Service Statement

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

This Service Statement is our "owner's manual" that generally describes all managed services provided or facilitated by Vision Technology Group, LLC ("VTG"); 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 Service Statement contains important provisions pertaining to the auto-renewal of the Services your Quote, as well as fee increases that may occur from time-to-time. Please read this Service Statement carefully and keep a copy for your records.

Onboarding Services

If onboarding services are provided under the Quote, then the following services will be provided to you.

- Uninstall any monitoring 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 antivirus application.
- 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 applicable devices.
- 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.

SERVICES	GENERAL DESCRIPTION
Remote Monitoring and Management	Software agents installed in Covered Equipment (defined below) report status and events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.
Backup and Disaster Recovery	• 24/7 monitoring of backup system, including offsite backup, offsite replication, and an onsite backup appliance ("Backup Appliance") • Troubleshooting and remediation of failed backup disks • Preventive maintenance and management of imaging software • Firmware and software updates of backup appliance • Problem analysis by the network operations team • Monitoring of backup successes and failures • Daily recovery verification Backup Data Security: All backed up data is encrypted in transit and at rest in 256-bit AES encryption. Backup Retention: Backed up data will be retained [for 14 days unless the customer requires more which will require additional storage] Backup Alerts: Managed servers will be configured to inform of any backup failures. Recovery of Data: If you need to recover any of your backed up data, then the following procedures will apply: • Service Hours: Backed up data can be requested during our normal business hours by submitting a service ticket to us by telephone or email. Or normal business hours are currently Monday- Friday 8AM to 5PM, and you will be notified if these hours change. Services may be provided during non-business hours; however, they are subject to higher fees and costs; see the "Service Levels" section below for details. • Request Method. Requests to restore backed up data should be made through one of the following methods: ○ Email: support@vtg.biz ○ Telephone: 540-437-0112

	• Restoration Time: We will endeavor to restore backed up data as quickly as possible following our receipt of your request to do so; however, in all cases data restoration services are subject to technician availability. Generally, we can restore between 0 and 100MB of data within 4 business hours of your request, and 100 MB to 500 MB within 8 business hours of your request. Data restoration exceeding 500 MB will be handled in accordance with technician availability.
Updates & Patching	• Deploy updates (e.g., x.1 to x.2), as well as bug fixes, minor enhancements, and security updates as deemed necessary on all managed hardware. • Perform minor hardware and software installations and upgrades of managed hardware. • Perform minor installations (i.e., tasks that can be performed remotely and typically take less than thirty (30) minutes to complete). • Deploy, manage, and monitor the installation of approved service packs, security updates and firmware updates as deemed necessary on all applicable managed hardware. • Servers will be patched after hours unless an emergency threat has been detected.
Firewall Solution	• Provide a FIPS 140-2 compliant firewall configured for your organization's specific bandwidth, remote access, and user needs. • Helps to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; provides website content filtering functionality.
Email Threat Protection	• Managed email protection from phishing, business email compromise (BEC), SPAM, and email-based malware. • Friendly Name filters to protect against social engineering impersonation attacks on managed devices. • Protection against social engineering attacks like whaling, CEO fraud, business email compromise or W-2 fraud. • Protects against newly registered and newly observed domains to catch the first email from a newly registered domain. • Protects against display name spoofing. • Protects against "looks like" and "sounds like" versions of domain names.
End User Security Awareness Training	• Online, on-demand training videos (multi-lingual). • Online, on-demand quizzes to verify employee retention of training content. • Baseline testing to assess the Phish-prone percentage of users; simulated phishing email campaigns designed to educate employees about security threats.

Hardware as a Service (HaaS)	• Provision and deployment of hardware provided as a service, i.e., any hardware or devices that are provided to you on a lease, rental, or loan basis. (Examples could include firewall appliances that are rented to you, and/or storage devices that are rented or loaned to you. Please see the Quote or other applicable schedule for complete hardware list – "HaaS Equipment") • Installation of HaaS Equipment. • Repair/replacement of HaaS Equipment (*see below for additional details*). • Technical support for HaaS Equipment. • Periodic replacement of HaaS Equipment (*see below for additional details*).

Labor for New / Replacement Workstations	Includes all labor charges for setup of new workstations, or replacement of existing workstations.
	
	• Labor covers:
	  ○ New computers / additional computers added during the term of the Quote;
	  ○ Replacement of existing computers that are four (4) or more years old (as determined by the manufacturer's serial number records);
	  ○ Replacement of existing computers that lost/stolen or irreparably damaged and/or out of warranty but not yet four years old;
	  ○ Operating systems upgrades – subject to hardware compatibility.
	
	The following restrictions apply:
	
	• Upgrades or installs of new or replacement computers are limited to three (3) devices per month unless otherwise approved in advance by VTG;
	• This service is not available for used or remanufactured computers;
	• New/replacement computers must be business-grade machines (not home) approved by Vision Technology Group.

Security as a Service (SeCaaS)	Unless otherwise stated in the Quote, our Security as a Service (SeCaaS) solution includes: • Firewall Solution (All Bundles) • Email Threat Protection (Essentials Plus, Complete, and Zero Trust) • End User Security Awareness Training (Essentials Plus, Complete, and Zero Trust) • Application Whitelisting (Complete and Zero Trust) • Multi-Factor Authentication (Zero Trust) • EDR (Essentials, Essentials Plus, Complete, and Zero Trust) • MDR (Essentials Plus, Complete, and Zero Trust) The SeCaaS Service may also include one or more of the following (please see the Quote for details): • Endpoint Detection and Response (EDR) services

- Utilizes artificial intelligence and machine learning to provide a comprehensive and adaptive protection paradigm in the managed environment.
- Detects unauthorized behaviors of users, applications, or network servers.
- Blocks suspicious actions before execution.
- Analyzes suspicious app activity in isolated sandboxes.
- Antivirus and malware protection for managed devices such as laptops, desktops, and servers.

- Managed Detection and Response (MDR) services
  - 24x7 managed network detection and response.
  - Real time and continuous (24x7) monitoring and threat hunting.
  - Real time threat response.
  - Alerts handled in accordance with our Alert Notification table, below.
  - Security reports, such as privileged activities, security events, and network reports, available upon request.
  - 24x7x365 access to a security team for incident response*

- Extended Detection and Response (XDR) services
  - A combination of our EDR and MDR services
  - Includes whitelisting for legitimate scripts and applications.
  - Includes dark web monitoring
    - 24x7 dark web monitoring for compromised, pre-designated company- or employee-related data.
    - 24x7 dark web monitoring for fully qualified domain name(s) used by Client.

- Application Whitelisting
  - In the field of Information Security, **Whitelisting** is an endpoint security solution that only allows tested, safe and approved applications to run on a device, computer or network system. Whitelisting security works in real-time and automatically updates to guarantee complete business data protection blocking all ransomware, malware, trojans, malicious scripts and other viruses

- Multi-Factor Authentication
  - A Two-factor authentication (2FA) is the simplest, most effective way to make sure users really are who they say they are. But, not every two-factor solution is the same. Some vendors only provide the bare minimum needed to meet compliance requirements – and some carry lots of hidden costs for deployment, operation and maintenance. Plus, many traditional solutions are clunky, error-prone and require extensive user training and support – costing your employees time and productivity.

Additional Description of Services

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

Hardware as a Service (HaaS)

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

Deployment. We will deploy the HAAS Equipment within the timeframe stated in the Quote, provided that you promptly provide all information that we reasonably request from you to complete deployment. This deployment guaranty does not apply to any software, other managed services, or hardware devices other than the HAAS Equipment. If you wish to delay the deployment of the HaaS Equipment, then you may do so provided that you give us written notice of your election to delay no later than five (5) days following the date you sign the Quote. Deployment shall not extend beyond two (2) months following the date on which you sign the Quote; as long as inventory is available.

Equipment Hardware Repair or Replacement. VTG will repair or replace HAAS Equipment by the end of the business day following the business day on which the applicable problem is identified by, or reported to, VTG and has been determined by VTG to be incapable of being remediated remotely.

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

Periodic Replacement of HaaS Equipment. From time to time and in our discretion, we may decide to swap out older HaaS Equipment for updated or newer equipment. (Generally, equipment that is five years old or older may be appropriate for replacement). If we elect to swap out HaaS Equipment due to normal, periodic replacement, then we will notify you of the situation and arrange a mutually convenient time for such activity.

Return of HaaS Equipment. Unless we expressly direct you to do so, you will not remove or disable, or attempt to remove or disable, any software agents that we installed in the HaaS Equipment. Doing so could result in network vulnerabilities and/or the continuation of license fees for the software agents for which you will be responsible, and/or the requirement that we remediate the situation at our then-current hourly rates, for which you will also be responsible. Within ten (10) days after the termination of HaaS-related Services, Client will provide VTG access to the premises at which the HaaS Equipment is located so that all such equipment may be retrieved and removed by us. If you fail to provide us with timely access to the HaaS Equipment or if the equipment is returned to us damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

Covered Equipment / Hardware / Software

Managed Services will be applied to the equipment listed in the Quote ("Covered Hardware").

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 Service Statement, 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 VTG's satisfaction.

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

Auto-Renewal. After the expiration of the initial Service Term, the Service Term will automatically renew for contiguous terms of one (1) year each 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.

Microsoft NCE Licensing: Regardless of the reason for the termination of the Services, you will be required to pay for all NCE Licenses that we acquire on your behalf. Please see "Microsoft Licensing 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 then-currently supported versions of such software and have all of the latest Microsoft service packs and critical updates installed.
- All software must be genuine, licensed and vendor-supported.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The 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 Service Statement.
- Client must provide us with exclusive administrative privileges to the Environment. If Client requires administrative (or "root") access, Client may be required to execute a waiver in VTG's favor before such access is provided by to Client or Client's designated representative.
- 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 VTG. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by VTG in writing:

- Customization of third party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- Battery backup replacement.
- Equipment relocation.
- The cost to bring the 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.

Service Levels

VTG's four Service/Security bundles fall under the following Classifications.

All bundles include the following 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 business hours unless otherwise specifically stated in the Quote. **Please note**: **The response times indicated below are service level objectives only, and may vary depending on the circumstances, such as third party delays, and/or parts or technician availability.**

We will respond to problems, errors, or interruptions in the provision of the Services in the timeframe(s) described below. Severity levels will be determined by VTG in our discretion after consulting with the Client.

All remediation services will initially be attempted remotely; VTG will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

	Response Time[1]	Normal Business Hours Monday – Friday, 8 AM to 5 PM	Extended Hours[2] Holidays, Non-Normal Business Hours
Phone	Live Answer	▪ For contact initiated during the normal business hours, a technician will respond to the issue in accordance with the severity levels/response times listed in the table, below. ▪ If an issue is not resolved during normal business hours, it will be logged and continued the following day. ▪ For contact initiated outside of normal business hours, a ticket will be logged, and work will begin on the next business day. ▪ For non-critical issues where a person is required onsite, we will schedule an engineer for an onsite visit in accordance with the severity of the problem and, at all times, subject to technician availability.	Extended hours are not included within the scope of our services unless "Extended Hours Technical Support" or something similar. A technician will respond to the issue in accordance with the severity levels/response times listed in the table, below. . **Additional / enhanced fees apply for technical services rendered during extended (i.e., non-business) hours. Please see below for details.** ▪ For non-critical issues where a person is required onsite, we will schedule an engineer for an onsite visit in accordance with the severity of the problem and, at all times, subject to technician availability.[4]
Email	4-48 Hours	Email support is for non-critical requests. ▪ Response time will vary from 4 hours to 48 hours depending on technician availability. Examples of non-critical requests are: ▪ Software installation ▪ Issues for which a workaround has been implemented ▪ Frequently asked questions (FAQ)-type requests ▪ Adding / Deleting users ▪ General consulting questions	

[1] **Response time is calculated from the time that the request for help is received by us though our designated support channels. Requests received in any other manner may result in delayed or non-responses.**

[2] **Technical support during extended (*i.e.*, non-business) hours are not included in the scope of our services unless the Quote expressly states that extended hour support is provided. Unless otherwise provided in the Quote (or unless extended hours are within the scope of services as expressly stated in a Quote, all technical support provided to you during extended hours will be billed at two times (2x) our then-current hourly rates, with a minimum of one (1) hour. All partial hours after the first hour are billed in fifteen (15) minute increments, with partial increments billed to the next higher increment.**

SEVERITY LEVEL(S)	RESPONSE TIME
Critical: Service not available (*e.g.*, all users and functions unavailable)	Response within two (2) business hours after notification.
Significant Degradation (*e.g.*, large number of users or business critical functions affected)	Response within four (4) business hours after notification.
Limited Degradation (*e.g.*, limited number of users or functions affected, business process can continue).	Response within eight (8) business hours after notification.
Small Service Degradation (e.g., business process can continue, one user affected).	Response within two (2) business days after notification.

* All time frames are calculated as of the time that VTG is notified of the applicable issue / problem by Client through VTG's designated support email, or by telephone listed in the Quote. Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts. Help desk support provided outside of our normal support hours will be billed to Client at the hourly rate of $150/hour (2 hour minimum applies).

Fees

The fees for the Services will be as indicated in the Quote. All amounts must be received by us within thirty (30) days of the invoice date.

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 service fees and, if applicable, data recovery 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 any third party services that we facilitate for you ("Pass Through Increases"). Since we do not control such 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. If onsite services are provided, we will travel up to 20 minutes from our office to your location at no charge. Time spent traveling beyond 20 minutes (*e.g.,* locations that are beyond 20 minutes from our office, occasions on which traffic conditions extend our drive time beyond 20 minutes one-way, etc.) will be billed to you at our then current hourly rates. In all cases you will be billed for all tolls, parking fees, and related expenses that we incur if we provide onsite services to you. In addition, we reserve the right to include additional service charges and/or administrative fees (not to exceed $20/onsite service call) to cover increases in fuel and fuel-related taxes and surcharges.

Appointment Cancellations. You may cancel or reschedule any appointment with us at no charge by providing us with notice of cancellation at least one business day in advance. If we do not receive timely

a notice of cancellation/re-scheduling, or if you are not present at the scheduled time or if we are otherwise denied access to your premises at a pre-scheduled appointment time, then you agree to pay us a cancellation fee equal to two (2) hours of our normal consulting time (or non-business hours consulting time, whichever is appropriate), calculated at our then-current hourly rates.

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

- **ACH**. When enrolled in an ACH payment processing method, you authorize us to electronically debit your designated checking or savings account, as defined and configured by you in our payment portal, for any payments due under the Quote. This authorization will continue until otherwise terminated in writing by you. We will apply a $35.00 service charge to your account for any electronic debit that is returned unpaid due to insufficient funds or due to your bank's electronic draft restrictions.
- **Credit Card**. When enrolled in a credit card payment processing method, you authorize us to charge your credit card, as designated by you in our payment portal, for any payments due under the Quote.

Microsoft Licensing Fees. The Services require that we purchase certain "per seat" licenses from Microsoft (which Microsoft refers to as New Commerce Experience or "NCE Licenses") in order to provide you with one or more of the following applications: Microsoft 365, Dynamics 365, Windows 365, and Microsoft Power Platform (each, an "NCE Application"). To leverage the discounts offered by Microsoft for these applications and to pass those discounts through to you, we 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 requires a one (1) year term, and NCE Licenses that are purchased at different times cannot be aggregated into a single term.** (By way of example: If we purchase NCE Licenses on your behalf on Jan. 1 ("Initial Licenses") and, six months later on June 1 we purchase additional NCE Licenses on your behalf ("Subsequent Licenses"), the Initial Licenses would expire on December 31; however, the Subsequent Licenses would expire on May 31 of the following year.) **For that reason, you understand and agree that regardless of the reason for termination of the Services, you are required to pay for all applicable NCE Licenses in full for the entire term of those licenses.** Provided that you have paid for the NCE Licenses in full, you will be permitted to use those licenses until they expire, even if you move to a different managed service provider.

Additional Terms

Authenticity

Everything in the managed environment must be genuine and licensed—including all hardware, software, etc. If we ask for proof of authenticity and/or licensing, you must provide us with such proof. All minimum hardware or software requirements as indicated in a Quote or this Services Statement ("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 VTG, 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 Service Statement 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

Anti-Virus; Anti-Malware

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. 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. In order to improve security awareness, you agree that VTG 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 VTG 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. VTG 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 VTG believes, in its discretion, that Client's email account(s) is/are being used in an improper or illegal manner.

VoIP/ Phone System

911 Dialing / Emergency Dialing - Limitations

The VoIP Service ("VoIP Service") may not support traditional 911 or E911 access to emergency services in all locations. The 911 dialing feature of the VoIP Service is not automatic; Client may be required to take affirmative steps to register the address where the VoIP Service will be used in order to activate the 911 Dialing feature. Client understands that Client must inform any users of the VoIP Service of the non-availability of traditional 911 or E911.

When a VoIP calling device is registered in a particular location, it cannot be moved without re-registering the device in the new location. Client agrees that it will not move any VoIP calling device without VTG's written consent. Client shall hold VTG harmless for any and all claims or causes of action arising from or related to Client's inability to use traditional 911 or E911 services.

When an emergency call is made, one or more third parties use the address of Client's registered location to determine the nearest emergency response location, and then the call is forwarded to a general number at that location. When the emergency location receives Client's call, the operator will not have Client's address and may not have Client's phone number. Client understands and agrees that users of the VoIP System must provide their address and phone number in order to get help. Client hereby authorizes VTG to disclose Client's name and address to third-party service providers, including, without limitation,

call routers, call centers and public service answering points, for the purpose of dispatching emergency services personnel to Client's registered location.

Client understands and agrees that 911 dialing does not and will not function in the event of a power failure or disruption. Similarly, the hosted VoIP Services will not operate (i) during service outages or suspensions or terminations of service by Client's broadband provider or ISP, or (ii) during periods of time in which Client's ISP or broadband provider blocks the ports over which the VoIP Services are provided. Client further understands and agrees that 911 Dialing will not function if Client changes its telephone number, or if Client adds or ports new telephone numbers to Client's account, unless and until Client successfully register its location of use for each changed, newly added or newly ported telephone number.

Client expressly agrees not to use VoIP System for auto-dialing, continuous or extensive call forwarding, telemarketing, fax broadcasting or fax blasting, or for any other use that results in excessive usage inconsistent with standard commercial calling patterns.

Patch Management

We will keep all managed hardware and managed software current with critical patches and updates ("Patches") as those Patches are released generally by the applicable manufacturers. Patches are developed by third party vendors and, on rare occasions, may make the Environment, or portions of the Environment, unstable or cause the managed equipment or software to fail to function properly even when the Patches are installed correctly. We will not be responsible for any downtime or losses arising from or related to the installation or use of any Patch. We reserve the right, but not the obligation, to refrain from installing a Patch if we are aware of technical problems caused by a Patch, or we believe that a Patch may render the Environment, or any portion of the Environment, unstable.

Backup (BDR) Services

All data transmitted over the Internet may be subject to malware and computer contaminants such as viruses, worms and trojan horses, as well as attempts by unauthorized users, such as hackers, to access or damage Client's data. Neither VTG nor its designated affiliates will be responsible for the outcome or results of such activities.

BDR services require a reliable, always-connected internet solution. Data backup and recovery time will depend on the speed and reliability of your internet connection. Internet and telecommunications outages will prevent the BDR services from operating correctly. In addition, all computer hardware is prone to failure due to equipment malfunction, telecommunication-related issues, etc., for which we will be held harmless. Due to technology limitations, all computer hardware, including communications equipment, network servers and related equipment, has an error transaction rate that can be minimized, but not eliminated. VTG cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that VTG 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 VTG 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, VTG 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. VTG is not a warranty service or repair center. VTG 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 VTG will be held harmless, and (ii) VTG 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 VTG's opinion and knowledge of the relevant facts and circumstances. By rendering advice, or by suggesting a particular service or solution, VTG 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. VTG 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 VTG 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 VTG-hosted or VTG-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 Service Statement, 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 VTG 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. VTG 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 VTG immediately to request the login information be reset or unauthorized access otherwise be prevented. VTG 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.