Services Guide

This Services Guide contains provisions that define, clarify, and govern the services described in the quote provided to you (the "Quote"). If you do not agree with the terms of this Services Guide, you should not sign the Quote and you must contact us for more information.

This Services Guide is our "owner's manual" that generally describes all managed services provided or facilitated by Northwest Hitech Solutions, LLC d/b/a Atekro ("Atekro"); 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.

Auditing Services

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:

- 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
- Cyber 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If deficiencies are discovered during the auditing process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and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.

General Onboarding Services

If general onboarding services are provided under the Quote, then one or all of the following services may be provided to you. The exact onboarding service(s) will be included in the Quote.

- Uninstall any monitoring and remote management tools or other software installed by previous IT consultants.
- Compile a full inventory of all protected servers, workstations, and laptops.
- Uninstall any previous virus protection and install our managed cyber security services.
- 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.
- Review Network Segmentation and IP Address Strategies
- Stabilize network and assure that all devices can securely access the file server.
- 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.

The foregoing 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.

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.

Managed Services

The following Services, if listed in the Quote, will be provided to you. All endpoint managed services require Remote Management on all managed endpoints and devices.

SERVICES	GENERAL DESCRIPTION
Remote Management	Software agents installed in Covered Equipment (defined below) that allow the following on a 24x7 basis: • remote access and management • execution of management scripts • installing and uninstalling software and/or agents • monitor and alerting • Install optional system tray icon and menu • execute and management of additional managed services as described below Note: All equipment covered by any managed services are required to have a remote management agent installed. This service does not include Basic Monitoring (see description below).
Basic Monitoring	Applies to Workstations & Servers • Setup and configure CPU usage, memory usage, & available disk space monitoring on a 24x7 basis. • Alerts are generated and responded to in accordance with the Client's remediation instructions. Remediation is prioritized in accordance with the Service Levels described below.
Advanced Server Monitoring - Applications	Applies to Servers Only • Basic Monitoring add-on to provide additional monitoring of critical services provided by a server. • Setup and configure monitoring & alerting which may include server applications, windows services, event logs, folder shares, etc.… The exact services to monitor will be listed in the quote. • Alerts are generated and responded to in accordance with the Client's remediation instructions. Remediation is prioritized in accordance with the Service Levels described below.
Advanced Monitoring - Active Directory	Applies to Servers running Active Directory Only • Setup and configure health monitoring for Active Directory controllers and alert when unhealthy. • Alerts are generated and responded to in accordance with the Client's remediation instructions. Remediation is prioritized in accordance with the Service Levels described below. Additional details are below.
Remote Monitoring & Management - Network	• If cloud management is available for installed equipment, we will register all covered network devices into our cloud management platform. • If included in the Quote, we will setup & configure additional monitoring agents to monitor the general health of the network including monitoring gateways, routers, switches, Wi-Fi nodes, and internet access. This may require an additional appliance and/or computer to be installed onsite. • Alerts are generated and responded to in accordance with the Client's remediation instructions. Remediation is prioritized in accordance with the Service Levels described below.

Critical & Security Patching	Applies to Workstations & Servers • Configure and Schedule automatic patching for all critical and security updates published by Microsoft on all managed Windows workstations and servers on a predetermined schedule. • Investigate any patch that failed to apply in accordance with the Service Levels described below. • If any patch is deemed as problematic, then we will blacklist and prevent the patch from installing.
Windows Feature Update Patching	Applies to Workstations & Servers • Review Windows minor feature enhancements, bug fixes, and service packs as deemed necessary and remotely applied based on a predetermined schedule. • Any major updates (i.e. major version upgrades) are project bases will be quoted and scheduled as a separate project.
Basic Anti-Virus	Applies to Workstations & Servers • Atekro will install and configure a signature based anti-virus on all managed workstations and servers. • Configure automatic updates for signatures and scanning engine.
Advanced Cyber Security for PC	Applies to Workstations & Servers • Atekro will install an Advanced Threat Detection agent with Real Time Scanning and AI Threat Detection on all managed workstations and servers. • Onboarding may take up to 1-2 weeks or more depending on the number of workstations and servers managed. • Once the onboarding is complete and the Advanced Threat Detection agent is running, we'll remove any existing Anti-Virus and notify you that you are running in full protection mode. • We will configure automatic updates to include updates to the Threat Detection agent and/or any updated data or signature files needed to stay up to date. • If a Cyber Threat is detected by the installed monitoring agent, it may perform the following based on the level of threat: • attempt to quarantine, isolate, and/or delete the file, script, and/or the application that is identified as a possible threat. • may isolate the workstations, server, or laptop from the network so that the threat does not spread. • may alert the user that a Cyber Threat has been detected and what action was taken. • If Managed Detection & Response is included, then additional action may be performed based on the Security Analyst's findings. Please see below. If additional remediations or recovery are recommended and/or required, you will be informed (email is ok for this purpose) and quoted based on the current pricing. This includes but not limited to rebuilding and/or replacing the workstations or servers, cleaning and reinstalling the removed application, replacing broken scripts, etc…
Advanced Cyber Security - Microsoft 365	• Atekro will Integrate the Advance Threat Detection service into your Microsoft 365 (Office 365) and optionally SharePoint, MS Teams, and OneDrive cloud services.

- Onboarding will include a Monitoring Only period for 1-5 days, possibly up to 2 weeks, for the purpose of learning typical system behavior so that appropriate policies can be applied.
- We will review and configure all policies.
- If a threat is detected, the email will be quarantined and alert sent to the recipient.
- If the threat detection agent only suspects that an email may be a threat, it will provide addition information to the recipient so that they can make the final determination.

Advanced Managed Detection & Response (MDR)

This is an Add-On service for Advanced Cyber Security for PC and/or Advanced Cyber Security for Microsoft 365

Once onboarding for Advanced Cyber Security for PC and/or Advanced Cyber Security for Microsoft 365 is complete, we will perform the following:

- Atekro will integrate your Advance Cyber Security agents (PC and/or M365) with our Security Operations Center for 24/7/365 cyber threat monitoring and response.
- If a threat is detected by our Security Operations Center, our cyber security analysts will quickly assess the threat and respond as needed. This may include one or more of the following:
    - Quarantine and/or remove the source of the cyber threat.
    - Quarantine the entire computer and remove all network access (prevent the threat from spreading)
    - Hunt for the threat within all other computers within your company.
    - Then hunt for the threat within any other company that is monitored.
    - If the threat is found in other computers, similar action may be performed.
- If action was taken against a cyber threat, you will be notified with details of the threat and any action taken.

If additional remediations or recovery are recommended and/or required, you will be informed (email is ok for this purpose) and quoted based on the current pricing. This includes but not limited to rebuilding and/or replacing the workstations or servers, cleaning and reinstalling the removed application, replacing broken scripts, etc…

Data Loss Protection for Email (DLP)

Requires Advanced Cyber Security for Microsoft 365

- Atekro will integrate Data Loss Protection for Email (DLP) into the mail flow which monitors all outgoing email for personal and/or sensitive data.
- The detection engine uses data patters to detect personal and/or sensitive data. Additional data detection patterns can be added on request and will incur additional fees for creating and testing new patters. Fee will be based on Atekro current pricing.
- If sensitive data is detected, an email will be sent to your administrator notifying them of the sensitive data. Depending on your configuration, the administrator can do the following:
    - Review the email and the user's reason why they are sending.
    - Reject or allow the email to be sent.

Cyber Security Training for Employees

- Atekro will create your management & employee training portal and upload your initial list of employees. A excel/csv list of employees will be required. We will provide you a template to use.
- After the initial onboarding, you, as a manager, will be able to view, add, update, and deactivate employees.
- Managers will be able to track user's training progress and score.

	• Registered employees will receive a link to the online portal where they can do the following: • Watch Cyber Security training videos with optional close caption and then take a retention test. • View Cyber Security short videos for ongoing general education. • View their progress and current training status. • All employee training is valid for 1 year. After 1 year, all employees are required to rewatch all cyber training videos. • Cyber Security shorts will be sent on a weekly basis to all registered employees. You may request that they only be sent to employees who have finished their training. • Managers will be able to send communication emails to all or selected registered employees. • Atekro will also provide an additional add-on module which will allow you to create simulated phishing attacks. If a user clicks a simulated email link and/or fills in data in a simulated form, the user will be notified and flagged for retraining.
Cyber Security Policy Management for Employees	Requires Cyber Security Training for Employees • Install and activate the Policy management module within the Cyber Security Training for Employees service. • Atekro will provide you a list of default polices templates that you can select, edit and publish to your employees. In addition, you'll also be able to create your own policies from scratch. Once published to your employees, they will be notified and required to read and acknowledge. • You'll be able to track which employees have read and acknowledged each policy. • All employee policy acknowledgement is valid for 1 year. After 1 year, all employees will be required to review and re-acknowledge all company policies.
Dark Web Monitoring	Requires Cyber Security Training for Employees • Atekro will register your domain URL and up to 5 domain emails for dark web monitoring. • If your URL or any of the 5 emails is found on the Dark Web, an email notification will be sent to all the managers. Additional URL monitoring is an additional fee.
Incident Response, Reporting and Documentation	Requires Cyber Security Training for Employees • Atekro will provide an additional add-on module to the Cyber Security Training for Employee portal for documenting, categorizing, and tracking security incidents.
Vulnerability Assessment	• Atekro will provide a questionnaire regarding your existing cyber security protection related to the security of your network. • Once completed, Atekro will review and develop an action plan to address any vulnerabilities identified. Implementing any actions items identified by the vulnerability assessment are not include. Atekro will provide a Statement or Work and Quote for any and all action items and/or projects recommended.
Embedded Content Filter for Employee Workstations	Applies to Workstations & Servers Content filtering is managed by policy in the cloud and is attached to a "Zone" (one zone is included). Additional Zones will incur a separate onboarding fee. Each

	workstation in a zone will retrieve the policy and enforce directly on the workstation. As changes are made to the policy in the cloud, the workstation agent will download the updates and enforce. • During onboarding, Atekro will perform the following: • Create and configure a single zone with a single content filtering policy. Filtered content my be done by browser, DNS, or both. • Meet with you to review all categories and/or URLs to filter, whitelist, and/or blacklist. • Install an agent on all workstation covered in the zone via our Remote Management agent. • If changes are needed to a policy, a request can be sent to our support team via any of the methods outline below. All changes will be performed during normal business hour and according to our services levels described below.
Managed Backup to Cloud	Applies to Workstation and Servers • Configure the cloud storage zone or zones for all workstations and servers. • Create and configure backup and retention policies. • If included in the Quote, we will also configure a local storage device and configure backup policies to store backups on the local storage device. This may be in addition to the cloud backups. It may also require additional hardware. • Install a backup agent on all covered workstations & servers and configure to use the appropriate backup policy or policies. • Monitor and verify all backups via manual and/or automated verifications systems. All manual inspections will be done on a regular schedule basis deemed appropriate by Atekro, unless otherwise stated in the Quote. • If a backup fails, Atekro will investigate and determine the cause of failure. If the repair is not minor, e.g,. the workstation and/or server has become corrupt or the hardware has failed, the repair may be billed separately at Atekro's current rates. We will provide you with written notice (email is acceptable for this purpose) and obtain your consent before performing any repair services for which fees will be charged. In the event of a complete system loss, please see our Disaster Recovery Service. If one or more individual files are lost and need to be recovered from a backup, please see Lost File Recovery. For more details, see below.
Managed Backup to Cloud – M365	Applies to Microsoft 365 Cloud Services • Integrate our cloud backup agent into Microsoft 365 account. • Create and configure backup and retention policies. • Monitor and verify all backups via manual and/or automated verifications systems. All manual inspections will be done on a regular schedule basis deemed appropriate by Atekro, unless otherwise stated in the Quote. • If a backup fails, Atekro will investigate and determine the cause of failure. If the repair is not minor, e.g,. the workstation and/or server has become corrupt or the hardware has failed, the repair may be billed separately at Atekro's current rates. We will provide you with written notice (email is acceptable for this purpose) and obtain your consent before performing any repair services for which fees will be charged.

Lost File Recovery	Managed Backup to Cloud is required. Individual file recover from backup is performed and billed based on Atekro's current rates unless otherwise stated in the Quote. For more details see below.
Disaster Recovery Service	• Atekro will execute full system recovery in the event of total system loss. • Managed Backup to Cloud services are required. For full details, see below.
Single Sign-On (SSO) Integration with MFA	SSO integration services are quoted, implemented, and billed in two phases. 1) Assess all current systems and create an SSO Implementation Plan. 2) Implement according to the SSO Implementation Plan Phase 1, we will provide the following: • Atekro will review all current users, user management systems, software solutions, assets, and sign-in strategies and recommend an SSO provider. • Atekro will prepare an SSO Integration Plan with the selected SSO provider. This will include the following: • General SSO integration strategy including configuration overview. • Identify all required user data for synchronization. • Identify all software, onsite & cloud, to integrate with the SSO provider. • Identify one or more MFA types to configure. • Identify and recommended SSO security policies. • Identify any work required by your company. • Create a testing plan for testing during all phases of implementation. • Atekro will schedule a 1-hour meeting to review with you our findings and the Integration Plan. We will also include a Quote for Phase 2, the implementation of the SSO Integration Plan. Phase 2, we will provide the following: • Atekro will configure your user management system integration with the selected SSO according to the SSO Integration Plan. • Atekro will integrate all software solutions identified in the SSO Integration Plan with the selected SSO provider. • Atekro will test and verify all integrations according to the SSO Integration Plan.
Cyber Security Insurance Compliance	IMPORTANT! Atekro does NOT offer Cyber Security Insurance directly. We have, however, partnered with a Cyber Security Insurance broker who can provide Cyber Security Insurance. If included in the Quote, Atekro will assist in facilitate and securing a Cyber Security Insurance Policy through a separate licensed Insurance broker or agent. As part of this service, we will provide the following: • Atekro will summit you to our Cyber Security Insurance partner in order to start your application process. • Atekro will work with you and the insurance provider, broker and/or agent to assist in satisfying insurance compliance requirements for the purpose of securing a Cyber Security Insurance Policy. Note, any additional work required by the

insurance provider, broker, or agent that is NOT part of the quote will be an addition fee and a separate Quote and Statement of Work will be required.

NOTE! Atekro can **NOT** guarantee an insurance policy will be grated.

Employee Onboarding Service

Employee onboarding services are for new or existing employees that need a new workstation and/or laptop. Services includes creating their user account in Active Directory and setting up their workstation and/or laptop for company use. This includes the following:

- Optionally, Atekro will procure a predefined business-grade workstation or laptop. If the exact model is not currently available from one of our normal distributors, we'll order a similar like kind model with equivalent or better features.
- Atekro will install all critical, security, incremental features updates and/or patches. This does not include any major OS updates. i.e., Windows 10 upgrades to Windows 11.
- Atekro will create the new employee user in Active Directory and assign them the requested security groups.
- Atekro will attach the workstation or laptop to your Active Directory domain.
- Atekro will install common software include Google Chrome (optional), 7-Zip, Adobe Reader, and our remote management agent. We may install additional software if listed in the quote or agreement.
- Optionally, Atekro will install Office 365 included Outlook and configure for the user's email. Office 365 user license is separate.
- Atekro will turn on BitLocker and securely store the BitLocker key in our secure client documentation application.
- If you have any of the other managed services we offer, Atekro will also install the required software and/or agents for that managed service. **<u>IMPORTANT</u>**: There will be additional costs for onboarding each workstation, and your monthly fees will be automatically increased to accommodate the change(s) to the managed IT environment.
- Optionally, Atekro will then package and ship the device to your new employee. The shipping and handling fee is separate and is dependent on the shipping costs and distance.
- If the employee is not new and getting a new replacement computer, then we will also copy their desktop and all "My Documents" folders include Documents, Music, Pictures, and Videos. Additional folders copied on request only.

The following restrictions apply:

- All hardware not previously purchased, will required payment before hardware can be ordered from our vendors.
- This service is not available for used or remanufactured computers with the following exception of any previously offboarded computer(see below) and is deemed reusable.
- New/replacement computers must be business-grade machines (not home) from a major manufacturer like Dell, HPE, or Lenovo.

Employee Offboarding Service

Employee Offboarding Service is similar Onboard but is for when an employee leaves the company and/or an employee needs a new workstation or laptop. This service includes the following:

- If you have any of our Managed Backup Services, Atekro will create a final backup of the workstation or laptop and retained according to the backup retention policy.

	• Atekro will completely reset the OS to its factory install. This includes the removal of all software, files, document, phones, etc… • If the workstation or laptop is to be retained/used in the managed environment, then prior to re-implementing the machine we will use industry standard methods to delete all prior data on the machine, rendering such data irrecoverable under normal circumstances. • If the workstation or laptop is not to be retained for future use, then we will physically destroy all storage devices on the machine to render all data on that machine irrecoverable.: ○ We will erase and/or destroy all hard drives.

Additional Description of Managed Services

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

Advanced Monitoring - Active Directory

We will actively monitor Active Directory to ensure the health of Active Directory. We may use existing monitoring agents, install additional agents, or execute health check scripts as needed. If any of the health checks fails, an alert will be sent to our technical team. Depending on your service levels, the team will either alert you and/or investigate and fix any minor issues found depending on your remediation response options.

If the repair is not minor, e.g,. the server has become corrupt or the hardware has failed, the repair may be billed separately at Atekro's current rates. We will provide you with written notice (email is acceptable for this purpose) and obtain your consent before performing any repair services for which fees will be charged.

If you have any issues that might indicate a problem with Active Directory, please submit a support ticket. See details below.

Managed Backup to Cloud

Managed Backup to Cloud is a backup service where backups can be sent directly to a dedicated backup cloud data center. No onsite device is required. A good reliable fast internet connection is required.

The Managed Backup to Cloud solution also supports saving backups to a local storage device. In this scenario, a second local copy of the backups can be created. This is very beneficial in that it creates multiple backup copies and can provide faster physical recovery. E.g. A recovery directly from the cloud can take longer due to the speed of transmitting the backup over the internet whereas a local backup can transmitted quicker. This only applies to servers and workstations that are on premise. i.e. They are on the same office/network as the local storage device.

While we will make every effort to ensure the integrity of the backups, we do not guarantee the integrity of any one backup increment or snapshot. In the event of a corrupted and/or a cyber security infected backup, backup recovery will depend on the point of the last successful un-infected backup.

Backup Retention

For server backups using a local storage device, the retention period is highly dependent on the size of the appliance and how many backups are saved to it.

For all backups sent directly to the cloud, we will configure the retention policy based on agreed policies. We will review and monitor backup retentions, as deemed necessary, to ensure policies are followed.

For Managed Backup to Cloud services that includes backup storage, usually in GB, any covered device's backups that exceed the allotted space may incur additional storage costs. While we aim to quote and allocate an appropriate amount of backup storage, we do not guarantee you will not exceed.

Virtual Recovery

Our Managed Backup to Cloud solution supports virtual recovery in the cloud. In the event of a system wide failure due to a catastrophic event which may include fire, flood, or a cyber-attack like ransomware, a virtual environment can be created very quickly using your backups stored in the cloud.

Important: Due to Microsoft Licensing, virtual recovery for Windows desktop workstations is not supported.

Please see our Disaster Recovery Service for more details.

Lost File Recovery

Managed Backup to Cloud is required.

Individual file recover from backup is performed and billed based on Atekro's current rates. If you need to recover any of your individual backed up file(s), then the following procedures will apply:

Request Method:
Requests to restore backed up data should be made through one of our normal service request methods (see below). Detail information about the file name, extension, and original stored location should be included in the request. Without this information, we will not be able to reliably identify and retrieve the file.

Service Hours:
File recovery requests will be perform during our normal business hours which are posted on our website. If request is outside of normal business hours and/or is deemed urgent, we will do our best to deliver the files as fast as possible but this is depended on the availability of a support tech. All file recoveries performed outside of normal business hours will incur fees based on the non-business hour support fees (see below).

Restoration Time:
We will endeavor to restore backed up data as quickly during normal hours as possible following our receipt of a request to do so; however, in all cases data restoration services are subject to technician availability. Unless the request is deemed urgent, all data restorations under 500MB will be performed at service level P4 (see below). Data restoration exceeding 500 MB will be handled similarly but given the size of the data, it may take longer.

File(s) Delivery:

If Remote Management is installed on the desired workstation or server and files are no large then 100 MB and your devices is online with a fast reliable internet connection, we may upload your recovered file(s) directly to your workstation or server and notify you of their location. If the file(s) are larger than 100 MB, the device is offline, or it does not have a fast reliable internet connection, we will send your files via another method which may incur additional charges for a storage device(s) (flash drive, mobile drive, etc…) and shipping & handling.

Disaster Recovery Service

Managed Backup to Cloud service is required.

Disaster Recovery Service is required when a workstation, server, or environment is completely compromised and/or damaged beyond repair. This includes any force majeure event including fire, flood, or a cyber-attack like ransomware. In order to recover any workstation, server, or complete environment, full backups are required on all effected equipment.

Disaster Recovery Service will be billed on a time and materials basis. Due to the nature of disaster recovery, time and costs cannot be estimated reliably. If this is a cyber-attack like ransomware and you have cyber security insurance, your insurance policy may cover all or some of the cost of recovery. We cannot guarantee coverage! Please consult with your insurance company for your actual coverage.

While we will make every effort to ensure the integrity of the backups, we do not guarantee the integrity of any device backup, backup increment, or snapshot. In the event of a corrupted and/or a cyber security infected backup, backup recovery will depend on the point of the last successful un-infected backup.

Important Notes about Virtual Recovery!

- *Due to Microsoft Licensing, virtual recovery for Windows desktop workstations is not supported.*
- *Many advance cloud features including but it not limited to, AWS Lambdas, Azure Functions, Service Meshes, Cloud Queues, etc… are not supported.*
- *In these cases, we must perform recovery directly to the device or cloud service.*

Request for Recovery

In the event of a completely compromised workstation, server, or environment, a support request should be sent immediately to our support team and/or your account manager via any of the method detailed below. Once we receive your request, we will begin the recovery process based on our below service levels.

Recovery Process

Phase 1 (Virtual Recovery):

We will create and start all virtual servers in our recovery cloud system. The order in which they are started will be based on your priorities and our disaster recovery plan. If available, we'll create a remote VPN link to your onsite network for connectivity. Once the virtualized environment is running, we will move to Phase 2.

> **Note**: *Our Managed Backup systems, when running in a recovered virtual environment, will continue to perform backups. When recovery is eventually performed on the physical device, it will include all new data while working in the virtual environment.*

Phase 2 (Physical Recovery):

Once all virtual servers are running in the virtual environment, we will begin planning and executing recovery to the physical devices, including workstations, laptops, VM Host, Virtual Machines, and cloud servers.

We will identify, organize, and schedule the order in which to recover all physical and/or virtual (cloud) devices according to your priorities our disaster recovery plan. Depending on the level of damage, new hardware may be required which will affect the schedule and cost. We will provide you a quote for all equipment required. Once we begin the physical recovery process, we will require direct access to the device or cloud services which may incur an onsite travel fee. Once a physical device is recovered, the virtual device will be shut down and the user must use the physical device.

Billing and Invoicing

All hardware and software must be paid in advance before we order the applicable devices/licenses from our distributors unless other arrangements are made in advance and in writing.

Unless specified in the quote or statement of work, the following billing policies will be in effect:

- All labor-based services, including projects, onboarding, support tickets, etc…, will be invoiced in arears every two weeks for actual time accrued.
- All ongoing monthly managed services will be invoiced in advanced. Any changes to the managed environment causing changes in quantity during that billing period will be prorated and included in the following month's invoice.

Covered Equipment / Hardware / Software

For services that are provided on a "per user" basis, our managed services will be provided for only one (1) Business Device 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."

Please note: Additional devices will require additional monthly monitoring/maintenance fees; please see your Quote for more details.

The Services will apply to the software listed in the Quote ("Supported Software") provided, however, that all Supported Software must, at all times, be properly licensed, and under a maintenance and support agreement from the Supported Software's manufacturer. In this Services Guide, Covered Hardware and Supported Software will be referred to as the "Environment" or "Covered Equipment."

Physical Locations Covered by Services

Services will be provided remotely unless, in our discretion, we determine that an onsite visit is required. Onsite visits will be scheduled in accordance with the priority assigned to the issue (below) and are subject to technician availability. Unless we agree otherwise, all onsite Services will be provided at Client's primary office location listed in the Quote. 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 Atekro' 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").

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 thirty (30) days before the end of the then-current Service Term. In addition, unless we agree otherwise in advance of a renewal term, the fees for the Services will be automatically updated to reflect the fee pricing/structure in place as of the date of renewal.

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.**

Assumptions / 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 a version that is currently supported by Microsoft and have all critical, security and service packs updates installed.
- All software must be genuine, licensed and vendor supported.
- All Servers, Workstation, and Laptops must be protected, at a minimum, a licensed and up-to-date signature-based virus protection software.
- The Environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored.
- All wireless data traffic in the 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, including all managed devices.
- Client must not affix or install any accessory, addition, upgrade, equipment, or device on to the firewall, server, or NAS appliances (other than electronic data) unless expressly approved in writing by us.

Exclusions

Services that are not expressly described in the Quote will be out of scope and will not be provided to Client unless otherwise agreed, in writing, by Atekro. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by Atekro in writing:

- 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 Environment up to the Minimum Requirements (unless otherwise noted in "Scope of Services" above).
- 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.
- We will not perform any service that is considered, according to Atekro, illegal, immoral, unethical, etc.
- Technical Service Requests (Support Tickets)

Service Levels

Automated monitoring is provided on an ongoing (*i.e.*, 24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our normal published business hours (excluding legal holidays and Atekro-observed holidays—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 Atekro at our discretion after consulting with the Client. All remediation services will initially be attempted remotely; Atekro will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

Severity	Trouble Description	Response Time
P1 (Critical)	Service not available causing critical business function to be unavailable and no workaround exists. (*e.g.*, all users and functions unavailable causing critical business stoppage)	Two (2) business hours after notification.
P2 (Severe)	Significate degradation or outage affecting critical business functions and a workaround exists; or only affects a small, limited number of users. (e.g., does affect critical business systems directly and/or users have a work around available.)	Four (4) business hours after notification.
P3 (Limited)	Significant Degradation or outage that does not directly affect critical business system. (*e.g.*, critical business systems can continue as normal without any immediate consequences)	Eight (8) business hours after notification.
P4 (Normal)	Small System Degradation that does not have a direct impact on users or critical business systems. (*e.g.*, critical business systems can continue as normal or only a few users are affected).	Two (2) business days after notification.
P5 (Low)	No Degradations of any business systems and no users are affected. This covers all change requests, new projects, scheduled maintenance, scheduled services, etc.… New projects will be scoped and scheduled separately.	Four (4) business days after notification or provide quote and schedule.

* All time frames are calculated as of the time that Atekro is notified of the applicable issue / problem by Client through Atekro' 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 are offered on a case-by-case basis and are subject to technician availability. If Atekro agrees to provide off-hours/non-business hours support ("Non-Business Hour Support"), then the 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:

Off-Hours	Rate Multiplier
Weekdays	1.5x
Weekends	2x
Atekro Observed Holidays	3x

All hourly services are billed in 15 minute increments, and partial increments are rounded to the next highest increment. A one (1) hour minimum applies to all Off-Hours/Non-Business Hour Support.

Atekro-Observed Holidays:

Atekro observes the following holidays:

- New Year's Day
- Martin Luther King Jr. Day
- President's Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- The day following Thanksgiving Day
- Christmas Eve – Half Day
- Christmas Day
- New Year's Eve – Half Day

If a holiday falls on a non-working business day, then the holiday will be observed on the closest business 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.

Requesting Additional Services

If additional services are requested, please include details about the services being requested and any relevant information via any of the methods below. We'll then schedule a follow up to review the request.

- Contact sales department by email or using our contact form on our website.
- If you have an account manager assign, you can email and/or call them directly.
- If you do not have an account manager assigned, then you can email clientmanager@atekro.com.

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, then you agree that the fees will be automatically and immediately modified to accommodate those changes.

Minimum Monthly Fees

The initial Fees indicated in Quote are the minimum monthly fees ("MMF") that will be charged to you during the term. You agree that the amounts paid by you under the Quote will not drop below the MMF regardless of the number of users or devices to which the Services are directed or applied, unless we agree to the reduction. All modifications to the amount of hardware, devices, or authorized users under the Quote (as applicable) must be in writing and accepted by both parties.

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 sixty (60) 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 sixty (60) 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.

Travel Time

Unless included in the quote, if local onsite services are required, a travel fee will be added at 1 ½ hours of our normal rates and will cover up to 25 driving miles from our office. This fee will be waived if billable onsite work is 6 hours or more for that day's work. Any distance beyond 25 driving miles will be billed to you at our 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 hourly rate (or non-business hourly rate, 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.

Check

You may pay by check provided that your check is delivered to us prior to the commencement of Services. Checks that are returned to us as incorrect, incomplete, or "not sufficient funds" will be subject to a $50 administration fee and any applicable fees charged to us by your bank or financial institution.

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 will 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. Each NCE License that we purchase may require a one (1) or three (3) year term. 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.

Removal of Software Agents

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 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 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 Atekro 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.

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 Atekro, 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 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

Cyber Security/Anti-Virus Protections

Our Cyber Security and Anti-Virus services utilize third party solution providers. These services can be highly effective tools in preventing cyber attacks and virus infiltrations; however, we cannot and do not guarantee that you won’t have a cyber security or virus infiltration.

Our anti-virus / anti-malware 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. In addition, 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. Moreover, we cannot and do not guarantee that you won’t have a cyber security or virus infiltration. In order to improve security awareness, you agree that Atekro 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.

Environmental Factors

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

Fair Usage Policy

Our Fair Usage Policy ("FUP") applies to all Services that are described or designated as "unlimited." An "unlimited" service designation means that, subject to the terms of this FUP, you may use the 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 Atekro 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. Atekro 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 Atekro believes, in its discretion, that Client's email account(s) is/are being used in an improper or illegal manner.

Patch Management

If Patch Management services are included in the Quote, then 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 Atekro nor its designated affiliates will be responsible for the outcome or results of such activities.

Cloud based 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. Atekro cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Atekro 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 Atekro 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, Atekro 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. Atekro is not a warranty service or repair center. Atekro 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 Atekro will be held harmless, and (ii) Atekro 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.

Quarterly Business Review; IT Strategic Planning

Suggestions and advice rendered to Client are provided in accordance with relevant industry practices, based on Client's specific needs and Atekro' opinion and knowledge of the relevant facts and circumstances. By rendering advice, or by suggesting a particular service or solution, Atekro is not endorsing any particular 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. Atekro 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 Atekro 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 is 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.

HaaS

You will use all Atekro-hosted or Atekro-supplied equipment and hardware (collectively, "Infrastructure") for your internal business purposes only. You shall not sublease, sublicense, rent or otherwise make the Infrastructure 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 Infrastructure 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.

Obsolescence

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

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 Atekro 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. Atekro 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 Atekro immediately to request the login information be reset or unauthorized access otherwise be prevented. Atekro 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.

Vendor Management

If Vendor Management services are listed in the Quote, then Atekro will facilitate support between Client and the following vendors: Lenovo, Amazon AWS, Microsoft Azure including Azure AD and Microsoft 365, Synology, and Zyxel