment portal, for any payments due under the Quote. This authorization will continue until otherwise terminated in writing by you.

We will apply a $35.00 service charge to your account for any electronic debit that is returned unpaid due to insufficient funds or due to your bank's electronic draft restrictions.

- **Credit Card**. When enrolled in a credit card payment processing method, you authorize us to charge your credit card, as designated by you in our payment portal, for any payments due under the Quote.

Microsoft Licensing Fees. The Services require that we purchase certain "per seat" licenses from Microsoft (which Microsoft refers to as New Commerce Experience or "NCE Licenses") in order to provide you with one or more of the following applications: Microsoft 365, Dynamics 365, Windows 365, and Microsoft Power Platform (each, an "NCE Application"). To leverage the discounts offered by Microsoft for these applications and to pass those discounts through to you, we may purchase NCE Licenses for one (1) year terms for the NCE Applications required under the Quote. **As per Microsoft's requirements, NCE Licenses cannot be canceled once they are purchased and cannot be transferred to any other customer. For that reason, you understand and agree that regardless of the reason for termination of the Services, you are required to pay for all applicable NCE Licenses in full for the entire term of those licenses.** Provided that you have paid for the NCE Licenses in full, you will be permitted to use those licenses until they expire, even if you move to a different managed service provider.

Additional Terms

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 Zella, and Client shall not modify these levels without our prior written consent.

Remediation

Unless otherwise provided in the Quote, remediation services will be provided in accordance with the recommended practices of the managed services industry. Client understands and agrees that remediation services are not intended to be, and will not be, a warranty or guarantee of the functionality of the Environment, or a service plan for the repair of any particular piece of managed hardware or software.

Configuration of Third Party Services

Certain third party services provided to you under this Services Guide 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 our knowledge or authorization could disrupt the Services and/or 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.

Dark Web Monitoring

Our dark web monitoring services utilize the resources of third party solution providers. 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.

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.

Co-Managed Environment

In co-managed situations (e.g., where you have designated other vendors or personnel, or "Co-managed Providers," to provide you with services that overlap or conflict with the Services provided by us), we will endeavor to implement the Services in an efficient and effective manner; however, (a) we will not be responsible for the acts or omissions of Co-Managed Providers, or the remediation of any problems, errors, or downtime associated with those acts or omissions, and (b) in the event that a Co-managed Provider's determination on an issue differs from our position on a Service-related matter, we will yield to the Co-Managed Provider's determination and bring that situation to your attention

Anti-Virus; Anti-Malware (EDR)

Our anti-virus / anti-malware (EDR) solution will generally protect the Environment from becoming infected with new viruses and malware ("Viruses"); however, Viruses that exist 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 Viruses and malware will be capable of being detected, avoided, or removed, or that any data erased, corrupted, or encrypted by malware will be recoverable. To improve security awareness, you agree that Zella 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 impacted by the incident will be recoverable. 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 Environment, or (ii) prevents normal access to the Environment, or impedes or disrupts the normal functions of the Environment. Our Threat Remediation Endpoint/Firewall/O365 services do not include remediation and/or recovery as defined in this section.

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.

Managed IT Fair Usage Policy

Our Fair Usage Policy ("FUP") applies to all Non-Telecom 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. 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 Zella 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. Zella 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 Zella 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.

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 Zella 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. Zella cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Zella 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 Zella 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, Zella 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. Zella is not a warranty service or repair center. Zella 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 Zella will be held harmless, and (ii) Zella 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 us in our capacity as a virtual chief technology or information officer will be for your informational and/or educational purposes only. Zella will not hold an actual director or officer position in Client's company, and we will neither hold nor maintain any fiduciary realtionship with Client. Under no circumstances shall Client list or place the Zella 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 Assessment

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 process, 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 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 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, security 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, security, or remediation activities for any Obsolete Element.

Hosting Services

You agree that you are responsible for the actions and behaviors of your users of the Services. In addition, you agree that neither Client, nor any of your employees or designated representatives, will use the Services in a manner that violates the laws, regulations, ordinances, or other such requirements of any jurisdiction.

In addition, Client agrees that neither it, nor any of its employees or designated representatives, will: transmit any unsolicited commercial or bulk email, will not engage in any activity known or considered to be "spamming" and carry out any "denial of service" attacks on any other website or Internet service; infringe on any copyright, trademark, patent, trade secret, or other proprietary rights of any third party; collect, attempt to collect, publicize, or otherwise disclose personally identifiable information of any person or entity without their express consent (which may be through the person or entity's registration and/or subscription to Client's services, in which case Client must provide a privacy policy which discloses any and all uses of information that you collect) or as otherwise required by law; or, undertake any action which is harmful or potentially harmful to Zella or its infrastructure.

Client is solely responsible for ensuring that its login information is utilized only by Client and Client's authorized users and agents. Client's responsibility includes ensuring the secrecy and strength of user identifications and passwords. Zella shall have no liability resulting from the unauthorized use of Client's login information. If login information is lost, stolen, or used by unauthorized parties or if Client believes that any hosted applications or hosted data has been accessed by unauthorized parties, it is Client's responsibility to notify Zella immediately to request the login information be reset or unauthorized access otherwise be prevented. Zella will use commercially reasonable efforts to implement such requests as soon as practicable after receipt of notice.

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.

Last Updated: December 2024