Statement of Work

Techo Services

This Statement of Work ("SOW") explains, in detail, the services referenced in the proposal or quote we provided to you (the "Quote"). By signing the Quote, you are agreeing to the terms laid out in this document. If anything here doesn't sit right with you, please reach out to us before signing — we're happy to walk through it.

Think of this SOW as the reference guide behind everything Techo Services ("Techo," "we," "us") is capable of delivering as part of our managed services offering. That said, you will only receive the specific items called out in your Quote (together, the "Services"). Anything not explicitly listed there falls outside scope and won't be delivered unless we put it in writing separately.

This document also covers how the agreement renews automatically and how pricing can change over time, so please hold onto a copy for future reference.

Getting Started: Onboarding

When your Quote includes onboarding, here's what that process covers:

- Removing monitoring agents or software left behind by a prior IT provider
- Building a complete inventory of protected servers, desktops, and laptops
- Removing legacy antivirus tools and deploying our managed antivirus platform
- Installing a remote-access agent on every managed device so we can provide support remotely
- Setting up patch management tooling and scanning for missing security patches
- Removing risky or unnecessary applications
- Tuning device performance — disk cleanup, malware/spyware sweeps, etc.
- Auditing the firewall and other network infrastructure
- Checking the condition of battery backup (UPS) units across the environment
- Documenting the current server setup and condition
- Assessing the existing backup approach and presenting backup options going forward
- Reviewing password policies and resetting device/user passwords as needed
- Where appropriate, flagging recommended changes to the environment

We may adjust this list at our discretion if we determine the environment calls for a different or expanded onboarding approach.

If we uncover problems during onboarding, we'll flag them and explain how they might affect our ongoing managed services. Important: unless your Quote says otherwise, onboarding does not include fixing any issues we find ("Issues") — and we can't promise that onboarding will catch every Issue that may exist.

Ongoing Managed Services

Ongoing services are the services billed to you on a recurring basis — typically monthly, starting on the date you sign your Quote, unless your Quote states a different billing start date. These services typically kick off once onboarding wraps up, so any onboarding delays will push back the start of ongoing service.

Core Service Categories

Below is the full menu of managed services we offer. You'll only receive the ones specifically named in your Quote.

Service	What It Includes
Remote Monitoring & Management	Agents installed on Covered Equipment report status and events around the clock; alerts are triggered and addressed per the response times outlined later in this document.
Backup & Disaster Recovery	24/7 monitoring of backup jobs, including offsite copies and offsite replication (local backup appliance monitoring included; appliance itself purchased separately) Troubleshooting and fixing failed backup drives Ongoing maintenance of imaging software Firmware/software updates for the backup appliance Problem analysis by our network operations team Tracking of backup successes and failures Quarterly test restores to verify recoverability

Backup Frequency: Backups are initially set to run hourly. Need a different cadence? Talk to your account lead. Note that some platforms (Microsoft 365, for example) cap how many backups can run per day — in those cases we'll back up as frequently as the platform allows, aiming for hourly.

Encryption: Data is encrypted in transit with 256-bit AES. At-rest encryption is also available — ask your account lead for details.

How Long We Keep Backups:

- Hourly snapshots: 2 weeks
- Daily snapshots: 6 weeks
- Weekly snapshots: 8 weeks
- Monthly snapshots: 6 months

Failure Alerts: Managed servers are configured to notify us automatically if a backup job fails.

Restoring Your Data: If you ever need data restored from backup, here's how that works:

- Availability: Restore requests are handled during our regular business hours, currently 9:00 AM–6:00 PM Eastern, Monday–Friday
- How to Request: Email support@techoservices.com or call our office line
- Turnaround: We move as fast as we can once a restore is requested, though actual timing depends on technician availability. As a general guideline: 0–100MB within about 4 hours, 100–500MB within about 8 hours. Anything larger than 500MB is handled based on technician availability at the time.

Updates & Patch Deployment

- Rolling out minor version updates, bug fixes, and security patches across managed hardware as needed
- Handling minor hardware/software installs and upgrades
- Completing quick-turnaround tasks — generally anything doable remotely in under 30 minutes
- Deploying and tracking approved service packs, security patches, and firmware updates across applicable managed hardware

Managed Firewall

- A FIPS 140-2 compliant firewall, sized and configured to your organization's bandwidth, remote access, and user requirements
- Blocks external access attempts into your internal network while enabling secure encrypted remote connections; scans inbound/outbound traffic for malware; filters website content

Email Threat Protection

- Defense against phishing, business email compromise (BEC), spam, and malware delivered via email
- Display-name filtering to catch social-engineering impersonation attempts
- Protection against whaling, CEO fraud, BEC, and W-2 fraud schemes

- Flags emails from newly registered or newly observed domains
- Detects spoofed display names
- Catches domains designed to “look” or “sound” like legitimate ones

Security Awareness Training for End Users

- On-demand training videos available in multiple languages
- On-demand quizzes to confirm staff retained the material
- Baseline phishing simulations to measure your team’s “phish-prone” percentage and ongoing simulated campaigns to reinforce good habits

Hardware as a Service (HaaS)

- Sourcing and deploying the hardware designated in your Quote (“HaaS Equipment”)
- Installing that equipment
- Repairing or replacing it when needed (details below)
- Providing technical support for it
- Periodically refreshing it over time (details below)

Labor for New & Replacement Workstations

Covers labor for setting up new machines or swapping out old ones.

What’s covered:

- New or additional computers added during your contract term
- Replacing machines that are 4+ years old (per manufacturer serial records)
- Replacing machines that are lost, stolen, irreparably damaged, or out of warranty — even if under 4 years old
- OS upgrades, assuming hardware compatibility

Limitations:

- Capped at 4 device setups/replacements per month unless we approve more in advance
- Doesn’t apply to used or refurbished machines
- New/replacement machines must be business-grade (not consumer-grade) from a major brand such as Dell or HPE

Remote & On-Site Support

Covers labor for supporting company-owned desktops, laptops, servers, cloud platforms (e.g., O365), printers, and general desktop issues. Subject to the Fair Usage Policy described later in this document.

Endpoint Protection

- EDR-AV: Endpoint Detection and Response antivirus
- MDR-AV: Managed Detection and Response, such as Huntress MDR

Note: this section describes our full service catalog — not necessarily what you personally receive. Always check your Quote to confirm which services apply to you. We may revise this list if we determine different or additional monthly activities are warranted.

Project-Based Add-On Services

These are offered separately, typically billed as fixed-fee projects.

HIPAA Audit & Policy Manual Development

We partner with a trusted third party (currently The Compliancy Group, www.compliancygroup.com) for HIPAA compliance work. They assign a dedicated compliance officer to guide you toward a HIPAA Seal of Compliance, and afterward provide audit-response support if a HIPAA violation issue ever comes up.

The 6-part audit covers:

- IT Risk Analysis
- Physical Site Audit
- Security Audit
- Privacy Audit
- Hi-Tech Audit
- Device Audit

Deliverables created along the way:

- HIPAA Privacy Policy & Procedure Manual
- HIPAA Security Policy & Procedure Manual
- IT Disaster Recovery Plan
- Business Continuity Plan

Also included: a central online repository for tracking HIPAA documentation, plus security awareness training delivered by The Compliancy Group. More info at www.compliancygroup.com.

techo

SOC 2 / ISO 27001 Readiness & Certification

We review your office and remote environment and advise on policies/procedures aligned to the SOC 2 and ISO 27001 frameworks. Once those are in place, our third-party partner issues the SOC 2 / ISO 27001 certification. Doesn't include third-party licensing costs or the actual implementation of the policies/procedures.

NIST Framework Assessment

Review of your environment with recommendations for aligning to the NIST Framework (more info: www.nist.gov/cybersecurity). Doesn't include the actual implementation of policies/procedures.

CIS Controls Assessment

Review of your environment with recommendations aligned to the CIS Controls Framework (more info: www.cisa.gov). Doesn't include the actual implementation of policies/procedures.

Risk Assessment

A NIST-based questionnaire (administered via third-party software) that produces a risk score for your organization.

NY SHIELD Act Compliance Review

Review of your environment and guidance on policies/procedures needed to align with the NY SHIELD Act (more info: www.nysenate.gov/legislation/bills/2019/s5575).

23 NYCRR Part 500 Compliance

Annual review and compliance check against 23 NYCRR Part 500, the NY DFS cybersecurity regulation for financial services firms (more info: www.dfs.ny.gov/industry_guidance/cyber_faqs).

Vulnerability Scanning

We run a vulnerability scan against your network and review the findings with you.

End User Security Awareness Training

- On-demand multilingual training videos
- On-demand comprehension quizzes
- Baseline phishing simulation testing and ongoing simulated campaigns

Phone: 718-635-2543
Email: Support@techoservices.com
Website: www.techoservices.com

Domain & Email Setup

Setting up an email server on your own domain through a cloud provider (Office 365, Google Workspace, etc.). Monthly user licensing is not included.

Azure AD / Intune Setup

- Azure Active Directory configuration
- Intune enrollment setup
- Deployment of Techo-developed security standards (geo-IP filtering, MFA enforcement, etc.)
- Device configuration profiles for Apple, Android, Windows, etc.
- Conditional Access policy setup
- Company-owned device enrollment

Any security standards, Conditional Access policies, or configuration profiles we develop will be reviewed with your designated contact and require approval before deployment.

Your Quote or an attached schedule will specify the number of device configurations and device counts included in the project. Monthly user licensing is not included.

Email Migration

Migrating mailboxes between platforms — on-prem to cloud, or cloud to cloud.

Data Migration

Migrating files/data between systems — on-prem to on-prem, on-prem to cloud (SharePoint, Google Workspace, etc.), or cloud to cloud (e.g., Dropbox to SharePoint).

Service Details & Additional Terms

Hardware as a Service — Expanded Terms

HaaS Equipment: We'll provide the hardware listed in your Quote. If no HaaS Equipment is explicitly named there, we'll send you a separate equipment list.

Deployment Timeline: We'll deploy your HaaS Equipment within the timeframe stated in your Quote, provided you give us the information we need promptly. This deployment commitment applies only to the HaaS Equipment itself — not to other software, services, or hardware. You may delay deployment by notifying us in writing within 5 days of signing your Quote; deployment cannot be pushed out more than 2 months past your signing date. During any delay period, you'll be billed 50% of the standard

monthly HaaS fee. Once deployed, full monthly fees (plus applicable usage charges) apply for the remaining contract term.

Repair & Replacement: We will repair or replace HaaS Equipment by the end of the next business day following identification of a problem that can't be fixed remotely. This commitment excludes the time needed to rebuild your system — configuring a replacement unit, rebuilding a RAID array, reinstalling the OS, reconfiguring applications, or restoring from backup.

If we miss this commitment in a way that materially impacts your hosted environment, you'll receive a credit equal to 5% of the monthly fee per hour of downtime beyond the first hour (which is allocated to diagnosis), capped at 100% of that month's fee for the affected equipment.

Equipment Refresh: We may periodically swap out aging HaaS Equipment (generally 5+ years old) for newer units. We'll coordinate timing with you in advance.

Returning Equipment: Don't remove or disable any software agents we've installed on HaaS Equipment unless we instruct you to. Doing so risks creating security gaps and may leave you responsible for ongoing license fees and/or our remediation costs at standard hourly rates. Within 10 days of HaaS service termination, you must give us access to retrieve the equipment. If access isn't provided in time, or equipment comes back damaged beyond normal wear, you agree to pay its replacement value.

What's Covered: Equipment & Software

Managed Services apply to devices where we've installed monitoring agents ("Covered Hardware"). We support software on Covered Hardware as long as it's under an active vendor support plan ("Supported Software"); anything outside vendor support is handled on a best-efforts basis only. Together, Covered Hardware and Supported Software make up the "Environment."

Changes to the Environment may trigger additional fees on your invoice. Unless we agree otherwise, new devices/licenses are billed at the rate already applicable to similar items in your Environment, prorated for mid-month additions.

Where We Provide Service

Most work is done remotely. We'll schedule an on-site visit only when we determine it's necessary, prioritized according to the severity levels described below and subject to technician availability. On-site work happens at the primary location listed in your Quote unless we agree otherwise, and may carry additional fees — see the response-time table below.

Contract Term & Renewal

Service — and billing — begins on the date your Quote specifies (the "Commencement Date") and runs through the Initial Term stated there. We may delay the Commencement Date until onboarding/transition work is finished and any onboarding issues are resolved to our satisfaction.

Services continue through the Initial Term and beyond until ended per the governing agreement, your Quote, or the renewal terms below (the "Service Term").

Auto-Renewal: Once the Initial Term ends, the Service Term automatically renews for additional periods matching the original term length, unless either party gives the other at least 30 days' written notice before the end of the current term that they don't wish to renew.

Microsoft NCE Licensing: No matter why services end, you remain responsible for paying for all Microsoft NCE licenses purchased on your behalf. See the Microsoft Licensing Fees section below.

Assumptions, Baseline Requirements & Exclusions

Our pricing, scheduling, and service delivery assume the following baseline conditions:

- Server hardware is under active manufacturer warranty
- Windows-based equipment runs currently supported versions with the latest service packs and critical updates installed
- All software is genuine, licensed, and vendor-supported
- Server file systems and email systems are protected by licensed, up-to-date antivirus software
- The Environment has a licensed, vendor-supported, monitorable server-based backup solution
- All wireless traffic in the environment is securely encrypted
- All servers connect to working UPS devices
- You provide installation media and license/key codes if something fails
- Costs to bring the environment up to these standards are not included in this SOW
- You provide us exclusive administrative access to the Environment
- You won't attach or install any accessory, upgrade, or device to firewalls, servers, or NAS appliances without our written approval

Out of Scope: Anything not explicitly listed in your Quote falls outside our scope and won't be delivered unless agreed in writing. In particular, the following are always excluded unless we agree otherwise in writing:

- Customizing third-party applications or any form of programming
- Supporting operating systems, applications, or hardware no longer supported by their manufacturer

- Any data or voice wiring/cabling work
- Replacing UPS batteries
- Relocating equipment
- Costs to bring the Environment up to baseline requirements (unless stated otherwise above)
- Hardware/software repair costs, parts, equipment, or shipping charges
- Travel/parking costs for on-site visits

Response Times & Severity Levels

Automated monitoring runs continuously, 24/7/365. All other services — response, repair, support, remediation — are provided during normal business hours (currently 8 AM–6 PM Eastern, Monday–Friday) unless your Quote states otherwise.

We respond to issues according to the severity table below. We determine severity level at our discretion, in consultation with you. Remediation is always attempted remotely first; on-site visits happen only if remote efforts don't resolve the issue, and only if your service plan covers on-site support.

Severity	Response Commitment
Critical (service down — all users/functions affected)	Monitored 24/7. 1-hour response during business hours; 4-hour response outside business hours.
Significant Degradation (large number of users or critical functions affected)	Monitored 12/5. 2-hour response during business hours.
Limited Degradation (limited users/functions affected; business can continue)	Response within 9 business hours.
Minor Degradation (single user affected; business can continue)	Response within 2 business days.

All timeframes start once we're notified through our designated support email, RMM agent, help desk, or phone line listed in your Quote. Notifications sent any other way may delay response. Help desk requests handled outside our normal support hours are billed at $250/hour (1-hour minimum).

techo

Fees & Billing

Fees for your Services are listed in your Quote.

Environment Changes: You'll initially be billed the monthly amount in your Quote. If your Environment changes, fees will adjust automatically to reflect that.

Minimum Monthly Fee: The fee in your Quote represents a minimum monthly commitment ("MMF") for the contract term. Your monthly payment won't drop below the MMF regardless of how many users or devices the Services apply to, unless we agree to a reduction in writing. Any changes to hardware/device/user counts must be documented and accepted by both parties.

Fee Increases: We reserve the right to raise monthly recurring and data recovery fees. If an increase exceeds 5% over the prior year's rate, you'll have 60 days from notice to terminate by providing written notice. You'll still owe fees accrued through the termination date and any pre-approved, non-recoverable expenses incurred through that date. Continuing to use the Services after the 60-day window means you've accepted the new rate.

Travel Time: On-site visits include up to 30 minutes of travel at no charge. Travel time beyond that (due to distance or traffic) is billed at our standard hourly rate, along with any tolls or parking we incur.

Cancelling Appointments: You can cancel or reschedule free of charge with at least 1 business day's notice. Without that notice — or if we arrive and can't access your premises — a cancellation fee equal to 2 hours of our standard (or after-hours, if applicable) consulting rate applies.

Automatic Payment: You may pay by ACH or credit card. If both are on file, ACH is attempted first; if it fails, we charge the card on file.

- ACH: You authorize us to debit your designated account for amounts owed under your Quote. This stays in effect until you cancel it in writing. A $45 fee applies to any returned/failed ACH debit.
- Credit Card: You authorize us to charge your card on file for amounts owed under your Quote.

Microsoft Licensing Fees: Certain services require us to purchase per-seat Microsoft "New Commerce Experience" (NCE) licenses for products like Microsoft 365, Dynamics 365, Windows 365, and Power Platform. To pass Microsoft's volume discounts to you, we buy these on annual terms. Per Microsoft's rules, NCE licenses can't be cancelled once purchased and can't transfer to another customer. Each purchase locks in its own 1-year term — licenses bought at different times don't combine into a single renewal date. (Example: licenses purchased Jan. 1 expire Dec. 31; additional licenses purchased June 1 expire the following May 31, on a separate cycle.) Regardless of why service ends, you're responsible for paying for the full term of any NCE licenses purchased on your behalf. As long as they're paid in full, you may keep using those licenses through their expiration — even if you switch providers.

Operating Terms

Authenticity & Licensing

Everything in your managed environment — hardware, software, everything — must be genuine and properly licensed. If we ask for proof, you agree to provide it. Minimum hardware/software requirements stated in your Quote or this SOW must be maintained on an ongoing basis as a condition of service.

Monitoring & Alerts

Unless your Quote says otherwise, monitoring and alerting services are limited to detecting and notifying — not automatically resolving — issues. We set monitoring thresholds, and you agree not to modify them without our written consent.

Remediation Scope

Unless your Quote states otherwise, remediation follows standard managed-services industry practices. You understand this isn't a warranty or guarantee that the Environment will always function properly, nor a repair plan for any specific piece of equipment or software.

Third-Party Service Configurations

Some third-party services we provide give you administrative access that lets you change settings ("Configurations") yourself. Doing so without our knowledge could disrupt service or increase costs. We recommend leaving Configurations alone unless we've approved a change — and you'll be responsible for any added costs that result if you make changes on your own.

Dark Web Monitoring

We rely on third-party tools for dark web monitoring. It's a useful layer of protection against certain types of cybercrime, but we can't guarantee it will catch every instance where your credentials or data appear online.

Changes to the Environment

Unauthorized changes to the Environment can significantly disrupt service quality and may affect your fees. Please don't add or remove hardware, install applications, or modify configuration/log files without checking with us first.

Working Alongside Other IT Vendors

If you use other vendors alongside us ("Co-Managed Providers") for overlapping or related services, we'll do our best to coordinate efficiently. That said: (a) we're not responsible for their actions, omissions, or any resulting problems, and (b) if a Co-Managed Provider's position on an issue conflicts with ours, we'll defer to them and let you know.

Antivirus & Anti-Malware

Our antivirus/anti-malware tools generally protect against new infections, but pre-existing infections at the time of deployment may require additional (billable) remediation. We can't guarantee detection or removal of all malware, or that data damaged by malware will be recoverable. To improve overall security, you agree we (or our designated partners) may share anonymized data — file scan results, URL reputation data, threat statistics — for the purpose of improving spam/malware protection. This never includes your personal or confidential information.

Security Incident Response

Unless your Quote says otherwise, responding to and recovering from a security incident is not included in your Services. If you need that help, we'll provide it on a time-and-materials basis at standard hourly rates. Because every incident is different, we can't guarantee how long recovery will take, that recovery is possible in every case, or that all affected data can be recovered. A "Security Incident" means any unauthorized access, use, or disclosure involving the Environment or your confidential information that compromises security/privacy, or that disrupts normal use of the Environment.

Environmental Conditions

Things like water, temperature extremes, or unusual lighting can cause equipment to malfunction. Unless your Quote states otherwise, we don't guarantee error-free or uninterrupted operation, or that video/audio equipment will always capture events clearly.

Fair Usage Policy

Our Fair Usage Policy applies to anything labeled "unlimited." That means you can use the service as much as reasonably needed without incurring extra time- or usage-based charges — but only during normal business hours, and subject to technician availability (which can't always be guaranteed). We may prioritize more urgent issues over less urgent ones at our discretion. You agree not to: open urgent tickets for non-urgent issues, request an unusually high volume of support inconsistent with normal industry usage (e.g., support requests used as a substitute for training your staff), or request support in a way that disrupts our ability to serve other clients.

Hosted Email Use

You're responsible for proper use of any Hosted Email we provide, and your use must comply with applicable acceptable use policies. You agree not to upload, post, transmit, or distribute (or let your users do so) content that's obscene, illegal, infringing, deceptive about its origin, disruptive to our or others' services, or that contains malware. You also agree not to use Hosted Email to send unsolicited bulk commercial email (spam) in violation of law. We may, at our discretion, suspend access if we believe an account is being misused.

Patch Management

We keep managed hardware/software current with critical patches as vendors release them. Occasionally a patch — even installed correctly — can cause instability. We're not responsible for downtime or losses tied to patch installation or use, and we reserve the right to hold off installing a patch if we're aware it causes problems or instability.

Backup & Disaster Recovery — Risk Disclosures

Internet-transmitted data can be exposed to malware and unauthorized access attempts; we're not responsible for the outcomes of such activity. BDR services depend on a reliable, always-on internet connection — backup/recovery speed depends on your connection quality, and outages will interrupt BDR functionality. All computer hardware carries some inherent risk of failure, for which we're held harmless. While we minimize the risk of data corruption or loss, we can't eliminate it entirely, and you agree we're held harmless if it occurs. We strongly recommend keeping a local backup copy of your data as an extra safeguard.

Procurement of Equipment & Software

Equipment or software we procure on your behalf ("Procured Equipment") may carry manufacturer warranties, which we'll pass through to you where possible. We don't make any separate warranties about the quality or usefulness of Procured Equipment ourselves. Some items may not be returnable, or may carry third-party restocking fees — those costs are yours if a return is requested. We're not a repair center, but we'll help facilitate warranty returns/repairs; however, the terms of the manufacturer's warranty (if any) govern, and we're held harmless for the outcome. Once Procured Equipment is handed to a shipping carrier, we're not responsible for its condition, quantity, or delivery timing.

Strategic Guidance & Quarterly Reviews

Advice we provide is based on standard industry practice and our understanding of your specific situation. Recommending a particular product or vendor doesn't mean we're endorsing that manufacturer over others.

Virtual CTO / CIO Services

Guidance we provide in a virtual CTO/CIO capacity is for informational and educational purposes only. We don't hold an actual officer or director role at your company, and no fiduciary relationship is created. You should not list Techo on your corporate records or accounts.

Sample Policies & Procedures

We may occasionally share sample/template policies for your use. These are informational only — not legal advice — and shouldn't replace guidance from qualified legal counsel. We don't guarantee these templates are complete, accurate, or sufficient for your specific needs, or that using them eliminates liability.

Penetration Testing & Vulnerability Assessments

Security devices and alarms (physical or virtual) may trigger during penetration testing, despite our best efforts to avoid this. You're responsible for notifying any alarm-monitoring company and law enforcement in advance about potential false alarms, and for ensuring those alarms aren't treated as real threats. Some advanced security systems may partially or fully shut down the Environment when triggered, causing downtime. We're not responsible for costs or claims arising from how a monitoring company or law enforcement responds, or from any shutdown triggered by an alarm/security system.

No Unauthorized Third-Party Testing

Unless we authorize it in writing, you may not run — or allow any third party to run — diagnostic or security testing against systems, protocols, or solutions we've implemented ("Testing Activity"). Diagnosing or fixing problems caused by unauthorized Testing Activity isn't covered under your Quote; if we agree to help, it's billed at standard hourly rates.

Hardware-as-a-Service Usage Terms

Equipment we host or supply ("Infrastructure") is for your internal business use only — no subleasing, sublicensing, or making it available to third parties without our written consent. You agree not to use the Infrastructure in a way that interferes with our other hosted equipment or with services we provide to other clients. We may throttle or suspend access if we reasonably believe your use violates your Quote, this SOW, or our governing agreement.

Equipment & Software Obsolescence

If any part of your environment becomes outdated, reaches end-of-life, or loses manufacturer support ("Obsolete Element"), we may mark it unsupported and ask you to replace it within a reasonable window. If you don't, we may either (a) continue supporting it on a best-efforts basis with no warranty around its functionality, or (b) remove it from the scope of Services with written notice (email is sufficient). Either way, we make no warranty regarding any Obsolete Element.

Hosting & Acceptable Use

You're responsible for how your users use the Services, and you agree that neither you nor your staff/representatives will violate applicable laws or regulations while using them.

You also agree that you and your team will not:

- Send unsolicited bulk/commercial email or engage in spamming
- Carry out denial-of-service attacks against any website or service
- Infringe on copyrights, trademarks, patents, trade secrets, or other proprietary rights
- Collect or disclose personal information without consent or proper legal basis (and if you collect it, you must maintain a privacy policy disclosing your data practices)
- Take any action that harms or could harm Techo or our infrastructure

You're solely responsible for keeping your login credentials secure and used only by authorized users. We have no liability for unauthorized use of your credentials. If credentials are lost, stolen, or compromised — or you suspect unauthorized access to hosted applications/data — notify us immediately so we can reset access. We'll act on such requests as quickly as reasonably possible.

Software Licensing Responsibility

If we're asked to reinstall or replicate software you provide as part of the Services, it's your responsibility to confirm it's properly licensed. We may require proof of licensing before installing or reinstalling software. License acquisition costs aren't included in your Quote unless explicitly stated.