Service Statement

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

This Services Statement is our "owner's manual" that generally describes all managed services provided or facilitated by CJS Associates ("CJS," "we," "us," or "our"); however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services"). Activities or items that are not specifically described in the Quote will be out of scope and will not be included unless otherwise agreed to by us in writing.

This Services Statement contains important provisions pertaining to the auto-renewal of the Services in the Quote, as well as fee increases that may occur from time-to-time. Please read this Services Guide carefully and keep a copy for your records.

Initial Audit / Diagnostic Services

If an Initial Audit / Diagnostic Services are listed in the Quote, then we will audit your managed information technology environment (the "Environment") to determine the readiness for, and compatibility with, ongoing managed services. Our auditing services are comprised of:

- Audit to determine general Environment readiness and functional capability
- Review of hardware and software configurations
- Review of current vendor service / warranty agreements for Environment hardware and software
- Security vulnerability check
- Backup and disaster recovery solution audit
- Speed test and ISP audit
- Print output audit
- Office phone vendor service audit
- Asset inventory
- Email and website hosting audit
- IT support process audit

If deficiencies are discovered during the auditing process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and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

Onboarding Services

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

- Uninstall any monitoring tools or other software installed by previous IT consultants.
- Compile a full inventory of all protected servers, workstations, and laptops.
- Uninstall any previous virus protection and install our managed antivirus application.
- Install remote support access application on each managed device to enable remote support.
- Configure patch management application and check for missing security updates.
- Uninstall unsafe applications or applications that are no longer necessary.
- Optimize device performance including disk cleanup, antivirus, and spyware scans.

- Review firewall configuration and other network infrastructure devices.
- Review status of battery backup protection on all devices.
- Stabilize network and ensure that all devices can securely access the file server.
- Review and document current server configuration and status.
- Determine existing backup strategy and status; prepare backup options for consideration.
- Review password policies and update user and device passwords.
- As applicable, make recommendations for changes that should be considered to the managed environment.

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

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

Ongoing / Recurring Services

Ongoing/recurring services are services that are provided to you on an ongoing basis and, unless otherwise indicated in a Quote, are billed to you monthly. Ongoing services generally begin upon the completion of onboarding services; therefore, any delays or interruptions to the onboarding services may delay the commencement of ongoing/recurring services.

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

Managed Services

The following describes our services, which can be purchased individually or as part of a Service Plan (See your Quote for details on which Service Plan and/or individual services you purchased):

SERVICES	GENERAL DESCRIPTION
Basic Managed Workstation	This bundle includes the following services (each of which is described in greater detail below): • Remote Monitoring and Management for Cybersecurity • Updates and Patching • Continuous and Preventative Maintenance • Managed Antivirus/Antimalware • Persistent Threat Detection
Advanced Managed Workstation	This bundle includes the following services (each of which is described in greater detail below): • Remote Monitoring and Management for Cybersecurity • Updates and Patching • Continuous and Preventative Maintenance • Managed Antivirus/Antimalware • Persistent Threat Detection (cont.) • Advanced Security Policy Management • Privileged Access Management • DNS Protection • Remote Helpdesk (unlimited) *Personal computer issues are excluded

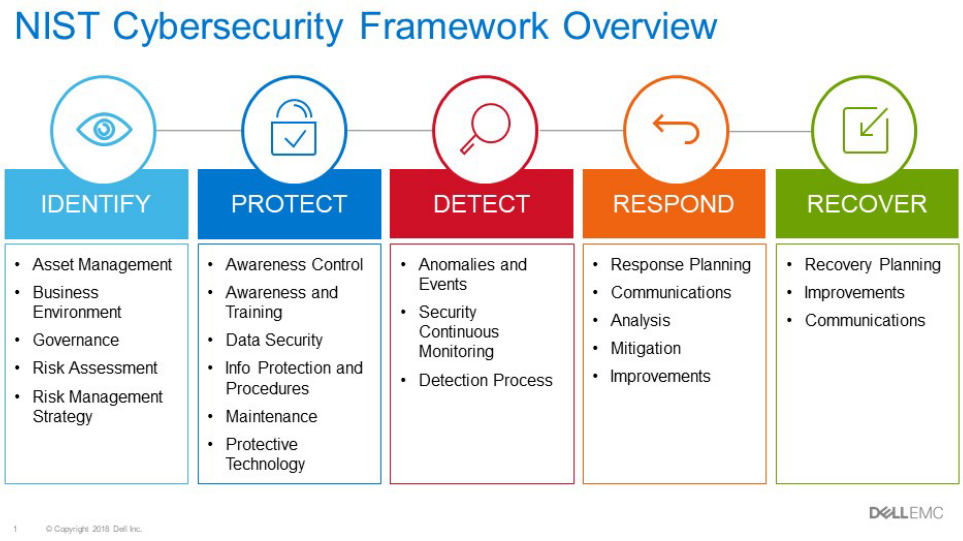
Advanced Managed Server	This bundle includes the following services (each of which is described in greater detail below): • Remote Monitoring and Management for Cybersecurity • Updates and Patching • Continuous and Preventative Maintenance • Managed Antivirus/Antimalware • Persistent Threat Detection • Advanced Security Policy Management • Privileged Access Management
Basic Managed User	This bundle includes the following services (each of which is described in greater detail below): • Email Threat Protection • M365 Backup + Archiving • End User Security Awareness Training
Advanced Managed User 8x5	This bundle includes the following services (each of which is described in greater detail below): • Email Threat Protection • M365 Backup + Archiving • End User Security Awareness Training • Remote Monitoring and Management for Cybersecurity* • Updates and Patching* • Managed Antivirus/Antimalware* • Persistent Threat Detection* • Advanced Security Policy Management* • Privileged Access Management* • US-Based Helpdesk (Work Hours) *Workstation tools are for Company machines only. Personal computer issues are excluded.
Advanced Managed User 24x7	This bundle includes the services in “Advanced Managed User 8x5” plus: • US-Based Helpdesk (24x7) *Workstation tools are for Company machines only. Personal computer issues are excluded.
Remote Monitoring and Management	Software agents installed in Covered Equipment (defined below) report status and IT-related events on a 24×7 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.
Remote Infrastructure Maintenance & Support	• Configuration, monitoring, and preventative maintenance services provided for the managed IT infrastructure • If remote efforts are unsuccessful then CJS 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 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.

Network Security Management	• **Configuration, monitoring, and preventative maintenance services provided for the managed IT network** • **If remote efforts are unsuccessful then CJS will dispatch a technician to the Client's premises to resolve covered incidents (timing of onsite support is subject to technician availability and scheduling)**
Disaster Recovery (for managed servers only)	• 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 • Biweekly 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:** Please see Quote for retention period **Capacity:** Please see Quote for capacity, i.e., amount of total data that will be backed up. **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, which are currently Monday through Friday 7am to 5pm EST. • **Request Method:** Requests to restore backed up data should be made through one of the following methods: ○ **Chat:** Included ○ **Telephone:** 410-671-5780 ○ **Email:** CJShelpdesk@CJSassociates.com • **Restoration Time:** We will endeavor to restore backed up data as quickly as possible following our receipt of a request to do so; however, in all cases data restoration services are subject to technician availability. Generally, we can restore between 0 and 100MB of data within 4 hours of your request, and 100 MB to 500 MB within 8 hours of your request. Data restoration exceeding 500 MB will be handled in accordance with technician availability. Please Note: This service is available for managed servers only. Additional costs may apply for recovery of data from individual workstations.
***Backup Monitoring**	• Monitors backup status for certain backup applications then-installed in the managed environment, such as successful completion of backup, failure errors, and destination free space restrictions/limitations. • Helps ensure adequate access to Client's data on 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 disaster recovery solution.

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.**
***Block of Hours / Allocated Consulting Hours**	If you purchase one or more blocks of technical support or consulting hours from CJS, then we will provide our professional information technology consulting services to you from time to time on an ongoing, "on demand" basis ("Services"). The specific scope, timing, term, and pricing of the Services (collectively, "Specifications") will be determined between you us at the time that you request the Services from us. You and we may finalize the Specifications (i) by exchanging emails confirming the relevant terms, or (ii) by you agreeing to an invoice, purchase order, or similar document we send to you that describes the Specifications (an "Invoice"), or in some cases, (iii) by us performing the Services or delivering the applicable deliverables in conformity with the Specifications. If we provide you with an email or an Invoice that contains details or terms for the Services that are different than the terms of than the Quote, then the terms of the email or Invoice (as applicable) will control for those Services only. A Service will be deemed completed upon our final delivery of the applicable portions of Specifications unless a different completion milestone is expressly agreed upon in the Specifications ("Service Completion"). (For example, sales of hardware will be deemed completed when the hardware is delivered to you; licensing will be completed when the licenses are provided to you, etc.) Any defects or deviations from the Specifications must be pointed out to us, in writing, within ten (10) days after the date of Service Completion. After that time, any issues or remedial activities related to the Services will be billed to you at our then-current hourly rates. Unless we agree otherwise in writing, Services will be provided only during our normal business hours, which are currently 9 – 6 PM Pacific Time. Services provided outside of our normal business hours are subject to increased fees and technician availability and require your and our mutual consent to implement. The priority given to implementing the Services will be determined our reasonable discretion, considering any milestones or deadlines expressly agreed upon in an invoice or email from CJS. If no specific milestone or deadline is agreed upon, then the Services will be performed in accordance with your needs, the specific requirements of the job(s), and technician availability.
Continuous and Preventative Maintenance	• Disk Cleanup • Automated scripts for maintenance • Software monitoring and classification • Critical log management
Managed AntiVirus/AntiMalware	• Managed intrusion protection offering multiple layers of defense to protect managed devices from attacks, malicious code, and suspicious processes • Centralized policy management • Actionable incident reporting • Assisted remediation* *Remediation activities are limited to the features and functions of the applicable third-party antivirus/antimalware solution

Persistent Threat Detection	• Persistent footholds detection helps detect persistent actors who may have gained unauthorized access to the managed network • Ransomware canaries • External Recon feature provides visibility into the managed network's external attack surface, identifying the means and methods by which attackers may attempt to attack the managed network • Assisted remediation* • 24x7 ThreatOps team that analyzes potential threats, creates incident reports, and assists in the remediation of cyberthreats * Remediation activities are limited to the features of the applicable third-party antivirus/ antimalware solution
Advanced Security Policy Management	• Implementation of lockdown policies to automate your protection • Monitors every 5 minutes to help ensure compliance • Ransomware protection policies • User Logon Report
Privileged Access Management	• Remove admin privileges • Audit & Remediation of access-related issues* • Provide granular-type Windows privilege control • Elevate privileges for requested applications & actions • Implement rules to automate future access requests * Remediation activities are limited to non-malware related access issues. Remediation of/from malware or virus activities are handled under our Managed Antivirus/Antimalware service, above
***Firewall Solution (firewall appliance provided by CJS)**	• Provide 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 must be returned to CJS upon the termination of Services.
***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.
Firewall (as a Service)	• Provide a FIPS 140-2 (or better) compliant firewall configured for your organization's specific bandwidth, remote access, and user needs • Helps to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; provides website content filtering functionality *Only applicable where specified as part of specific managed networks

Email Threat Protection	• **Managed email protection from phishing, business email compromise (BEC), SPAM, and email-based malware** • **Friendly Name filters to protect against social engineering impersonation attacks on managed devices** • **Protection against social engineering attacks like whaling, CEO fraud, business email compromise or W-2 fraud** • **Protects against newly registered and newly observed domains to catch the first email from a newly registered domain** • **Protects against display name spoofing** • **Protects against "looks like" and "sounds like" versions of domain names**
M365 Backup + Archive	Provides advanced cloud-based storage to protect and preserve Microsoft Office 365 and Gmail data, while also providing journaling-based email archiving for Exchange and Gmail to preserve, search, hold & comply with compliance regulations
End User Security Awareness Training (BPP)	• 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 • Tiered by user count stated in the Quote
Hardware as a Service (HaaS)	• Provision and deployment of designated hardware (see the Quote or other applicable schedule for complete hardware list – *"HaaS Equipment". Refer to Additional Description of Services—Hardware as a Service (HaaS)"* section for details) • Installation of HaaS Equipment • Repair/replacement of HaaS Equipment (see below for additional details) • Technical support for HaaS Equipment • Periodic replacement of HaaS Equipment (see below for additional details)
Two Factor Authentication	• Advanced two factor authentication with advanced admin 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
Password Manager	• Password Vault: Securely store and organize passwords in a secure digital location accessed through your browser or an app • Password Generation: Generate secure passwords with editable options to meet specific criteria • 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. • Single Sign-On: Single sign-on grants authorized employees or users access to applications with a single set of login credentials, based on a user's identity and permission levels. Single sign-on relies on SAML (Security Assertion Markup Language), a secure, behind-the-scenes protocol, to authenticate users to cloud, mobile, legacy, and on-premise apps • Browser App: Browser extension permits easy access to all of your information • Smart-Phone App: Mobile phone app enables access to your vault and stored information on your mobile device.

Labor for New/Replacement Workstations	**Includes all labor charges for setup of new workstations, or replacement of existing workstations.** • **Labor covers:** • **New computers / additional computers added during the term of the Quote;** • **Replacement of existing computers that are four (4) or more years old (as determined by the manufacturer's serial number records);** • **Replacement of existing computers that lost/stolen or irreparably damaged and/or out of warranty but not yet four years old;** **Operating systems upgrades – subject to hardware compatibility.** **The following restrictions apply:** • **Upgrades or installs of new or replacement computers are limited to four (4) devices per month unless otherwise approved in advance by CJS;** • **This service is not available for used or remanufactured computers; and,** • **• New/replacement computers must be business-grade machines (not home) from a major manufacturer like Dell, Intel, HPE, Apple or Lenovo**
Wi-Fi Services	• CJS will install at the Client's premises a sufficient number of Wireless Access Points to provide a bandwidth of at least 10Mbps (download) in all areas requiring wireless network coverage, as agreed upon by CJS and Client • CJS will maintain, supervise, and manage the wireless system, including hardware and software at no additional cost • Installed equipment will be compatible with the then-current industry standards, and renew the hardware through new Quote to Client every five years at the latest • CJS 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)
NIST Risk Assessment	• Perform a cybersecurity assessment under NIST CSF using the NIST Risk Management Framework & NIST 800-53 • Identifies how Client currently assesses, mitigates, and tracks its cybersecurity requirements • Identifies authorized and unauthorized devices in the managed network • Identifies gaps or deficiencies in the Client's operations that would prevent compliance under NIST CSF. The assessment will cover the following five core areas of the NIST framework: 

	The results of the assessment will be provided in a report that will identify detected risks and your organization's current maturity levels (i.e., indicators that represent the level of capabilities within your organization's security program) and will propose actionable activities to help increase relevant maturity levels and augment your organization's security posture. **Please Note:** This service is limited to an assessment/audit only. Remediation of issues discovered during the assessment, as well as additional solutions required to bring your managed environment into compliance, are not part of this service. After the audit is complete, we will discuss the results with you to determine what steps, if any, are needed to bring your organization into full compliance.
***Virtual Chief Information Officer (vCIO)**	Act as the main point of contact for certain business-related IT issues and concerns. • Assist in creation of information/data-related plans and budgets • Provide strategic guidance and consultation across different technologies • Create company-specific best standards and practices • Provide education and recommendations for business technologies • Participate in scheduled meetings to maintain goals • Maintain technology documentation • Assess and make recommendations for improving technology usage and services.
***Voice Over IP (VoIP) Services**	• 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

Additional Description of Services

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

Hardware as a Service (HaaS)

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

Deployment: We will deploy the HAAS Equipment within the timeframe stated in the Quote, provided that you promptly provide all information that we reasonably request from you to complete deployment. This deployment guaranty does not apply to any software, other managed services, or hardware devices other than the HAAS Equipment. If you wish to delay the deployment of the HaaS Equipment, then you may do so provided that you give us written notice of your election to delay no later than five (5) days following the date you sign the Quote. Deployment shall not extend beyond two (2) months following the date on which you sign the Quote. You will be charged at the rate of fifty percent (50%) of the monthly recurring fees for the HaaS-related services during the period of delay. Following deployment, we will charge you the full monthly recurring fee (plus other usage fees as applicable) for the full term indicated in the Quote.

Equipment Hardware Repair or Replacement: CJS will repair or replace HAAS Equipment by the end of the business day following the business day on which the applicable problem is identified by, or reported to, CJS and has been determined by CJS to be incapable of being remediated remotely.
This warranty does not include the time required to rebuild your system, such as the time required to configure a replacement device, rebuild a RAID array, reload the operating system, reload and configure applications, and/or restore from backup (if necessary).

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

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

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

Usage. You will use all CJS-hosted or CJS-supplied equipment and hardware for your internal business purposes only. You shall not sublease, sublicense, rent or otherwise make the HaaS Equipment available to any third party without our prior written consent. You agree to refrain from using the infrastructure in a manner that unreasonably or materially interferes with our other hosted equipment or hardware, or in a manner that disrupts or that is likely to disrupt the services that we provide to our other clientele. We reserve the right to throttle or suspend your access and/or use of the HaaS Equipment if we believe, in our sole but reasonable judgment, that your use of the infrastructure violates the terms of the Quote, this Services Guide, or the Agreement.

Covered Equipment/Hardware/Software

In this Services Guide, "Covered Devices" and "Supported Software" will be referred to collectively as the "Environment" or "managed environment."

Hardware Managed Services will be applied to the equipment listed in the Quote ("Covered Hardware"), or on which we install our software agents (or similar monitoring software), and a list of these devices will be provided to you separately ("Covered Devices"). You will be provided with an updated list of Covered Hardware once all software agents have been installed. 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 but which are/have been receiving Services.

Software Managed Services will apply to the software listed in the Quote ("Supported Software") provided, however, that all Supported Software must, at all times, be properly licensed, and under a maintenance and support agreement from the Supported Software's manufacturer. CJS will provide support for any software applications that are licensed through us, as well as any software that we approve in writing (email is sufficient for this purpose). Such software ("Supported Software") will be supported up to Level 2-type support; support required above this level will be facilitated with the applicable software vendor/producer. Coverage for non-

Supported Software is outside of the scope of the Services and will be provided to you on a time and materials basis. Should our technicians provide you with advice concerning non-Supported Software, the provision of that advice should be viewed as an accommodation, not an obligation, to you.

CJS provides the Services on a "per user" basis. As such, our Managed 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 the Client and used primarily for business, (ii) is regularly connected to Client's managed network, and (iii) has installed on it a software agent through which we (or our designated third party providers) can monitor the device. In this Service Guide, covered Business Devices are referred to as "Covered Hardware".

Physical Locations Covered by Services

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

Term; Termination

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

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

Auto-Renewal. Unless otherwise expressly stated in the Quote, upon the expiration of the Initial Service Term, the Service Term will automatically renew for contiguous terms equal to the initial Service Term unless either party notifies the other of its intention to not renew or renegotiate the Services with no less than thirty (30) days prior written notice of termination (email is sufficient for this purpose). If the effective date of termination falls on a day other than the last day of the calendar month, then the date of termination will automatically become the last day of the calendar month in which termination occurs.

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

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

Within ten (10) days after being directed to do so, Client will remove, package and ship, at Client's expense and in a commercially reasonable manner, all hardware, equipment, and accessories provided to Client by CJS that were used in the provision of the Services. If you fail to timely return all equipment to us, or if the equipment is returned to us damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

Minimum Requirements/Exclusions

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

- Server hardware must be under current warranty coverage
- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software and have all of the latest Microsoft service packs and critical updates installed
- All software must be genuine, licensed and vendor-supported
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software
- The managed environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored
- All wireless data traffic in the environment must be securely encrypted
- There must be an outside static IP address assigned to a network device if advised in the quote, allowing VPN/RDP control access
- All servers must be connected to working UPS devices
- All workstations and network gear must be connected to appropriate Surge Protection or UPS devices
- Recovery coverage assumes data integrity of the backups or the data stored on the backup devices. We do not guarantee the integrity of the backups or the data stored on the backup devices. Server restoration will be to the point of the last successful backup
- Client must provide all software installation media and key codes in the event of a failure
- Any costs required to bring the Environment up to these minimum standards are not included in this Service Statement
- Client must provide us with exclusive administrative privileges to the Environment
- 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

Minimum Requirements. In addition to the above, the following minimum requirements apply to all managed services:

- All Covered Devices (defined above) shall be under warranty with the manufacturer or other vendor or be less than 3 years old. If a Covered Device reaches the age of 3 years during the term of Services, Client shall purchase a warranty covering either the repair or replacement of the device;
- All Covered Devices must be running a then-current, vendor-supported operating system; and
- All Covered Devices must meet or exceed the hardware requirements necessary to run the installed operating system(s) and all other Supported Software (defined above).
- If any Covered Device fails to meet and/or maintain the minimum standards listed above, then Client agrees to work constructively and cooperatively with CJS to replace the device at Client's expense through CJS.
- Client acknowledges that, due to the lack of manufacturer support, Covered Devices or Supported Software that does not meet the minimum standards listed above ("Legacy Systems") may, at CJS's sole discretion, result in a higher monthly charge for the Services. Client agrees to pay such additional charges for which CJS informs Client, in advance of incurring such charges. Client further agrees that a failed Legacy System, may, at CJS's discretion, be considered obsolete and/or unserviceable.
- In all cases, requests to perform service on, or provide the Services to, a failed or failing Legacy System will be determined by CJS on a case-by-case basis.

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

- Customization of third party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- Battery backup replacement.
- Equipment relocation.
- The cost to bring the Environment up to the Minimum Requirements (unless otherwise noted in "Scope of Services" above).

- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.

Service Levels

Automated monitoring is provided on an ongoing (*i.e., 24x7x365*) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our business hours (currently M-F, 8:00 AM – 5:00 PM Pacific Time, excluding legal holidays and CJS-observed holidays as listed below), unless otherwise specifically stated in the Quote or as otherwise described below.

We will respond to problems, errors, or interruptions in the provision of the Services during business hours in the timeframe(s) described below. Severity levels will be determined by CJS in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; CJS 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 processes can continue)	Response within eight (8) business hours after notification
Small Service degradation (e.g., business processes 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 CJS is notified of the applicable issue / problem by Client through CJS's designated chat, email (CJShelpdesk@CJSassociates.com) or by telephone at 925-687-0400. Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts. Help desk support provided outside of our normal support hours will be provided on a case-by-case basis and will be billed to Client at the hourly rate of $300/hour (2 hour minimum applies).

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 CJS 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 hourly rate of $300/hour (2 hour minimum applies).

All hourly services are billed in 6 minute increments, and partial increments are rounded to the next highest increment. A one (1) hour minimum applies to all Non-Business Hour Support.

CJS-Observed Holidays: CJS 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 the MSA), then Client will be entitled to receive a pro-rated service credit equal to 1/30 of that calendar month's recurring service fees (excluding hard costs, licenses, etc.) for each day on which the Target Service Level is missed. Under no circumstances shall credits exceed 30% of the total monthly recurring service fees under an applicable Quote.

Fees

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

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

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

Increases. In addition, we reserve the right to increase our monthly recurring fees and, if applicable, our data recovery-related fees; provided, however, if an increase is more than five percent (5%) of the fees charged for the Services in the prior calendar year, then you will be provided with a sixty (60) day opportunity to terminate the Services by providing us with written notice of termination. You will be responsible for the payment of all fees that accrue up to the termination date and all pre-approved, non-mitigatable expenses that we incurred in our provision of the Services through the date of termination. Your continued acceptance or use of the Services after this sixty (60) day period will indicate your acceptance of the increased fees.

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

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

Travel Time. If onsite services are provided, 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.

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

- **ACH.** When enrolled in an ACH payment processing method, you authorize us to electronically debit your designated checking or savings account, as defined and configured by you in our payment portal, for any payments due under the Quote. This authorization will continue until otherwise terminated in writing by you. We will apply a $35.00 service charge to your account for any electronic debit that is returned unpaid due to insufficient funds or due to your bank's electronic draft restrictions.
- **Credit Card.** When enrolled in a credit card payment processing method, you authorize us to charge your credit card, as designated by you in our payment portal, for any payments due under the Quote.
- **Check.** You may pay by check provided that your check is delivered to us prior to the commencement of Services. Checks that are returned to us as incorrect, incomplete, or "not sufficient funds" will be subject to a $50 administration fee and any applicable fees charged to us by your bank or financial institution.

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

Additional Terms

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

Monitoring Services; Alert Services
Unless otherwise indicated in the Quote, all monitoring and alert-type services are limited to detection and notification functionalities only. Monitoring levels will be set by CJS, and Client shall not modify these levels without our prior written consent. Initially, the policies will be set to a baseline standard as determined by CJS; however, Client is advised to establish and/or modify the policies that correspond to Client's specific monitoring and notification needs.

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

Configuration of Third Party Services
Certain third party services provided to you under this Service Statement may provide you with administrative access through which you could modify the configurations, features, and/or functions ("Configurations") of those services. However, any modifications of Configurations made by you without our knowledge or authorization could disrupt the Services and/or or cause a significant increase

in the fees charged for those third party services. For that reason, we strongly advise you to refrain from changing the Configurations unless we authorize those changes. You will be responsible for paying any increased fees or costs arising from or related to changes to the Configurations.

Dark Web Monitoring
Our dark web monitoring services utilize the resources of third party solution providers. Dark web monitoring can be a highly effective tool to reduce the risk of certain types of cybercrime; however, we do not guarantee that the dark web monitoring service will detect all actual or potential uses of your designated credentials or information.

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

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

Anti-Virus; Anti-Malware
Our anti-virus / anti-malware solution will generally protect the Environment from becoming infected with new viruses and malware ("Viruses"); however, Viruses that exist in the Environment at the time that the security solution is implemented may not be capable of being removed without additional services, for which a charge may be incurred. We do not warrant or guarantee that all Viruses and malware will be capable of being detected, avoided, or removed, or that any data erased, corrupted, or encrypted by malware will be recoverable. To improve security awareness, you agree that CJS 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." An "unlimited" service designation means that, subject to the terms of this FUP, you may use the service as reasonably necessary for you to enjoy the use and benefit of the service without incurring additional time-based or usage-based costs. However, unless expressly stated otherwise in the Quote, all unlimited services are provided during our normal business hours only and are subject to our technicians' availabilities, which cannot always be guaranteed. In addition, we reserve the right to assign our technicians as we deem necessary to handle issues that are more urgent, critical, or pressing than the request(s) or issue(s) reported by you. Consistent with this FUP, you agree to refrain from (i) creating urgent support tickets for non-urgent or non-critical issues, (ii) requesting excessive support services that are inconsistent with normal usage patterns in the industry (e.g., requesting support in lieu of training), (iii) requesting support or services that are intended to interfere, or may likely interfere, with our ability to provide our services to our other customers.

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

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

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

Backup (BDR) Services
All data transmitted over the Internet may be subject to malware and computer contaminants such as viruses, worms and trojan horses, as well as attempts by unauthorized users, such as hackers, to access or damage Client's data. Neither CJS 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. CJS cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that CJS 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 CJS 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, CJS 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. CJS is not a warranty service or repair center. CJS 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 CJS will be held harmless, and (ii) CJS is not responsible for the quantity, condition, or timely delivery of the Procured Equipment once the equipment has been tendered to the designated shipping or delivery courier.

Business Review / IT Strategic Planning Meetings

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

VCTO or VCIO Services

The advice and suggestions provided us in our capacity as a virtual chief technology or information officer will be for your informational and/or educational purposes only. CJS 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 CJS on Client's corporate records or accounts.

Sample Policies, Procedures.

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

Penetration Testing; Vulnerability Assessment

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

No Third Party Scanning

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

Obsolescence

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

Hosting Services

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

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

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

Licenses

If we are required to re-install or replicate any software provided by you as part of the Services, then it is your responsibility to verify that all such software is properly licensed. We reserve the right, but not the obligation, to require proof of licensing before installing, re-installing, or replicating software into the managed environment. The cost of acquiring licenses is not included in the scope of the Quote unless otherwise expressly stated therein.

VOIP – Dialing 911 (Emergency) Services

The following terms and conditions apply to your use of any VoIP service that we facilitate for you or that is provided to you by a third-party provider of such service. Please note, by using VoIP services you agree to the provisions of the waiver at the end of this section. If you do not understand or do not agree with any of the terms below, you must not subscribe to, use, or rely upon any VoIP service and, instead, you must contact us immediately.

There is an important difference in how 9-1-1 (i.e., emergency) services can be dialed using a VoIP service as compared to a traditional telephone line. Calling emergency services using a VoIP service is referred to as "E911."

Registration: You are responsible for activating the E911 dialing feature by registering the address where you will use the VoIP service. **This will not be done for you, and you must take this step on your own initiative.** To do this, you must log into your VoIP control panel and provide a valid physical address**. If you do not take this step, then E911 services may not work correctly, or at all, using the VoIP service. Emergency service dispatchers will only send emergency personnel to a properly registered E911 service address.**

Location: The address you provide in the control panel is the location to which emergency services (such as the fire department, the police department, etc.) will respond. For this reason, it is important that you correctly enter the location at which you are using the VoIP services. PO boxes are not proper addresses for registration and must not be used as your registered address. Please note, even if your account is properly registered with a correct physical address, (i) there may be a problem automatically transmitting a caller's physical location to the emergency responders, even if the caller can reach the 911 call center, and (ii) a VoIP 911 call may go to an unstaffed call center administrative line or be routed to a call center in the wrong location. These issues are inherent to all VoIP systems and services. **We will not be responsible for, and you agree to hold us harmless from, any issues, problems, incidents, damages (both bodily- and property-related), costs, expenses, and fees arising from or related to your failure to register timely and correctly your physical location information into the control panel.**

Address Change(s): If you change the address used for E911 calling, the E911 services may not be available and/or may operate differently than expected. Moreover, if you do not properly and promptly register a change of address, then emergency services may be directed to the location where your services are registered and not where the emergency may be occurring**. For that reason, you must register a change of address with us through the VoIP control panel no less than three (3) business days prior to your anticipated move/address change.** Address changes that are provided to us with less than three (3) business days' notice may cause incorrect/outdated information to be conveyed to emergency service personnel. If you are unable to provide us with at least three (3) business days' notice of an address change, then you should not rely on the E911 service to provide correct physical location information to emergency service personnel. Under those circumstances, you must provide your correct physical location to emergency service dispatchers if you call them using the VoIP services.

If you do not register the VoIP service at your location and you dial 9-1-1, that call will be categorized as a "rogue 911 call." **If you are responsible for dialing a rogue 911 call, you will be charged a non-refundable and non-disputable fee of $250/call.**

Power Loss: If you lose power or there is a disruption to power at the location where the VoIP services are used, then the E911 calling service will not function until power is restored. You should also be aware that after a power failure or disruption, you may need to reset or reconfigure the device prior to utilizing the service, including E911 dialing.

Internet Disruption: If your internet connection or broadband service is lost, suspended, terminated or disrupted, E911 calling will not function until the internet connection and/or broadband service is restored.

Account Suspension: If your account is suspended or terminated, then all E911 dialing services will not function.

Network Congestion: There may be a greater possibility of network congestion and/or reduced speed in the routing of E911 calls as compared to 911 dialing over traditional public telephone networks.

WAIVER: You hereby agree to release, indemnify, defend, and hold us and our officers, directors, representatives, agents, and any third party service provider that furnishes VoIP-related services to you, harmless from any and all claims, damages, losses, suits or actions, fines, penalties, costs and expenses (including, but not limited to, attorneys' fees), whether suffered, made, instituted or asserted by you or by any other party or person (collectively, "Claims") arising from or related to the VoIP services, including but not limited to any failure or outage of the VoIP services, incorrect routing or use of, or any inability to use, E911 dialing features. The foregoing waiver and release shall not apply to Claims arising from our gross negligence, recklessness, or willful misconduct.