Services Guide

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

This Services Guide is our "owner's manual" that generally describes all managed services provided or facilitated by Computer Point ("Computer Point," "we," "us," or "our"); **however, only those services specifically described in the Quote will be facilitated and/or provided to you.**

This Services Guide is governed under our Master Services Agreement ("MSA"). You may locate our MSA through the link in your Quote or, if you want, we will send you a copy of the MSA by email upon request. Capitalized terms in this Services Guide will have the same meaning as the capitalized terms in the MSA, unless otherwise indicated below.

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

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

Initial Audit / Diagnostic Services

In most cases, we will conduct an initial audit of your information technology (IT) environment to determine the readiness for, and compatibility with, our proposed ongoing managed services. This audit may include some or all the following:

- Audit to determine general Environment (defined below) readiness and functional capability
- Review of hardware and software configurations
- Review of current vendor service / warranty agreements for Environment hardware and software
- Basic security vulnerability check
- Basic backup and file recovery solution audit
- Speed test and ISP audit
- Print output audit
- Office telephone vendor service audit
- Asset inventory
- Email and website hosting audit
- IT support process audit

If deficiencies are discovered during the auditing process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and provide you with options to correct the deficiencies. **Please note, unless otherwise expressly agreed by us in writing, auditing services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the auditing process**. Issues that are discovered in the Environment after the auditing process is completed may be addressed in one or more subsequent quotes.

Onboarding Services

Onboarding is the stage during which we prepare the Environment for the managed services described in the Quote. During this phase, we will work with your Authorized Contact(s) to review the information we need to prepare the targeted environment. In addition:

- It is Client's responsibility to have its previous IT service providers' tools and software agents ("Prior Tools") removed in cooperation with Computer Point's installation of our tools, as well as to uninstall then-existing administrative passwords or keys (or provide us with those passwords and keys) as necessary for Computer Point to implement its services. Additional charges may apply if Computer Point is required to uninstall Prior Tools, seize administrative access, or undertake any other efforts reasonably necessary for Computer Point to acquire administrative access.
  Uninstall any monitoring tools or other software installed by previous IT service providers ("Prior Tools"). Please note: If we are unable to uninstall or disable Prior Tools remotely, then an onsite visit may be required for which additional fees, such as travel time, may apply. In any event, if Prior Tools cannot be removed then we will bring that situation to your attention and, to the extent reasonably practicable, quarantine the Prior Tools so they become inoperative. We do not warrant or guarantee that all Prior Tools will be capable of being removed permanently, or that unremovable Prior Tools will become or remain inoperative.
- Compile a full inventory of all protected servers, workstations, and laptop
- Uninstall any previous endpoint protection and install our managed security solutions (as indicated in the Quote)
- Install remote support access agents (*i.e.*, software agents) on each managed device to enable remote support
- Configure Windows® and application patch management agent(s) and check for missing security updates
- Uninstall unsafe applications or applications that are no longer necessary
- Optimize device performance including disk cleanup and endpoint protection scans
- Review firewall configuration and other network infrastructure devices
- Review status of battery backup protection on all mission critical devices
- Stabilize network and assure that all devices can securely access the file server
- Review and document current server configuration and status
- Determine existing business continuity strategy and status; prepare backup file recovery and incident response option for consideration
- Review password policies and update user and device passwords.
- As applicable, make recommendations for changes that should be considered to the managed environment

This list is subject to change if we determine, at our discretion, that different or additional onboarding activities are required.

If deficiencies are discovered during the onboarding process, we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of our monthly managed services. **Please note, unless otherwise expressly stated in the Quote, onboarding-related services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the onboarding process.**

The duration of the onboarding process depends on many factors, many of which may be outside of our control—such as product availability/shortages, required third party vendor input, etc. As such, we can estimate, but cannot guarantee, the timing and duration of the onboarding process. We will keep you updated as the onboarding process progresses.

Ongoing / Recurring Managed Services

The table below describes all managed services provided or facilitated by Computer Point; however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services"). **Please review the Quote to determine which of the managed services listed below will be provided to / facilitated for you.**

Ongoing/recurring managed services are provided to you or facilitated for you on an ongoing basis and, unless otherwise indicated in a Quote, are billed monthly. Some ongoing/recurring services will begin with the commencement of onboarding services; others will begin when the onboarding process is completed. Please direct any questions about start or "go live" dates to your account manager.

Managed Services

(Please refer to the Quote to determine which Managed Services you will be receiving.)

SERVICES	GENERAL DESCRIPTION
Backup and File Recovery	Implementation and facilitation of a backup and file recovery solution from our designated Third Party Provider. • 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. All facilities housing backed up data implement physical security controls and logs, including security cameras, and have multiple internet connections with failover capabilities. Backup Retention: Backed up data will be retained for the periods indicated below, unless a different time period is expressly stated in the Quote. This includes both on-premise and cloud backups. • *On-Premise Backups* All on-premise backups will be stored on a Network Attached Storage (NAS) device, which will be kept in a secure location with restricted access. On-premise backups will be performed daily and retained on a rolling thirty (30) day basis. • *Cloud Backups* All cloud backups will be stored in a secure, off-site location that meets the organization's security standards. Cloud backups will be performed daily and retained on a rolling thirty (30) day basis. 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. • Request Method. Requests to restore backed up data should be made through one of the following methods:

	○ Email: _____ ○ Web portal: _____ ○ Telephone: _____ • Restoration Time: We will endeavor to restore backed up data as quickly as possible following our receipt of a request to do so; however, in all cases data restoration services are subject to (i) technician availability and (ii) confirmation that the restoration point(s) is/are available to receive the backed up data.
Backup Monitoring	Implementation and facilitation of a backup monitoring solution from our designated Third Party Provider. Features include: • Monitoring backup status for certain backup applications then-installed in the managed environment, such as successful completion of backup, failure errors, and destination free space restrictions/limitations. • Helping ensure adequate access to Client's data in the event of loss of data or disruption of certain existing backup applications. **Note: Backup monitoring is limited to monitoring activities only and is not a backup and file recovery solution.**
Dark Web Monitoring	Implementation and facilitation of a Dark Web Monitoring solution from our designated Third Party Provider. Credentials supplied by Client will be added into a system that continuously uses human and machine-powered monitoring to determine if the supplied credentials are located on the dark web. If compromised credentials are found, they are reported to Help Desk Services staff who will review the incident and notify affected end-users. Dark web monitoring can be a highly effective tool to reduce the risk of certain types of cybercrime; however, we do not guarantee that the dark web monitoring service will detect all actual or potential uses of your designated credentials or information.
Email Threat Protection	Implementation and facilitation of a trusted email threat protection solution from our designated Third Party Provider. • 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. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.** **All hosted email is subject to the terms of our Hosted Email Policy and our Acceptable Use Policy.**
Endpoint Antivirus & Malware Protection	Implementation and facilitation of an endpoint malware protection solution from our designated Third Party Provider.

	• Artificial intelligence and machine learning to provide a comprehensive and adaptive protection paradigm to managed endpoints. • Detection of unauthorized behaviors of users, applications, or network servers. • Blocking of suspicious actions before execution. • Analyzing suspicious app activity in isolated sandboxes. • Antivirus and malware protection for managed devices such as laptops, desktops, and servers. • Protection against file-based and fileless scripts, as well as malicious JavaScript, VBScript, PowerShell, macros and more. • Whitelisting for legitimate scripts. • Blocking of unwanted web content. • Detection of advanced phishing attacks. • Detection / prevention of content from IP addresses with low reputation. *** Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
End User Security Awareness Training	Implementation and facilitation of a security awareness training solution from an industry-leading third party solution provider. • 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. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Firewall as a Service (firewall appliance provided by Computer Point)	• Provide a 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. • Firewall appliance is subject to "Hardware as a Service" terms and conditions located in this Guide. • Firewall appliance must be returned to Computer Point upon the termination of service. Client will be responsible for missing or damaged (normal wear and tear excepted) appliance.
Firewall Solution (firewall appliance provided / purchased by Client)	• Monitors, updates (software/firmware), and supports Client-supplied firewall appliance. • 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.
Managed Detection & Response (MDR)	Implementation and facilitation of a top-tier MDR solution from our designated Third Party Provider. • 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 Service response times, below. • Security reports, such as privileged activities, security events, and network reports, are available upon request.

	• 24x7x365 access to a security team for incident response* * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Password Manager	Implementation and facilitation of a password management protection solution from our designated Third Party Provider. • Password Vault: Securely store and organize passwords in a secure digital location accessed through your browser or an app. • Password Generation: Generate secure passwords with editable options to meet specific criteria. • Financial Information Vault: Securely store and organize financial information such as bank accounts and credit card information in a secure digital location accessed through your browser or an app. • Contact Information Vault: Store private addresses and personal contact information within your vault accessed through your browser or an app. • Browser App: Browser extension permits easy access to your information including the vaults, financial information, contact information, and single sign-on through the app. • Smart-Phone App: Mobile phone app enables access to your vault and stored information on your mobile device.
Penetration (Pen) Testing	Penetration testing (or "pen" testing) simulates a cyberattack against your IT infrastructure to identify exploitable vulnerabilities. Unlike ongoing vulnerability scanning services that provide a constant, static level of network scanning, pen testing may involve several stages of reconnaissance and actual attack methodologies (such as brute force attacks and/or SQL injection attacks) and may include unconventional and targeted attacks that occur during business and non-business hours. Pen testing may consist of any of the following: **External Pen Testing:** exposes vulnerabilities in your internet-facing systems, networks, firewalls, devices, and/or web applications that could lead to unauthorized access. **Internal Pen Testing:** Validates the effort required for an attacker to overcome and exploit your internal security infrastructure after access is gained. **PCI Pen Testing:** Using the goals set by the PCI Security Standards Council, this test involves both external and internal pen testing methodologies. **Web App Pen Testing:** Application security testing using attempted infiltration through a website or web application utilizing PTES and the OWASP standard testing checklist. Please see additional terms for Penetration Testing below.
Remote Helpdesk	• Remote support provided during normal business hours for managed devices and covered software • Tiered-level support provides a smooth escalation process and helps to ensure effective solutions.
Remote Infrastructure Maintenance & Support	• Configuration, monitoring, and preventative maintenance services provided for the managed IT infrastructure

- If remote efforts are unsuccessful, then Computer Point will dispatch a technician to the Client's premises to resolve covered incidents (timing of onsite support is subject to technician availability and scheduling).

Remote Monitoring and Management

Software agents installed in Covered Equipment (defined below) report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.

- Includes capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD partitions, not external devices such as USB or mapped drives)
- Includes routine operating system inspection and cleansing to help ensure that disk space is increased before space-related issues occur.
- Review and installation of updates and patches for supported software.

In addition to the above, our remote monitoring and management service will be provided as follows:

Event	Server	Workstation
Hardware Failures	Yes	No
Device Offline	Yes	No
Failed/Missing Backup	Yes	No
Failed/Missing Updates	Yes	Yes
Low Disk Space	Yes	No
Agent missing/misconfigured	Yes	Yes
Excessive Uptime	Yes	No
Automatic Reboots (weekly)	No	Yes

Security Incident & Event Monitoring (SIEM)

Implementation and facilitation of an industry leading SIEM solution from our designated Third Party Provider.

The SIEM service utilizes threat intelligence to detect threats that can exploit potential vulnerabilities against your managed network.

- Initial Assessment. Prior to implementing the SIEM service, we will perform an initial assessment of the managed network at your premises to define the scope of the devices/network to be monitored (the "Initial Assessment").

- Monitoring. The SIEM service detects threats from external facing attacks as well as potential insider threats and attacks occurring inside the monitored network. Threats are correlated against known baselines to determine the severity of the attack.

- Alerts & Analysis. Threats are reviewed and analyzed by third-party human analysts to determine true/false positive dispositions and actionability. If it is determined that the threat was generated from an actual security-related or operationally deviating event (an "Event"), then you will be notified of that Event.

  Events are triggered when conditions on the monitored system meet or exceed predefined criteria (the "Criteria"). Since the Criteria are established and optimized over time, the first thirty (30) days after deployment of the SIEM services will be used to identify a baseline of the Client's environment and user behavior. During this initial thirty (30) day period, Client may experience some "false positives" or, alternatively, during this period not all anomalous activities may be detected.

Note: The SIEM service is a monitoring and alert-based system only; remediation of detected or actual threats are not within the scope of this service and may require Client to retain Computer Point's services on a time and materials basis.

Server Monitoring & Maintenance	As part of our RMM service, we will monitor and maintain managed servers as follows: • Software agents installed in covered servers report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below. • Online status monitoring, alerting us to potential failures or outages • Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives) • Performance monitoring, alerting us to unusual processor or memory usage • Server essential service monitoring, alerting us to server role-based service failures • Endpoint protection agent monitoring, alerting us to potential security vulnerabilities • Routine operating system inspection and cleansing • Secure remote connectivity to the server and collaborative screen sharing • Review and installation of updates and patches for Windows and supported software • Asset inventory and server information collection
Multi-Factor Authentication	Implementation and facilitation of a multi-factor authentication solution from our designated Third Party Provider. • Advanced two factor authentication with advanced administrative features • Secures on-premises and cloud-based applications • Permits custom access policies based on role, device, location • Identifies and verifies device health to detect “risky” devices
Server Next-Generation Antivirus	Implementation and facilitation of a top-tier, next generation antivirus protection solution from our designated Third Party Provider. Software agents installed in covered server devices protect against malware and prevent intruder access. Used in coordination with other endpoint security layers and security solutions to form a comprehensive defense strategy. • Next-generation deep learning malware detection, file scanning, and live protection for Server OS • Web access security and control, application security and control, intrusion prevention system • Data loss prevention, exploit prevention, malicious traffic detection, disk and boot record protection
Updates & Patching	• Remotely deploy updates (e.g., x.1 to x.2), as well as bug fixes, minor enhancements, and security updates as deemed necessary on all managed hardware. • Perform minor hardware and software installations and upgrades of managed hardware. • Perform minor installations (i.e., tasks that can be performed remotely and typically take less than thirty (30) minutes to complete). • Deploy, manage, and monitor the installation of approved service packs, security updates and firmware updates as deemed necessary on all applicable managed hardware. Please note: 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.
Voice Over IP (VoIP) Services	Implementation and facilitation of an industry-recognized VoIP solution from our designated Third Party Provider. Features include: • Scalable VoIP-based telephone service with call transferring, voicemail, caller ID, call hold, conference calling, and call waiting functionalities. • Central control panel provides access to VoIP-related configurations, including physical address registration, call routing, updating greetings, and ability to turn on/off service features. • Ability to use mobile app dialing **Important**: There are additional terms related to the VoIP service, including your use of E911 features, toward the end of this Services Guide. Please read them carefully. You may be required to sign an additional consent form indicating your understanding and acceptance of the limitations of 911 dialing using the VoIP services.
Vulnerability Scanning	Implementation and facilitation of an industry-recognized vulnerability scanning solution from our designated Third Party Provider. Vulnerability scanning identifies holes in the managed network that could be exploited. External vulnerability scans (which pertain to the IP address assigned to each customer location through the Client's ISP) are run monthly. Internal vulnerability scans (which pertain to all systems inside the managed network) are run at least annually. Vulnerability results will be discussed during business review meetings with Client. Vulnerability reports will be made available on request. Please see additional terms for vulnerability scanning below.
Wi-Fi Services	Computer Point will install at the Client's premises Wireless Access Points to provide bandwidth in all areas requiring wireless network coverage, as agreed upon by Computer Point and Client. • Computer Point will maintain, supervise, and manage the wireless system at no additional cost. • Installed equipment, if provided by Computer Point, will be compatible with the then-current industry standards. • Computer Point will provide remote support services during normal business hours to assist with device connectivity issues. (Support services will be provided on a "best efforts" basis only, and Client understands that some end-user devices may not connect to the wireless network, or they may connect but not perform well). Please note: Any Wi-Fi devices, such as access points or routers, which are supplied by Client cannot be older than five (5) years from the applicable device's original date of manufacture, and in all cases must be supported by the manufacturer of the device(s).
Workstation Next-Generation Malware Solution	Implementation and facilitation of an industry-recognized, next generation workstation malware protection solution from our designated Third Party Provider. Software agents installed in covered devices protect against malware and prevent intruder access. Used in coordination with other endpoint security layers and security solutions to create a comprehensive defensive strategy. • Next-generation deep learning malware detection, file scanning, and live protection for Workstation OS.

	• Web access security and control, application security and control, intrusion prevention system. • Data loss prevention, exploit prevention, malicious traffic detection, disk, and boot record protection.
Workstation Monitoring & Maintenance	Software agents installed in covered workstations report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below. • Online status monitoring, alerting us to potential failures or outages. • Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives). • Performance monitoring, alerting us to unusual processor or memory usage. • Endpoint protection agent monitoring, alerting us to potential security vulnerabilities. • Routine operating system inspection and cleansing. • Secure remote connectivity to the workstation and collaborative screen sharing. • Review and installation of updates and patches for Windows and supported software. • Asset inventory and workstation information collection.

Project-Related Services

For project-based services, one-time or limited-time engagements, or similar engagements listed in a Quote ("Projects"), the following provisions shall apply:

- All our labor will be billed to you at our then-current hourly rate in fifteen (15) minute increments, with partial increments being rounded to the next highest increment.
- Project-related services will be performed during normal work hours only. If Project work is required to be performed after-hours or during non-business hours, our hourly rates will be increased as per the table below for the time expended in off-hours or non-business hours.
- You agree to reimburse us for all reasonable and pre-approved travel costs and expenses that are directly attributable to, or are reasonably required to be incurred, while providing Project-related services. Computer Point reserves the right to require pre-payment of anticipated travel costs and expenses.
- Our current hourly rates, and applicable rate multipliers for after-hours or non-business hours work, are as follows:

Category	Business Hours Onsite ($/hr)	Business Hours Remote ($/hr)	Onsite Minimum Charge (hr)	Remote Minimum Charge (hr)	After-hours Rate Premium Multiplier	Priority Rate Premium Multiplier
Network Engineer	**$**	**$**	**2**	**0.75**	**1.5**	**1.75**
Server Engineer	**$**	**$**	**2**	**0.75**	**1.5**	**1.5**
Field Technician	**$**	**$**	**2**	**0.75**	**1.25**	**1.5**
Consulting Services	**$**	**$**	**1**	**1**	**1.5**	**1.5**

Policies and Procedures Applicable to Services

Software Licensing: All software provided to you by or through Computer Point is licensed, not sold, to you ("Software"). In addition to any Software-related requirements described in Computer Point's Master Services Agreement, Software may also be subject to end user license agreements (EULAs), acceptable use policies (AUPs), and other restrictions all of which must be strictly followed by you and any of your authorized users.

When installing/implementing software licenses in the managed environment or as part of the Services, we may accept (and you agree that we may accept) any required EULAs or AUPs on your behalf. You should assume that all Software has an applicable EULA and/or AUP to which your authorized users and you must adhere. If you have any questions or require a copy of the EULA or AUP, please contact us.

Covered Environment. Services will be applied to the number of devices indicated in the Quote ("Covered Hardware"). The list of Covered Hardware may be modified by mutual consent (email is sufficient for this purpose); however, we reserve the right to modify the list of Covered Hardware at any time if we discover devices that were not previously included in the list of Covered Hardware and which are receiving Services, or as necessary to accommodate changes to the quantity of Covered Hardware.

Unless otherwise stated in the Quote, Covered Devices will only include technology assets (such as computers, servers, and networking equipment) owned by the Client's organization. As an accommodation, Computer Point may provide guidance in connecting a personal device to the Client's organization's technology, but support of personal devices is generally not included in the Scope of Services.

If the Quote indicates that the Services are billed on a "per user" basis, then the Services will be provided for up to two (2) Business Devices used by the number of users indicated in the Quote. A "Business Device" is a device that (i) is owned or leased by Client and used primarily for business, (ii) is regularly connected to Client's managed network, and (iii) has installed on it a software agent through which we (or our designated Third Party Providers) can monitor the device.

We will provide support for any software applications that are licensed through us. Such software ("Supported Software") will be supported on a "best effort" basis only and any support required beyond Level 2-type support will be facilitated with the applicable software vendor/producer. Coverage for non-Supported Software is outside of the scope of the Quote and will be provided to you on a "best-effort" basis and a time and materials basis with no guarantee of remediation. Should our technicians provide you with advice concerning non-Supported Software, the provision of that advice should be viewed as an accommodation and not an obligation to you.

If we are unable to remediate an issue with non-Supported Software, then you will be required to contact the manufacturer/distributor of the software for further support. Please note: Manufacturers/distributors of such software may charge fees, some of which may be significant, for technical support; therefore, we strongly recommend that you maintain service or support contracts for all non-Supported Software ("Service Contract"). If you request that we facilitate technical support for non-Supported Software and if you have a Service Contract in place, our facilitation services will be provided to you at our then-current hourly rates.

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, at our discretion, we determine that an onsite visit is required. Computer Point visits will be scheduled in accordance with the priority assigned to the issue (below) and are subject to technician availability. Unless we agree otherwise, all onsite Services will be provided at Client's primary business location. Additional fees may apply for onsite visits: Please review the Service Level section below for more details.

Evolving Technologies: Technologies can evolve rapidly. In certain instances, depending on the scope and timing of an applicable service, technologies comprising or included in a service may evolve before the service can be fully implemented. Should this occur, we will provide you with options to leverage the latest version of the evolved technology and inform you of the attendant fees and costs to do so. If you decline to implement the evolved technology, then we will continue to implement the service as indicated in the Quote; however, you understand and agree that (i) you will not benefit from improvements in the evolved technology, and (ii) the applicable technology and service may become obsolete more quickly.

Minimum Requirements / Exclusions. The scheduling, fees and provision of the Services are based upon the following assumptions and minimum requirements, all of which must be provided/maintained by Client at all times:

- Server hardware must be under current warranty coverage
- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software and have all the latest Microsoft service packs and critical updates installed.
- All software must be genuine, licensed, and vendor- or OEM-supported.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The managed environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored.
- All wireless data traffic in the managed environment must be securely encrypted.
- All servers must be connected to working UPS devices.
- Recovery coverage assumes data integrity of the backups or the data stored on the backup devices. We do not guarantee the integrity of the backups or the data stored on the backup devices. Server restoration will be to the point of the last successful backup.
- Client must provide all software installation media and key codes in the event of a failure.
- Any costs required to bring the Environment up to these minimum standards are not included in this Services Guide.
- Client must provide us with exclusive administrative privileges to the Environment.
- Client must not affix or install any accessory, addition, upgrade, equipment, or device on to the firewall, server, or NAS appliances (other than electronic data) unless expressly approved in writing by us.

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 Computer Point**. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by Computer Point in writing:

- Customization of third party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.

- Battery backup replacement.
- Equipment relocation.
- The cost to bring the managed environment up to these minimum requirements (unless otherwise noted in the Quote).
- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.

Service Levels. Automated services are provided on an ongoing (*i.e.*, 24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our business hours (currently M-F, 8:30 AM – 5 PM Eastern Time, excluding legal holidays and Computer Point-observed holidays as listed below), unless otherwise specifically stated in the Quote or as otherwise described below.

We will respond to problems, errors, or interruptions in the provision of the Services in the timeframe(s) described below. Severity levels will be determined by Computer Point in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; Computer Point will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

Trouble / Severity	Response Time
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.
Long Term Project, Preventative Maintenance	Response within four (4) business days after notification.

* All time frames are calculated as of the time that we are notified of the applicable issue / problem by Client through our designated support portal, help desk, or by telephone at the telephone number listed in the Quote. Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts.

Support During Off-Hours/Non-Business Hours: Technical support provided outside of our normal business hours is offered on a case-by-case basis and is subject to technician availability. If Computer Point agrees to provide off-hours/non-business hours support ("Non-Business Hour Support"), then that support will be provided on a time and materials basis (which is not covered under any Service plan), and will be billed to Client at the rates (and hourly multipliers) indicated in the table in "Project-Related Services," above.

Computer Point-Observed Holidays: Computer Point observes the following holidays:

- New Year's Day

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

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

Fees. The fees for the Services will be as indicated in the Quote.

Reconciliation. Fees for certain Third Party Services that we facilitate or resell to you may begin to accrue prior to the "go-live" date of other applicable Services. (For example, Microsoft Azure or AWS-related fees begin to accrue on the first date on which we start creating and/or configuring certain hosted portions of the Environment; however, the Services that rely on Microsoft Azure or AWS may not be available to you until a future date). You understand and agree that you will be responsible for the payment of all fees for Third Party Services that are required to begin prior to the "go-live" date of Services, and we reserve the right to reconcile amounts owed for those fees by including those fees on your monthly invoices.

Changes to Environment. Initially, you will be charged the monthly fees indicated in the Quote. Thereafter, if the managed environment changes, or if the number of authorized users accessing the managed environment changes, then you agree that the fees will be automatically and immediately modified to accommodate those changes.

Travel Time. If onsite services are provided for managed services, we will travel up to 45 minutes from our office to your location at no charge. Time spent traveling beyond 45 minutes (*e.g.,* locations that are beyond 45 minutes from our office, occasions on which traffic conditions extend our drive time beyond 45 minutes one-way, etc.) will be billed to you at our then current hourly rates. In addition, you will be billed for all tolls, parking fees, and related expenses that we incur if we provide onsite services to you.

Appointment Cancellations. You may cancel or reschedule any appointment with us at no charge by providing us with notice of cancellation at least one business day in advance. If we do not receive timely a notice of cancellation/re-scheduling, or if you are not present at the scheduled time or if we are otherwise denied access to your premises at a pre-scheduled appointment time, then you agree to pay us a cancellation fee equal to two (2) hours of our normal consulting time (or non-business hours consulting time, whichever is appropriate), calculated at our then-current hourly rates.

Access Licensing. One or more of the Services may require us to purchase certain "per seat" or "per device" licenses (often called "Access Licenses") from one or more Third Party Providers. (Microsoft "New Commerce Experience" licenses as well as Cisco Meraki "per device" licenses are examples of Access Licenses.) Access Licenses cannot be canceled once they are purchased and often cannot be transferred to any other customer. For that reason, you understand and agree that regardless of the reason for termination of the Services, fees for Access Licenses are non-mitigatable and you are required to pay for all applicable Access Licenses in full for the entire term of those licenses. Provided that you have paid for the Access Licenses in full, you will be permitted to use those licenses until they expire.

Term; Termination. The Services will commence, and billing will begin, on the date indicated in the Quote ("Commencement Date") and will continue through the initial term listed in the Quote ("Initial Term"). We reserve the right to delay the Commencement Date until all onboarding/transition services (if any) are completed, and all deficiencies / revisions identified in the onboarding process (if any) are addressed or remediated to Computer Point's satisfaction.

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

Per Seat/Per Device Licensing: **Regardless of the reason for the termination of the Services, you will be required to pay for all per seat or per device licenses that we acquire on your behalf. Please see "Access Licensing" in the Fees section above for more details.**

Removal of Software Agents; Return of Firewall & Backup Appliances: Unless we expressly direct you to do so, you will not remove or disable, or attempt to remove or disable, any software agents that we installed in the managed environment or any of the devices on which we installed software agents. Doing so without our guidance may make it difficult or impracticable to remove the software agents, which could result in network vulnerabilities and/or the continuation of license fees for the software agents for which you will be responsible, and/or the requirement that we remediate the situation at our then-current hourly rates, for which you will also be responsible. Depending on the particular software agent and the costs of removal, we may elect to keep the software agent in the managed environment but in a dormant and/or unused state.

Within ten (10) days after being directed to do so, you must remove, package and ship, at your expense and in a commercially reasonable manner, all hardware, equipment, and accessories leased, loaned, rented, or otherwise provided to you by Computer Point "as a service." If you fail to timely return all such equipment to us, or if the equipment is returned to us damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

Offboarding. Subject to the requirements in the MSA, Computer Point will off-board Client from Computer Point's under a plan agreed-upon by Client and Computer Point. Please note, we strongly recommend that, for transition purposes, you overlap Computer Point's services with the services of any incoming provider for at least one (1) full calendar month. This will help avoid gaps in critical services and a more efficient and effective transition process. As noted elsewhere in this Services Guide, neither Client nor its incoming provider may remove any of the software agents installed in the Environment without Computer Point's consent. Doing so may cause Client to incur additional costs and fees for which Client will be solely responsible.

Additional Policies

The following additional policies ("Policies") apply to Services that we provide or facilitate under a Quote. By accepting a Service for which one or more of the Policies apply, you agree to the applicable Policy.

Authenticity

Everything in the managed environment must be genuine and licensed, including all hardware, software, etc. If we ask for proof of authenticity and/or licensing, you must provide us with such proof. All minimum hardware or software requirements as indicated in a Quote or this Services Guide ("Minimum Requirements") must be implemented and maintained as an ongoing requirement of us providing the Services to you.

Monitoring Services; Alert Services

Unless otherwise indicated in the Quote, all monitoring and alert-type services are limited to detection and notification functionalities only. Monitoring levels will be set by Computer Point, and Client shall not modify these levels without our prior written consent.

Configuration of Third Party Services

Certain third party services provided to you under a Quote may provide you with administrative access through which you could modify the configurations, features, and/or functions ("Configurations") of those services. However, any modifications of Configurations made by you without authorization could disrupt the Services and/or cause a significant increase in the fees charged for those third party services. For that reason, we strongly advise you to refrain from changing the Configurations unless we authorize those changes. You will be responsible for paying any increased fees or costs arising from or related to changes to the Configurations.

Modification of Environment

Changes made to the Environment without our prior authorization or knowledge may have a substantial, negative impact on the provision and effectiveness of the Services and may impact the fees charged under the Quote. You agree to refrain from moving, modifying, or otherwise altering any portion of the Environment without our prior knowledge or consent. For example, you agree to refrain from adding or removing hardware from the Environment, installing applications on the Environment, or modifying the configuration or log files of the Environment without our prior knowledge or consent.

Anti-Virus; Anti-Malware

Our anti-virus / anti-malware solution will generally protect the Environment from becoming infected with new viruses and malware ("Malware"); however, Malware that exists in the Environment at the time that the security solution is implemented may not be capable of being removed without additional services, for which a charge may be incurred. We do not warrant or guarantee that all Malware will be detected, avoided, or removed, or that any data erased, corrupted, or encrypted by Malware will be recoverable. To improve security awareness, you agree that Computer Point 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 or systems impacted by the incident will be

recoverable or remediated. For the purposes of this paragraph, a Security Incident means any unauthorized or impermissible access to or use of the Environment, or any unauthorized or impermissible disclosure of Client's confidential information (such as user names, passwords, etc.), that (i) compromises the security or privacy of the information or applications in, or the structure or integrity of, the managed environment, or (ii) prevents normal access to the managed environment, or impedes or disrupts the normal functions of the managed environment.

Environmental Factors

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

Fair Usage Policy

Our Fair Usage Policy ("FUP") applies to all services that are described or designated as "unlimited" or which are not expressly capped in the number of available usage hours per month. An "unlimited" service designation means that, subject to the terms of this FUP, you may use the applicable service as reasonably necessary for you to enjoy the use and benefit of the service without incurring additional time-based or usage-based costs. However, unless expressly stated otherwise in the Quote, all unlimited services are provided during our normal business hours only and are subject to our technicians' availabilities, which cannot always be guaranteed. In addition, we reserve the right to assign our technicians as we deem necessary to handle issues that are more urgent, critical, or pressing than the request(s) or issue(s) reported by you. Consistent with this FUP, you agree to refrain from (i) creating urgent support tickets for non-urgent or non-critical issues, (ii) requesting excessive support services that are inconsistent with normal usage patterns in the industry (*e.g.*, requesting support in lieu of training), (iii) requesting support or services that are intended to interfere, or may likely interfere, with our ability to provide our services to our other customers.

Hosted Email

You are solely responsible for the proper use of any hosted email service provided to you ("Hosted Email").

Hosted Email solutions are subject to acceptable use policies ("AUPs"), and your use of Hosted Email must comply with those AUPs—including ours. In all cases, you agree to refrain from uploading, posting, transmitting or distributing (or permitting any of your authorized users of the Hosted Email to upload, post, transmit or distribute) any prohibited content, which is generally content that (i) is obscene, illegal, or intended to advocate or induce the violation of any law, rule or regulation, or (ii) violates the intellectual property rights or privacy rights of any third party, or (iii) mischaracterizes you, and/or is intended to create a false identity or to otherwise attempt to mislead any person as to the identity or origin of any communication, or (iv) interferes or disrupts the services provided by Computer Point 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. Computer Point 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 Computer Point believes, in its discretion, that Client's email account(s) is/are being used in an improper or illegal manner.

Backup (BDR) Services

All data transmitted over the Internet may be subject to malware and computer contaminants such as viruses, worms and trojan horses, as well as attempts by unauthorized users, such as hackers, to access or damage Client's data. Neither Computer Point 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. Computer Point cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Computer Point shall be held harmless if such data corruption or loss occurs. **Client is strongly advised to keep a local backup of all stored data to mitigate against the unintentional loss of data.**

Procurement

Equipment and software procured by Computer Point 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, Computer Point 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. Computer Point is not a warranty service or repair center. Computer Point 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 Computer Point will be held harmless, and (ii) Computer Point is not responsible for the quantity, condition, or timely delivery of the Procured Equipment once the equipment has been tendered to the designated shipping or delivery courier.

Business Review / IT Strategic Planning Meetings

We strongly suggest that you participate in business review/strategic planning meetings as may be requested by us from time to time. These meetings are intended to educate you about recommended (and potentially crucial) modifications to your IT environment, as well as to discuss your company's present and future IT-related needs. These reviews can provide you with important insights and strategies to make your managed IT environment more efficient and secure. You understand that by suggesting a particular service or solution, we are not endorsing any specific manufacturer or service provider.

VCTO or VCIO Services

The advice and suggestions provided by us in our capacity as a virtual chief technology or information officer (if applicable) will be for your informational and/or educational purposes only. Computer Point will not hold an actual director or officer position in Client's company, and we will neither hold nor maintain any fiduciary relationship with Client. Under no circumstances shall Client list or place Computer Point on Client's corporate records or accounts.

Sample Policies, Procedures.

From time to time, we may provide you with sample (*i.e.*, template) policies and procedures for use in connection with Client's business ("Sample Policies"). The Sample Policies are for your informational use only, and do not constitute or comprise legal or professional advice, and the policies are not intended to be a substitute for the advice of competent counsel. You should seek the advice of competent legal counsel prior to using or distributing the Sample Policies, in part or in whole, in any transaction. We do not warrant or guarantee that the Sample Policies are complete, accurate, or suitable for your (or your customers') specific needs, or that you will reduce or avoid liability by utilizing the Sample Policies in your (or your customers') business operations.

Penetration Testing; Vulnerability Scanning

You understand and agree that security devices, alarms, or other security measures, both physical and virtual, may be tripped or activated during the penetration testing and/or vulnerability scanning processes, despite our efforts to avoid such occurrences. You will be solely responsible for notifying any monitoring company and all law enforcement authorities of the potential for "false alarms" due to the provision of the penetration testing or vulnerability scanning services, and you agree to take all steps necessary to ensure that false alarms are not reported or treated as "real alarms" or credible threats against any person, place, or property. Some alarms and advanced security measures, when activated, may cause the partial or complete shutdown of the Environment, causing substantial downtime and/or delay to your business activities. We will not be responsible for any claims, costs, fees, or expenses arising or resulting from (i) any response to the penetration testing or vulnerability scanning services by any monitoring company or law enforcement authorities, or (ii) the partial or complete shutdown of the Environment by any alarm or security monitoring device.

No Third Party Scanning

Unless we authorize such activity in writing, you will not conduct any test, nor request or allow any third party to conduct any test (diagnostic or otherwise), of the security system, protocols, processes, or solutions that we implement in the managed environment ("Testing Activity"). Any services required to diagnose or remediate errors, issues, or problems arising from unauthorized Testing Activity are not covered under the Quote, and if you request us (and we elect) to perform those services, those services will be billed to you at our then-current hourly rates.

Obsolescence

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

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-Specific Policies Applicable to the Services

To the extent that the Services include or use any of the third party solutions listed in the table below, you understand and agree that the applicable services' end user license, reseller, and/or customer agreements as listed below shall apply to your use or the Service(s).

Third Party Solution Provider	Service	Terms
3CX	VoIP, Telephony	https://www.3cx.com/company/terms-and-conditions/
Acronis	Network Security, Data Backup, Disaster Recovery	https://dl.acronis.com/u/pdf/Acronis_corporate_EULA_en-US.pdf
Arctic Wolf	Security, SIEM Solution	If you are a direct customer with Arctic Wolf, then the following applies: https://arcticwolf.com/wp-content/uploads/2024/06/Solutions-Agreement-online_2024.06-FINAL-1.pdf
Adobe Sign	Digital Signature/Acceptance	https://www.adobe.com/legal/terms.html
Altaro Backup	Backup	https://www.altaro.com/eula.php
Autotask	Professional Services Automation	Covered under Kaseya's Master Agreement: https://www.kaseya.com/legal/kaseya-master-agreement/
Auvik	IT Asset Management, Network Analysis	https://www.auvik.com/privacy-and-legal/
Axcient	Disaster Recovery	https://axcient.com/master-subscription-agreement/
Backblaze	Backup	https://www.backblaze.com/company/policy/terms-of-service
Barracuda	Help Desk	https://www.barracuda.com/company/legal/terms-and-conditions
Bitdefender Antivirus	Security, Endpoint Protection	https://www.bitdefender.com/en-us/site/view/eula-for-accessing-bitdefender-managed-detection-and-response-service
Blackpoint Cyber	Managed Detection & Response; Security	https://blackpointcyber.com/reseller-agreement/
BreachSecureNow	Security Awareness Training	https://www.breachsecurenow.com/terms-and-conditions/
Bullphish	Security Awareness Training	Covered under Kaseya's Master Agreement: https://www.kaseya.com/legal/kaseya-master-agreement/ also: https://www.idagent.com/terms-of-use/
Cisco Umbrella	Networking Solutions, Cybersecurity	https://www.cisco.com/site/us/en/about/legal/contract-experience/index.html
Cloud Radial	Ticketing Portal, vCIO Planner, Warranty Reporting	https://www.cloudradial.com/terms
Compliancy Group	Compliance Assessment & Training	https://compliancy-group.com/terms-of-use/

Third Party Solution Provider	Service	Terms
Crowdstrike	Endpoint Protection, Network Detection, Recovery, Compliance Assessments	https://www.crowdstrike.com/en-us/software-terms-of-use/?srsltid=AfmBOopMxk90hTXBpq16ncRt5tXRgMujrj-P-qpadt7Q-59EFYgp8i-k
CyberHawk / Rapidfire Tools	Network IT Change Detection	https://cyberhawk.pro/eula/
CyberQP	Password Management	https://cyberqp.com/terms-and-conditions/
Cylance	Managed Detection & Response	https://www.sonicwall.com/medialibrary/serviceplans/cylance-tier-1.pdf
Cynomi	Risk & Compliance Assessments	https://cynomi.com/eula/
Cytracom	Network Security, Telephony	https://www.cytracom.com/legal
Dark Web ID		(See ID Agent, below)
Datto EDR, Datto AV, Ransomware Detection Product Terms	Security	https://www.datto.com/legal/datto-edr-datto-av-ransomware-detection-product-terms/?x-craft-preview=q9T1QJysjG&token=Vb7LjyDIC1sWR2n4Q-SnVRGZskSHcIjc
Dropsuite	O365 Backup	No EULA online, but requires you to agree: • to protect all Dropsuite's (and its licensors') existing and future Intellectual Property Rights in the Dropsuite Data Backup Service; • to require the End User to use the Dropsuite Data BackUp Service (which it may either name or describe generically in its End User Terms and Conditions) only for lawful personal purposes or for its lawful internal business purposes; • to prohibit the End User from copying, reproducing, reverse-engineering, decompiling, disassembling, reselling, distributing or modifying the Dropsuite Data Backup Service (whether named or described generically) without the written consent of the MSP, except to the extent expressly permitted by any law or treaty that is in force in the territory where that law or treaty cannot be excluded, restricted or modified, provided that where the End User seeks any such consent from the MSP, the MSP must not provide it unless and until it has sought and obtained the consent of Dropsuite to include exclusions of liability that are no less protective than the warranty exclusions set out in clause 8 of DropSuite's Online Terms of Service (https://dropsuite.com/terms/) and to include limitations on liability that are no less protective than the warranty exclusion set out in clause 10 of DropSuite's Online Terms of Service. See https://dropsuite.com/terms/ for more details.

Third Party Solution Provider	Service	Terms
		Dropsuite Retention Policy: https://help.dropsuite.com/hc/en-us/articles/22814916296215-Retention-Policy-Guide
Duo	Multifactor Authentication	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/Cisco_General_Terms.pdf
Fortinet	Network Security	https://www.fortinet.com/content/dam/fortinet/assets/legal/Fortinet-Service-Offering-Terms.pdf
Galactic Advisors	Cybersecurity; Security Awareness Training; Penetration Testing	(no posted EULA or terms of service.)
Graphus	Anti-Phishing Software, Email Protection	Covered under Kaseya's Master Agreement: https://www.kaseya.com/legal/kaseya-master-agreement/ https://www.graphus.ai/terms-of-use/
Huntress	Endpoint Security, Risk Assessments, Policy & Procedure Development	https://www.huntress.com/terms-of-use
ID Agent	Dark Web Monitoring	Now covered under Kaseya's Master Agreement: https://www.kaseya.com/legal/kaseya-master-agreement/ also: https://www.idagent.com/terms-of-use/
IT Glue	IT Inventory & Documentation Solution	https://www.itglue.com/terms-of-use/
iDrive 360	Backup & Storage	https://www.idrive.com/endpoint-backup/terms-and-conditions
Infima Security	Security Awareness Training	https://infimasec.com/legal/tos
Infosec Institute	Cybersecurity Training & Certification	https://www.infosecinstitute.com/infosec-license-agreement/
IronScales	Email Protection, Cybersecurity Training	https://www.ironscales.com/hubfs/PDFs/IRONSCALES%20-%20End%20User%20License%20Agreement%20-%20April%202022.pdf
JumpCloud	Cross Platform Device Management, Automated Onboarding & Offboarding, Multifactor Authentication	https://jumpcloud.com/legal/daasa
Kaseya (applies to all software and services provided by Kaseya)		https://www.kaseya.com/legal/kaseya-end-user-license-agreement-eula/

Third Party Solution Provider	Service	Terms
Kaseya 365	Remote Management & Monitoring, Patch Management, Endpoint Protection & Response, Malware/Endpoint Protection, Endpoint Backup	Covered under Kaseya's Master Agreement: https://www.kaseya.com/legal/kaseya-master-agreement/ Also: https://www.kaseya.com/legal/kaseya-365-product-terms-of-use/
KnowBe4	Security Awareness Training	https://www.knowbe4.com/managed-service-provider-agreement
LastPass	Password Management	https://www.goto.com/company/legal/terms-and-conditions
Liongard	Onboarding, Configuration Change Detection, Asset Discovery & Inventory	https://www.liongard.com/terms-of-use/
MalwareBytes	Security, Endpoint Protection	https://www.malwarebytes.com/eula
Microsoft Office 365		https://azure.microsoft.com/en-us/support/legal/subscription-agreement/?country=us&language=en
Microsoft applications (such as Azure Stack and individual Microsoft applications)		https://www.microsoft.com/en-us/useterms/
Mimecast		
nAble (Cove Backup)	Network Patching, Security, Storage	https://www.n-able.com/legal/software-services-agreement
NinjaOne	Remote Monitoring & Management, IT Asset Management, Patch Management, Mobile Device Management	https://www.ninjaone.com/license-agreement/
Palo Alto Networks	Endpoint Protection, Managed Detection & Response, Security Assessments	https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo-alto-networks-end-user-license-agreement-eula.pdf
Petra Security	Endpoint Protection, Security	https://commonpaper.com/standards/cloud-service-agreement/2.1
Phin Security	Security Awareness Training	https://secure.phinsolutions.com/modal/Terms.aspx
Probax	Data Backup	https://probax.io/eula
Proofpoint	Email Protection	https://www.proofpoint.com/us/legal/license
Rapid Fire Tools	Network Diagnosis/Evaluation	Covered under Kaseya's Master Agreement: https://www.kaseya.com/legal/kaseya-master-agreement/
Rocket Cyber	Managed Detection & Response	Covered under Kaseya's Master Agreement: https://www.kaseya.com/legal/kaseya-master-agreement/

Third Party Solution Provider	Service	Terms
SaaS Alerts	Cloud Productivity Alerts	Covered under Kaseya's Master Agreement: https://www.kaseya.com/legal/kaseya-master-agreement Also: https://saasalerts.com/product-terms-of-use
ScalePad	Lifecycle Management	https://app.scalepad.com/pages/terms
Sentinel One	Security	https://www.sentinelone.com/legal/master-subscription-agreement/ Also, https://www.sentinelone.com/legal/
ShadowProtect	Data Backup, Data Restoration	https://buy.storagecraft.com/ViewLicenseAgreement.aspx?id=5&ReturnUrl=amF2YXNjcmlwdDp3aW5kb3cuY2xvc2UoKQ=+
SolarWinds		https://www.solarwinds.com/legal/eula
SonicWall (all legal)	Hardware Security, Firewalls, Security	https://www.sonicwall.com/legal/end-user-product-agreements
SonicWall Managed Security Services	Security	https://www.sonicwall.com/medialibrary/legal/SonicWall-Managed-Security-Services-Terms.pdf
Spanning	Cloud-Based Data Backup	Covered under Kaseya's Master Agreement: https://www.kaseya.com/legal/kaseya-master-agreement/ Also: https://www.spanning.com/spanning-terms-of-use/
SuperOps		https://superops.com/terms
Threatlocker	Cybersecurity , Endpoint Protection, Network Monitoring	https://legacyportal.threatlocker.com//popups/eula.aspx
Todyl	Security	https://www.todyl.com/terms
Trend Micro	Endpoint Security, Network Security, Email Security, Identity Security	https://www.trendmicro.com/en_us/about/legal.html?modal=en-english-cloud-services-terms-of-service.pdf
Ubiquiti	Networking, Network Switches, WiFi	https://www.ui.com/eula
Vonahi	Network Penetration Testing	https://www.vonahi.io/terms
Vanta	Compliance & Risk Management	https://www.vanta.com/eula
Veeam	Backup, Data Recovery, Storage	https://www.veeam.com/legal/eula.html
Wasabi	Cloud Storage	https://wasabi.com/legal/terms-of-use
WatchGuard	Network Security, Virtual Private Network Solutions, License Management	https://www.watchguard.com/wgrd-trust-center/terms-of-use
Webroot	Endpoint Protection, Email Security	https://www-cdn.webroot.com/5616/6507/9887/Third_Party_Services_Terms_for_End_Users_-_Updated_10.6.22.pdf

Additional Terms Applicable to Microsoft Products

You shall comply with the special product terms published by Microsoft for all its partners that participate in Microsoft's New Commerce Experience (NCE)/Cloud Solution Provider (CSP) reseller programs. Those product terms are located here: https://partner.microsoft.com/en-us/licensing/licensing-agreements.

If you obtain Microsoft licenses through Computer Point, you agree to Microsoft's terms and conditions for such licenses. This includes, but is not limited to: (a) pricing and the contract length during which that pricing is effective; (b) contract length acquired (*e.g.,* annual or monthly); (3) type of payment (*e.g.,* annual or monthly); (4) license co-terms to the annual or monthly license date for added licenses; (5) all licenses set to auto-renew unless explicitly set to not renew; (6) Microsoft's renewal date, which may differ from Computer Point's contractual date, in which case you shall be bound to Microsoft even after the Services terminate; and (8) your obligation to Microsoft if you terminate a Microsoft license early.

Microsoft's current contract terms are 36-months, 12-months or 30-days from license purchase date. Additional licenses can be purchased co-terminus to initial license purchase and term. During those term(s), Microsoft does not allow a decrease in license counts beyond their reduction allowance period and any termination or decrease in license counts by you shall not result in a decrease of contract costs. **You are responsible for such Microsoft charges regardless of your usage of such licenses.** Computer Point will make every effort to align your licenses and minimize license usage when you cooperate with such efforts, but Computer Point is limited by Microsoft requirements within the program and as such, you are bound to those terms and shall pay such Microsoft charges for the entire length of Microsoft's contract requirements.

Acceptable Use Policy

The following policy applies to all hosted services provided to you, including but not limited to (and as applicable) hosted applications, hosted websites, hosted email services, and hosted infrastructure services ("Hosted Services").

Computer Point does not routinely monitor the activity of hosted accounts except to measure service utilization and/or service uptime, security-related purposes and billing-related purposes, and as necessary for us to provide or facilitate our managed services to you; however, we reserve the right to monitor Hosted Services at any time to ensure your compliance with the terms of this Acceptable Use Policy (this "AUP") and our master services agreement, and to help monitor and ensure the safety, integrity, reliability, or security of the Hosted Services.

Similarly, we do not exercise editorial control over the content of any information or data created on or accessible over or through the Hosted Services. Instead, we prefer to advise our customers of inappropriate behavior and any necessary corrective action. If, however, Hosted Services are used in violation of this AUP, then we reserve the right to suspend your access to part or all of the Hosted Services without prior notice.

Violations of this AUP: The following constitute violations of this AUP:

- **Harmful or illegal uses**: Use of a Hosted Service for illegal purposes or in support of illegal activities, to cause harm to minors or attempt to contact minors for illicit purposes, to transmit any material that threatens or encourages bodily harm or destruction of property or to transmit any material that harasses another is prohibited.
- **Fraudulent activity**: Use of a Hosted Service to conduct any fraudulent activity or to engage in any unfair or deceptive practices, including but not limited to fraudulent offers to sell or buy products, items, or services, or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters" is prohibited.
- **Forgery or impersonation**: Adding, removing, or modifying identifying network header information to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous remailers or nicknames does not constitute impersonation.
- **SPAM**: Computer Point has a zero tolerance policy for the sending of unsolicited commercial email ("SPAM"). Use of a Hosted Service to transmit any unsolicited commercial or unsolicited bulk e-mail is prohibited. You are not permitted to host, or permit the hosting of, sites or information that is advertised by SPAM from other networks. To prevent unnecessary blacklisting due to SPAM, we reserve the right to drop the section of IP space identified by SPAM or denial-of-service complaints if it is clear that the offending activity is causing harm to parties on the Internet, if open relays are on the hosted network, or if denial of service attacks are originated from the hosted network.
- **Internet Relay Chat (IRC)**: The use of IRC on a hosted server is prohibited.
- **Open or "anonymous" proxy**: Use of open or anonymous proxy servers is prohibited.
- **Cryptomining:** Using any portion of the Hosted Services for mining cryptocurrency or using any bandwidth or processing power made available by or through a Hosted Services for mining cryptocurrency, is prohibited.
- **Hosting spammers**: The hosting of websites or services using a hosted server that supports spammers, or which causes (or is likely to cause) our IP space or any IP space allocated to us or our customers to be listed in any of the various SPAM databases, is prohibited. Customers violating this policy will have their server immediately removed from our network and the server will not be reconnected until such time that the customer agrees to remove all traces of the offending material immediately upon reconnection and agree to allow Computer Point to access the server to confirm that all material has been completely removed. Any subscriber guilty of a second violation may be immediately and permanently removed from the hosted network for cause and without prior notice.
- **Email/message forging**: Forging any email message header, in part or whole, is prohibited.

- **Unauthorized access**: Use of the Hosted Services to access, or to attempt to access, the accounts of others or to penetrate, or attempt to penetrate, Computer Point's security measures or the security measures of another entity's network or electronic communications system, whether or not the intrusion results in the corruption or loss of data, is prohibited. This includes but is not limited to accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other networks, as well as the use or distribution of tools designed for compromising security such as password guessing programs, cracking tools, or network probing tools.
- **IP infringement**: Use of a Hosted Service to transmit any materials that infringe any copyright, trademark, patent, trade secret or other proprietary rights of any third party, is prohibited.
- **Collection of personal data**: Use of a Hosted Service to collect, or attempt to collect, personal information about third parties without their knowledge or consent is prohibited.
- **Disruptive Activity:** Use of the Hosted Services for any activity which affects the ability of other people or systems to use the Hosted Services or the internet is prohibited. This includes "denial of service" (DOS) attacks against another network host or individual, "flooding" of networks, deliberate attempts to overload a service, and attempts to "crash" a host.
- **Distribution of malware**: Intentional distribution of software or code that attempts to and/or causes damage, harassment, or annoyance to persons, data, and/or computer systems is prohibited.
- **Excessive use or abuse of shared resources**: The Hosted Services depend on shared resources. Excessive use or abuse of these shared network resources by one customer may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network performance is prohibited. You are prohibited from excessive consumption of resources, including CPU time, memory, and session time. You may not use resource-intensive programs which negatively impact other customers or the performances of our systems or networks.
- **Allowing the misuse of your account**: You are responsible for any misuse of your account, even if the inappropriate activity was committed by an employee or independent contractor. You shall not permit your hosted network, through action or inaction, to be configured in such a way that gives a third party the capability to use your hosted network in an illegal or inappropriate manner. You must take adequate security measures to prevent or minimize unauthorized use of your account. It is your responsibility to keep your account credentials secure.

To maintain the security and integrity of the hosted environment, we reserve the right, but not the obligation, to filter content, Computer Point requests, or website access for any web requests made from within the hosted environment.

Revisions to this AUP: We reserve the right to revise or modify this AUP at any time. Changes to this AUP shall not be grounds for early contract termination or non-payment.

Data Processing Policy ("DPP")

Responsibility for Processing of Personal Information

Roles: You are a Controller, and Computer Point is a Processor, for the Processing of Personal Information pursuant to the services provided by Computer Point under any Quote (the "Services").

Purposes: You and we acknowledge that the Personal Information you disclose to us is provided only for the limited and specified Business Purpose(s), and for no other reason. We will Process Personal Information solely for the purpose of providing or facilitating (as applicable) the Services.

No Additional Obligations: Unless otherwise specified in the Quote or otherwise agreed in writing by us, you shall not provide us with any data that imposes specific data security or data protection obligations on us other than those obligations specified in this DPP or a Quote. If you require additional services to address specific data security or data protection requirements applicable to your business, they must be agreed upon in writing between us and you before they can be implemented. We do not warrant or guaranty that we can or will agree to any such additional data security or data protection requirements. Until and unless we agree to provide such additional data-related services, you remain responsible for compliance with your specific regulatory, legal or industry data security obligations that apply to such data.

Restrictions: Computer Point will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purpose, or (ii) outside of the direct business relationship between Computer Point and you; or (c) combine Personal Information received from or on behalf of you with Personal Information received from or on behalf of any third party, or collected from Computer Point's own interaction with Individuals, except to perform a Business Purpose permitted by applicable law and/or the applicable Quote.

We will notify you of our use of Computer Point Affiliates and Third Party Subprocessors in accordance with this DPP, and we will make sure that Computer Point Affiliates and Third Party Subprocessors are subject to applicable written agreements as per Applicable Law.

We will provide a level of protection to Personal Information as required by the Quote, the MSA, and Applicable Law which, in all cases, shall be a reasonable care of protection. Notwithstanding the foregoing, you may take such reasonable steps as may be necessary (a) to remediate our unauthorized use of Personal Information, and (b) to ensure that Personal Information is used in accordance with the terms of this DPP by exercising your rights under this DPP and the Services Agreement. We will notify you if we determine that we are unable to meet our privacy or confidentiality obligations.

Your Instructions

You may provide additional instructions in writing to us regarding the Processing of Personal Information in accordance with Applicable Data Protection Law. We will promptly comply with all such instructions to the extent necessary for us to (i) comply with our Processor obligations under Applicable Data Protection Law or (ii) assist you to comply with your Controller obligations under Applicable Data Protection Law relevant to your use or receipt of the Services.

We will follow your instructions at no additional cost to you and within the timeframes reasonably necessary for you to comply with your obligations under Applicable Data Protection Law. We will immediately inform you if, in our opinion, your instructions infringe Applicable Data Protection Law; however, (a) under no circumstances shall we be responsible

for providing legal advice to you, and (b) no communication from us to you shall be considered to be, or relied upon as, legal advice.

Privacy Inquiries; Requests

If you receive a request or inquiry from an Individual related to Personal Information Processed by us, including an Individual's request to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Information, you must forward that request to our designated Privacy Officer (listed below) for follow-up. If we directly receive any inquiries from Individuals that have identified you as the Controller, we will promptly pass on such requests to you without responding to the Individual. Otherwise, we will advise the Individual to identify and contact the relevant controller(s).

Computer Point's Affiliates and Third Party Subprocessors

General Authorization: You hereby provide Computer Point with general written authorization to engage Computer Point Affiliates and Third Party Subprocessors as necessary to assist in the performance and/or provision of the Services.

Requirements: To the extent we engage Third Party Subprocessors and/or Computer Point Affiliates, we will require those entities to have and maintain the same level of data protection and security as Computer Point under the terms of this DPP and Applicable Data Protection Law. You will be entitled, upon written request, to receive copies of the relevant privacy and security terms of our agreement with any Third Party Subprocessors and Computer Point Affiliates that may Process Personal Information.

Subprocessor List: Computer Point maintains a list of Computer Point Affiliates and Third Party Subprocessors that may Process Personal Information ("Subprocessor List"). The Subprocessor List is below, and we will provide you with an updated list throughout the term of the Services if you request us to do so in writing. Changes, if any, will automatically modify and be included in the Subprocessor List.

Objections: Within thirty (30) calendar days of us providing notice to you (as described above), you may object to the intended involvement of a Third Party Subprocessor or Computer Point Affiliate by notifying us of the objection in writing. We will work together with you in good faith to find a mutually acceptable resolution to address any timely objection.

Cross-Border Data Transfers

Personal Information will be stored in our designated data storage centers in the United States or such other locations described in a Quote or other documentation from us to you; however, we may Process Personal Information globally as necessary to perform the Services, such as for support, incident management or data recovery purposes. Should it be necessary to do so, you and we will review supplemental measures that may be required based on applicable Data Protection Law for the transfer of Personal Information to countries that do not offer an adequate level of protection. Under those circumstances, you and we agree to work together in good faith to find a mutually acceptable resolution to address such supplementary measures.

Security; Confidentiality

We will maintain appropriate technical and organizational security measures for the Processing of Personal Information in our possession or control designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. Our security measures may include, for example, (i) utilizing firewall, router, and VPN-based access controls, (ii) regular examinations of security risks, (iii) role-based access controls

implemented in a manner consistent with the principle of "least privilege," (iv) logging of all access to host servers, applications, databases, routers, switches, etc., (v) password protection that includes minimum length requirements and periodic resets, (vi) implementation of anti-malware and anti-spyware solutions, and (vii) security incident and event management (SIEM) systems. All Computer Point and Computer Point Affiliates employees, and Third Party Subprocessors that Process Personal Information, are subject to written confidentiality arrangements.

Audit Rights

Timing: You may audit our compliance with our obligations under this DPP up to one time per year at your cost. More frequent audits will be permitted if expressly required by Applicable Data Protection Law.

Requests: We must receive your request for an audit in writing and no less than two (2) weeks before the proposed audit date. Your request must describe the proposed scope, duration, and start date of the audit. We will promptly review the proposed audit plan and provide you with any concerns or questions, and work cooperatively with you to agree on a final audit plan within a reasonable timeframe. Audits must be conducted during regular business hours and may not unreasonably interfere with our normal business activities.

Third Party Auditors: If you engage a third party auditor to conduct an audit, the third party must be mutually agreed to by you and by us unless the third party is a Regulator. We will not unreasonably withhold our consent to a third party auditor; however, prior to conducting any audit, a third party auditor must execute a written confidentiality agreement reasonably acceptable to us or otherwise be bound by a statutory or legal confidentiality obligation.

Copies: You agree to promptly provide us with a copy of any audit report, which will be considered confidential information. You agree to use or disclose the audit report only for the purposes of meeting your regulatory audit requirements and/or confirming compliance with the requirements of this DPP, and for no other purpose. Each party will bear its own costs in relation to the audit, unless we promptly inform you upon our review of the audit plan that we expect to incur additional charges or fees in the performance of the audit that are not covered by the fees payable under the Services Agreement, such as additional license or third party contractor fees. You will be responsible for paying those fees; however, we agree to try in good faith to mitigate those fees to the extent reasonably practicable.

Acceptance of Prior Reports. Notwithstanding the foregoing, if the scope of a proposed audit is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or a similar audit report issued by a qualified third party auditor within the prior twelve (12) months from the date of your audit request, and if we provide that report to you confirming there are no known material changes in the controls audited, you agree to accept the findings of the report in lieu of an audit of the same controls covered by the report.

Incident Management and Breach Notification

If we confirm that an Information Breach has, or likely has, occurred, then we will notify you the situation without undue delay but at the latest within 72 hours after confirmation. As information regarding the Information Breach is collected or otherwise becomes available to us, we will also provide you with (i) a description of the nature and reasonably anticipated consequences of the Information Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of information that were the subject of the Information Breach. You agree to coordinate with us on the content and timing of any public statements or required notices to affected Individuals and/or notices to relevant Regulators.

Return and Deletion of Personal Information

Upon termination of the Services, we will either promptly return or destroy (at our discretion) the Personal Information in our custody or control; provided, however, we shall be entitled to retain a copy of part or all of the Personal Information as reasonably necessary to evidence the parties' business relationship and/or the scope or type of Services provided or facilitated thereunder. Any Personal Information retained shall be considered to be your confidential information, and shall be treated as such at all times.

Legal Requirements

If we are required by law to provide access to Personal Information (such as to comply with a subpoena or other legal process, or to respond to government requests), then we will promptly inform you of that requirement. If, in the opinion of our counsel, a request for access ("Access Request") is legally valid and binding on us, then we will provide access as required unless we are otherwise ordered by a court of competent jurisdiction to refrain from doing so. You agree to indemnify us for all fees, costs, and expenses we incur in the process of determining whether the Access Request is valid, as well as any subsequent fees and costs we may incur relevant to the disclosure process.

Data Protection Officer

Computer Point's Chief Privacy Officer and local Data Protection Officer is _____, email: _____.

Definitions

- "**Applicable Data Protection Law**" means all data privacy or data protection laws or regulations globally that apply to the Processing of Personal Information under this DPP, including Applicable European Data Protection Law, Applicable UK Data Protection Law, the California Consumer Privacy Act as amended ("CCPA") and other U.S. state laws.
- "**Applicable European Data Protection Law**" means (i) the EU General Data Protection Regulation EU/2016/679, as supplemented by applicable EU Member State law and as incorporated into the EEA Agreement; and (ii) the Swiss Federal Act of 19 June 1992 on Data Protection, as amended.
- "**Applicable UK Data Protection Law**" means (i) the UK GDPR, meaning the EU General Data Protection Regulation EU/2016/679, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 pursuant to amendments to the EU General Data Protection Regulation EU/2016/679 made by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020; and (ii) the UK Data Protection Act 2018, as amended.
- "**Europe**" means for the purposes of this Data Processing Agreement (i) the European Economic Area, consisting of the EU Member States, Iceland, Liechtenstein and Norway; and (ii) Switzerland.
- "**Individual**" shall have the same meaning as the term "data subject" or the equivalent term under Applicable Data Protection Law.
- "**Information Breach**" means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed on systems controlled by Computer Point.
- "**Master Services Agreement**" means the master terms and conditions applicable to all services provided or facilitated by Computer Point, a copy of which can be found at _____.
- **"Process/Processing", "Controller", "Processor"** and **"Binding Corporate Rules"** (or the equivalent terms) have the meaning set forth under Applicable Data Protection Law.
- "**Quote**" shall have the meaning set forth in the Master Services Agreement.

- "**Service Provider**", "**Sell**", "**Share**", "**Business Purpose**", and "**Commercial Purpose**" have the meaning set forth under the law of the state in which you are headquartered; however, if no such law reasonably applies or defines such terms, then the terms shall have the same meaning as indicated in the CCPA.
- "**Computer Point Affiliate(s)**" means the subsidiar(y)(ies) of Computer Point that may Process Personal Information as set forth in this DPP.
- "**Personal Information**" shall have the same meaning as the term "personal data", "personally identifiable information (PII)" or the equivalent term under Applicable Data Protection Law.
- "**Regulator**" shall have the same meaning as the term "supervisory authority", "data protection authority" or the equivalent term under Applicable Data Protection Law.
- "**Services**" or the equivalent terms "**Service Offerings**" or "**services**" means any services that you have purchased through one or more Quotes.
- "**Third Party Subprocessor**" means a third party, other than a Computer Point Affiliate, which Computer Point subcontracts with and which may Process Personal Information as set forth in this DPP.

List of Approved Computer Point Subprocessors

Note: Subprocessors may have their own list of subprocessors. Please see each subprocessor's site for details.

Entity Name	Processing Activity	Location
ActiveCampaign	Email Marketing	USA (https://www.activecampaign.com)
Akamai Technologies	Sales & Customer Support	USA
Amazon Web Services (AWS)	Hosting	USA (https://aws.amazon.com)
Backblaze	Hosting	USA (Https://backblaze.com)
Box	Data Storage	USA
Calendly	Administrative	USA
DocuSign	Electronic Signature	USA
Cloudflare, Ltd.	Content Delivery	Processed at the data center closest to the end user. See: https://www.cloudflare.com/network/
CloudRadial	Customer Service	USA https://www.cloudradial.com)
ChurnZero	Security	USA (https://churnzero.com/security)
Dropbox	Data Storage	USA
Endear	Marketing	USA
Fortinet	Security	USA (https://www.fortinet.com/corporate/about-us/gdpr)
Google Cloud Platform	Cloud Infrastructure; Hosting	USA (https://cloud.google.com)
Huntress	Security	USA (https://support.huntress.io/hc/en-us/articles/14695369658259-Data-Processing-Addendum)
Hubspot	Marketing	USA

Ironclad	Contract Management	USA
Knowbe4	Security Awareness Training	USA (https://www.knowbe4.com/legal/global-data-processing-addendum)
Limelight Networks	Hosting	USA (https://www.limelight.com)
Looker	Data Analytics	USA
Mailchimp	Marketing	USA (https://mailchimp.com/about/security)
Microsoft Azure	Cloud Infrastructure; Hosting	Ireland (default) USA (on request) (https://azure.microsoft.com)
Netsuite	Accounting	USA
NorthPass	Customer Education	USA (https://www.northpass.com/privacy-policy)
ShareIt	Payment Processing	USA (https://www.mycommerce.com)
SafeAeon	Cloud Infrastructure; Security; Security Assessments	USA (https://www.safeaeon.com/privacy-policy/)
Salesforce.com	Customer Relationship Management; Customer Support	USA (https://www.salesforce.com)
Snowflake Inc.	Cloud Infrastructure	Germany (https://www.snowflake.com)
Twilio, Inc.	Calling & SMS Functionality	USA (https://www.twilio.com)
Wasabi Technologies	Hosting	USA (https://wasabi.com)
WithSecure	Security	USA (https://www.withsecure.com/content/dam/with-secure/en/investor/2023_WithSecure_Data_Processing_Agreement.pdf)
Zendesk, Inc.	Customer Support	USA (https://www.zendesk.com/trust-center)
Zoho Corporation	Customer Support	USA (https://www.zoho.com)