cjsassociates℠
IT Solutions for the Office and Cloud

SERVICES GUIDE

Managed IT Services — Definitions & Standards

This Services Guide is part of your agreement with CJS Associates, LLC.
It works together with your Quote and your Master Services Agreement (MSA).

Version 2.1 | July 2026

Table of Contents

© 2026 CJS Associates, LLC. Confidential.

0. Introduction

This Services Guide is part of your agreement with CJS Associates, LLC. It works alongside two other documents: your Quote, which lists the specific services and pricing for your account, and the Master Services Agreement (MSA), which governs the legal terms of our relationship with you.

This guide does three things:

- **Defines each service CJS provides —** what is included, what is not, and what you can expect.
- **Sets the service standards —** how we respond to issues, what our coverage hours are, and what your environment needs to qualify for managed coverage.
- **Serves as a reference —** if you have a question about what is or is not covered, the answer should be in here. If it is not, contact us.

How conflicts work: If there is ever a conflict between this guide and the MSA, this guide governs. If there is a conflict between either of those documents and your Quote, the Quote governs. This means your Quote can always be used to tailor the terms of your agreement to your specific situation. When in doubt, contact us — we would rather answer a question than have a misunderstanding become a problem.

How to read this guide: Services are organized to match your Quote. *MSP — User Services* covers what protects your people and their devices. *MSP — Company Services* covers your business infrastructure. *Microsoft 365 Licensing* covers your Microsoft environment. *Optional Add-Ons* covers services not included in a standard plan. *Service Standards* defines how we work and what your environment must meet to receive managed coverage. The *Glossary* at the back defines every technical term used in this document.

© 2026 CJS Associates, LLC. Confidential.

1. MSP — User Services

User services are billed per user or per device, depending on your agreement. Every person covered under a managed service plan has a service tier assigned to them. The services in this section apply to each covered user and their primary company-owned device unless otherwise noted.

1.1 MSP Managed User — 24x7

The *MSP Managed User* plan is the foundation of CJS managed IT service. It covers a single user and their primary company-owned workstation with full protection, monitoring, and 24x7 support access. Every covered user receives the following:

- **24x7 Help Desk Access:** Your team can contact our help desk any time — days, nights, weekends, and holidays, including all major holidays. Tier 1 and Tier 2 issues are handled around the clock. Issues requiring senior engineering are addressed Monday through Friday, 8:00 AM to 5:00 PM PT.
- **Remote Monitoring & Management (RMM):** Your workstation is continuously monitored for performance, health, and security. We receive alerts when something goes wrong — often before you notice a problem.
- **Operating System (OS) and Third-Party Patching:** Operating system updates and patches for supported third-party software are applied on a scheduled basis to keep your workstation secure and current.
- **Managed EDR (Endpoint Detection & Response):** Real-time protection against viruses, malware, and ransomware at the device level. Threats are detected, contained, and remediated automatically where possible.
- **Managed ITDR (Identity Threat Detection & Response):** Monitors your Microsoft 365 user identity for suspicious activity, unauthorized access attempts, and credential-based threats.
- **Managed ISPM (Identity Security Posture Management):** Continuously monitors how your Microsoft 365 identity and access permissions are configured — identifying accounts with excessive access, weak policies, or signs of misconfiguration before they become a vulnerability.
- **Managed ESPM (Endpoint Security Posture Management):** Continuously monitors the security configuration of your workstation — checking for policy gaps, missing protections, or settings that fall outside the secure baseline CJS maintains for your environment.
- **Multi-Factor Authentication (MFA):** MFA is enabled and enforced for your Microsoft 365 account as part of the standard security baseline.
- **Email Threat Protection:** Your Microsoft 365 email is protected against phishing, spoofing, and malicious attachments. SPF, DKIM, and DMARC are configured for your domain.
- **Password Manager:** A business-grade password manager is included to support strong, unique credential practices across your accounts.
- **Workstation Backup:** Data within the standard backup scope configured for your workstation is automatically backed up on a continuous basis. In the event of data loss or a complete device failure, your files can be restored quickly — and once a replacement device is set up, reconnecting to your backed-up data is fast and straightforward. *See Section 1.2 for scope and retention details and Section 2.6.2 for backup policy*.
- **Microsoft 365 / Intune Management:** Your Microsoft 365 environment is managed and maintained as part of your user plan, including device enrollment in Intune where applicable.

> **Note:** *What is not included in the MSP Managed User plan: support for personal devices, software outside the managed scope, and any service not listed above or in your Quote. See Section 5.5 — Exclusions for the full list.*

© 2026 CJS Associates, LLC. Confidential.

1.2 Workstation Backup

Workstation backup is included as part of the *MSP Managed User* plan. CJS backs up data within the standard backup scope configured for your workstation, protecting your data against accidental deletion, file corruption, and device failure.

- **Standard retention:** All workstation backups are retained for 90 days. Files deleted or changed within the last 90 days can be recovered.
- **Extended retention:** Retention beyond 90 days is available at additional cost. Contact CJS to discuss extended retention options.
- **Device failure:** If your workstation fails entirely, CJS will rebuild your device or configure a replacement and restore your backed-up files. Getting back to your data is as simple as connecting your new device — your files come with you.
- **What is backed up:** CJS backs up data within the standard backup scope configured during onboarding, which typically includes your Documents, Desktop, and Pictures. Data stored outside the configured backup scope — including local-only folders, external drives, or application-specific storage locations — is not covered by this service. If you have questions about what is backed up in your specific environment, contact CJS. *See Section 2.6.2 for full backup policy, including information on why CJS does not perform full system image backups.*

> **Note:** *Clients are responsible for maintaining good data practices, including saving business-critical files within the configured backup scope. CJS provides guidance on data practices during onboarding and at scheduled business reviews.*

1.3 Hardware Warranty & Repair

Hardware warranty coordination and routine repair labor are included in your managed service plan. CJS handles the process of working with manufacturers and vendors when covered hardware needs repair or replacement — you do not need to navigate vendor support on your own.

- **Manufacturer warranty:** When covered hardware fails and is under manufacturer warranty, CJS coordinates the warranty claim and repair process on your behalf.
- **Routine repair labor:** Minor hardware repairs that can be performed efficiently by CJS — such as memory upgrades, drive replacements, or component swaps — are included as part of the managed service at no additional labor charge.
- **Out-of-warranty repair:** If a device falls outside the scope of manufacturer warranty, CJS will make reasonable efforts to repair it. Out-of-scope repairs are billable at standard rates. CJS will notify you before proceeding with any billable repair work.
- **Hardware replacement:** When hardware must be replaced, CJS procures and configures replacement equipment. Hardware and setup costs are billed separately.

> **Note:** *Physical repair of hardware damaged by environmental factors, accidents, or unauthorized modifications is outside standard managed scope and will be quoted separately. Devices beyond the covered age threshold may not be eligible for warranty coordination.*

© 2026 CJS Associates, LLC. Confidential.

1.4 MSP Managed Mobile User — 24x7

The *MSP Managed Mobile User* plan covers a single user whose primary work device is a company-owned mobile device, including tablets and smartphones. This plan is designed for team members who do their work away from a desk and anyone whose workflow lives on a mobile device.

Mobile Users receive 24x7 Help Desk Access, Managed ITDR, Managed ISPM, Multi-Factor Authentication, Email Threat Protection, Password Manager, and Microsoft 365 / Intune Management as define in the *MSP Managed User* plan (Section 1.1). The following services are specific to the mobile user's managed device:

- **Mobile Device Management (MDM):** The user's primary company-owned mobile device is enrolled, configured, and managed under CJS's *Mobile Device Management* platform. Security policies, including screen lock, encryption, and access controls, are applied and enforced at the device level. In the event of a lost or stolen device, CJS can remotely wipe company data.
- **Operating System (OS) and Application Updates:** Operating system and application updates and patches for the managed iOS or Android device are applied on a scheduled basis to keep your device secure and current.
- **Application Management:** Company-approved applications are managed and distributed to the managed device.

Note: *What is not included in the MSP Managed Mobile User plan: support for a managed workstation — a user who regularly works from a dedicated computer is covered under the MSP Managed User plan (Section 1.1); additional mobile devices beyond the primary device and personal devices (BYOD), both covered under Section 1.8; support for software outside the managed scope; and any service not listed above or in your Quote. See Section 5.5 — Exclusions for the full list.*

1.5 MSP Managed Workstation

The *MSP Managed Workstation* plan applies the same protection and management scope as the *MSP Managed User* plan to a single company-owned workstation. This model is used in environments where billing by device rather than by user better reflects the managed scope.

All services listed under Section 1.1 apply to each workstation covered under this plan, including 24x7 help desk access, RMM, patching, EDR, and workstation backup.

Note: *The MSP Managed Workstation and MSP Managed User plans are identical in service scope. The difference is billing structure — per device versus per user. Your Quote specifies which model applies to your account.*

© 2026 CJS Associates, LLC. Confidential.

1.6 Shared Workstation

The *Shared Workstation* plan covers a single company-owned device that is regularly used by more than one person — for example, a front desk terminal, a shared production workstation, or a kiosk. It provides the same full managed service scope as the *MSP Managed User*, with pricing that reflects the number of users sharing the device.

- **Service scope:** Full managed service coverage identical to the *MSP Managed User*, including 24x7 help desk access, RMM, patching, EDR, and all identity management for each associated user.
- **Base price:** The *Shared Workstation* base price covers management of the device itself. See your Quote for the applicable rate.
- **Covered users (1-10):** Employees who use the workstation and are already covered under a user plan (Sections 1.1 or 1.4) are fully served by their existing coverage. They do not add to the *Shared Workstation* price.
- **Attached users (1-10):** Employees who regularly use the workstation but are not covered under a user plan are billed as attached users, in the tiers reflected in your Quote. This provides help desk access and service for those individuals when working on the shared device.
- **More than 10 users:** Contact CJS to discuss pricing for workstations shared by more than ten users.

Note: *The number of users associated with a shared workstation is established during the discovery and onboarding process. If the number of regular users changes, please notify CJS so your agreement can be updated accordingly.*

1.7 Add-On: Second Machine

The *Second Machine Add-On* extends the same managed service coverage as the *MSP Managed User* plan to a second company-owned workstation assigned to the same user. This is typically used when a user has both an office workstation and a remote laptop. This add-on is required for every company-owned workstation used for company work. CJS cannot secure and support an environment where unmanaged company owned machines consistently access company systems and data.

All services listed under Section 1.1 apply to the second device. The device must be company-owned and assigned to the same user as the primary managed device.

This add-on applies to workstations only — desktops and laptops. Additional mobile devices are covered under the *Mobile Device Management* add-on under Section 1.8.

Note: *This add-on applies per user, not per device pool. A user with three company-owned devices would require two Second Machine add-ons.*

© 2026 CJS Associates, LLC. Confidential.

1.8 Add-On: Mobile Device Management (MDM)

Mobile Device Management is an add-on that extends managed security and policy enforcement to company mobile devices — smartphones and tablets.

- **Device enrollment and configuration:** Company mobile devices are enrolled and configured under CJS's *mobile device management* platform.
- **Security policy enforcement:** Screen lock requirements, encryption, and access controls are applied and enforced at the device level.
- **Remote wipe:** In the event of a lost or stolen device, CJS can remotely wipe company data from the enrolled device.
- **Application management:** Company-approved applications can be managed and distributed to enrolled devices.
- **Relationship to user plans:** A *Mobile User's* primary device is already managed under their user plan (Section 1.4) and does not require this add-on. MDM applies to mobile devices beyond a user's included primary device.

Note: *MDM applies to company-owned mobile devices. Personal devices (BYOD) may be enrolled at the client's request, subject to additional scoping. CJS manages company policy enforcement on enrolled devices — not personal device content. Where employees access company data from personal devices, CJS strongly recommends one of two protections: enrolling those devices in MDM with the employee's written consent, or establishing a company policy that prohibits company data from being stored on any personal, unmanaged device.*

© 2026 CJS Associates, LLC. Confidential.

2. MSP — Company Services

MSP — Company Services covers the infrastructure that your entire organization depends on. Where user services protect individual people and their devices, company services protect the systems that keep everyone connected and operational — your servers, your network, your internet presence, your data backups. A problem at the company level affects every person on your team, which is why these services are managed, monitored, and maintained as a foundation beneath everything else.

2.1 Remote Help Desk — Company-Wide Access

Every registered employee at your organization has access to the *CJS Remote Help Desk*. If anyone at your company needs IT assistance, they can reach us — and the help desk is always the right first call.

- **Coverage hours:** 24 hours a day, 7 days a week, 365 days a year including holidays for Tier 1 and Tier 2 support issues. There are no after-hours fees for standard help desk contact.
- **Help desk escalation:** When the help desk determines that a situation requires immediate senior engineering attention — such as an active security incident or critical system failure — they will escalate on your behalf at any hour. This process is handled by CJS and carries no additional charges.
- **Client-initiated escalation:** If you or your team contact CJS senior staff directly outside of standard business hours, this may be treated as an after-hours engagement and could incur additional charges depending on the nature of the request. Routing through the help desk first ensures your issue is triaged appropriately and avoids unnecessary charges.

> **Note:** *The remote help desk supports issues with covered, managed devices and services. Support for personal devices, software outside the managed scope, or issues caused by unauthorized changes to your environment is outside scope.*

2.2 Server Management

CJS manages your organization's servers under your managed service agreement. Server management includes remote monitoring, patch management, performance maintenance, server and security configuration, and escalated support. Four server types are supported:

2.2.1 Physical On-Premises Server

A physical server located at your place of business and managed remotely by CJS. CJS monitors health, applies patches and updates, manages server and security configuration, and responds to alerts.

2.2.2 On-Premises Virtual Server

A virtual server environment hosted on physical hardware at your location. CJS manages both the virtual machine layer and the underlying host, including patching, monitoring, configuration, and support.

2.2.3 Cloud-Hosted Virtual Server

A virtual server hosted in a cloud environment where CJS holds administrative control. CJS handles provisioning, monitoring, patching, and ongoing management. Cloud hosting costs are billed separately per your Quote.

© 2026 CJS Associates, LLC. Confidential.

2.2.4 Vendor-Managed Cloud-Hosted Server

A cloud-hosted server for line-of-business applications where administrative control is held by the software vendor, not CJS. CJS manages your organization's relationship with that server: supporting your users' access, coordinating with the vendor on your behalf, and serving as your technical advocate when issues arise.

Note: *The scope of CJS's role with a Vendor-Managed Cloud-Hosted Server differs from the other server types because administrative access to the server itself is held by the vendor. CJS cannot guarantee the same level of management as environments where we hold full administrative control. This service is included on your Quote where applicable.*

Note: *Server hardware repair or replacement is not included in the server management service. CJS will coordinate with hardware vendors on your behalf where applicable. See Section 5.5 for exclusions.*

2.3 Network Components

CJS manages the network infrastructure at your location as part of the *MSP — Company Services*. The components listed below are within managed scope when included in your Quote.

2.3.1 Firewall / Gateway Management

CJS manages your organization's firewall and network gateway. Our standard approach begins with managing the existing hardware in place at your location. As we assess your environment, we will recommend transitioning to CJS-preferred hardware where it will materially improve security, reliability, or financial efficiency.

Note: *CJS-preferred hardware represents our baseline service level and pricing. Managing client-supplied hardware of a different make or model may carry an adjusted rate to account for additional management complexity. When using non-CJS-preferred hardware, we cannot guarantee the same level of service quality as environments running CJS-standard equipment. Your Quote will specify which model applies.*

2.3.2 Managed Switches

Network switches within the managed environment are monitored and maintained by CJS, including configuration, firmware updates, and performance monitoring. Quotes differentiate between small and large switch configurations — your Quote specifies the applicable tier.

2.3.3 Wireless Access Points

Wireless access points within the managed environment are monitored and maintained by CJS, including configuration, firmware updates, and network segmentation where applicable.

2.3.4 Printer & Scanner Management

All printers used for company purposes at covered locations are included within managed scope. This covers networked printers, personal direct-connect printers, and shared multifunction printers (MFPs) used by your team on-premises. CJS monitors, configures, and maintains covered printers, including firmware updates and vendor escalation when required.

Note: *Printer management applies to all printers in use at covered business locations as noted on your quote.*

© 2026 CJS Associates, LLC. Confidential.

2.3.5 Smart Power / UPS

Proper power protection is a requirement for all managed environments. CJS requires the following minimum standards:

- **Servers and primary network equipment:** An Uninterruptible Power Supply (UPS) is required for all on-premises servers and primary network gear including switches and firewalls. A UPS provides battery backup power that keeps your equipment running during a power outage long enough to prevent data loss and allow for a safe shutdown.
- **All other managed hardware:** A surge protector is required at minimum for all other managed workstations and hardware at covered locations.

Note: *If your environment does not currently meet these power protection standards, CJS will include the appropriate equipment on your Quote. Power protection is a client-provided requirement — CJS will recommend and coordinate procurement but the equipment is owned and maintained by the client unless otherwise specified in a HaaS agreement.*

2.3.6 VPN

Virtual Private Network (VPN) configuration is supported by CJS on a case-by-case basis for environments that require secure site-to-site access — most commonly organizations that still rely on a physical on-premises server for data storage or line-of-business applications.

VPN is not CJS's recommended long-term solution. Cloud-based infrastructure eliminates the need for VPN in most scenarios while providing faster access, lower maintenance overhead, and stronger security. Where VPN is included in your managed environment, it will be specified in your Quote.

2.3.7 High Availability

High Availability refers to a network or infrastructure design where redundant systems are in place so that if a primary component fails — a server, a network connection, or a power source — a backup automatically takes over with minimal or no interruption to your business. Common examples include dual-WAN internet connections and redundant server configurations. CJS addresses *High Availability* needs on a case-by-case basis through *Professional Services*.

2.4 Network Security Management

CJS actively manages security at the network level, providing a layer of protection that complements device-level endpoint security (EDR) and identity security (ITDR). *Network Security Management* covers:

- **Firewall Rules Management:** Maintenance and enforcement of firewall rules that control what traffic is permitted into and out of your network.
- **Intrusion Detection & Prevention (IDS/IPS):** Active monitoring for and prevention of unauthorized access attempts and suspicious traffic patterns at the network level.
- **Content Filtering:** Restriction of access to websites, content categories, and specific applications that pose security risks or violate company policy.
- **Region / Location Filtering:** Blocking of network traffic originating from or destined for geographic regions associated with elevated security risk.
- **Virtual Local Area Network (VLAN) Management & Network Segmentation:** Separation of your network into distinct zones to isolate sensitive systems and reduce the risk of lateral movement if a security incident occurs.
- **Log Management:** Collection and retention of network event logs for monitoring, troubleshooting, and security review purposes.

© 2026 CJS Associates, LLC. Confidential.

2.5 CJS Internet Services & Security

CJS manages your organization's internet presence, connectivity, and email security infrastructure. This service is quoted as *CJS Internet Services and Security* and includes:

- **ISP Management:** CJS manages your relationship with your internet service provider, including troubleshooting connectivity issues, coordinating during outages, and serving as your advocate when ISP-side problems affect your business.
- **Domain Management:** Management of your organization's registered domains, including renewals, DNS record updates, and registrar coordination.
- **Public DNS Management:** Configuration and maintenance of your public DNS records to ensure your domain resolves correctly and securely.
- **Email and Web Host Management:** Management of your email hosting and web hosting environments, including coordination with hosting providers on your behalf.
- **Email Protection:** Configuration of the following email authentication and security standards to protect your domain from spoofing and phishing:
  - SPF (Sender Policy Framework) — identifies which mail servers are authorized to send email from your domain
  - DKIM (DomainKeys Identified Mail) — adds a digital signature to outgoing email to verify authenticity
  - DMARC (Domain-based Message Authentication, Reporting, and Conformance) — enforces authentication policies and provides reporting on email activity for your domain

Note: *CJS manages hosting relationships on your behalf — we do not operate proprietary CJS hosting infrastructure. Your hosting is provided through third-party providers. Third-party provider terms apply to the underlying services. "Internet presence" as defined in this section refers to your domain, DNS, and email infrastructure — it does not include website design, development, or content management*

2.6 Managed Backup & Disaster Recovery (MBDR)

CJS provides *Managed Backup and Disaster Recovery* for covered servers, workstations, and Microsoft 365 data. *MBDR* protects your organization's data and enables recovery in the event of hardware failure, data corruption, accidental deletion, or a security incident.

All *MBDR* services operate on a standard 90-day retention period. Data deleted or changed within the last 90 days can be recovered, subject to the backup schedule at the time of the incident. Extended service retention beyond 90 days is available at additional cost.

Note: *Backups run on a scheduled basis, which means there is always a window between the last completed backup and the present moment. Data created or modified after the last successful backup cannot be recovered through this service. CJS monitors backup jobs and will alert you to any failures, but cannot guarantee recovery of data that falls outside the completed backup window. This is an industry-standard characteristic of all scheduled backup solutions.*

2.6.1 MBDR — Servers

Managed backup and recovery for covered on-premises and cloud-hosted servers. Covers automated scheduled backups, monitoring of backup job completion with failure alerting, and recovery coordination in the event of data loss. Available for Physical On-Premises Servers, On-Premises Virtual Servers, Cloud-Hosted Virtual Servers, and Vendor-Managed Cloud-Hosted Servers where applicable.

© 2026 CJS Associates, LLC. Confidential.

2.6.2 MBDR — Workstations

Workstation backup is included as part of the *MSP Managed User* plan. CJS backs up data within the standard backup scope configured for your workstation, protecting it against accidental deletion, file corruption, and device failure. *See Section 1.2 for scope and retention details*.

CJS does not perform full system image backups of workstations. This is a deliberate design choice based on three practical realities:

- **Cost and performance:** A full system image captures everything on a device — the operating system, every installed application, all system files — generating significantly more data and higher storage costs. It also requires more time to run and can interfere with normal work during the backup window.
- **Cyber recovery:** In the event of a ransomware attack or other security incident, restoring a full system image could restore the compromised environment along with it. The correct response to a cyber incident is to rebuild the system clean — and then restore only the data. Backing up data rather than the full system means your recovery is both faster and safer.
- **What actually matters:** In the vast majority of recovery scenarios, what you need back is your files — not your operating system or application configurations, which CJS can reinstall quickly on any device.

In the event of complete device failure, CJS will configure a replacement device and restore your backed-up files. Getting back to work is straightforward — your data comes with you to the new machine.

CJS will also work with your team during onboarding and through regular business reviews to establish good data practices — ensuring your important files are consistently saved in a way that keeps them protected and recoverable.

2.6.3 MBDR — Microsoft 365 Tenant

Backup of your organization's Microsoft 365 environment, including all data within the M365 tenant. Covers:

- **Exchange Online:** All mailbox data including email, calendar, and contacts for covered users.
- **OneDrive for Business:** All files stored in each covered user's OneDrive.
- **SharePoint Online:** Site content and document libraries within your tenant.
- **Microsoft Teams:** Team channel content and associated files. Note: individual and group chat messages outside of team channels are not included in this backup. If preservation of direct message history is a requirement for your organization, contact CJS to discuss options.

> **Note:** *Recovery time for MBDR services depends on the volume of data, the type of recovery required, and the state of the environment at the time of the incident. CJS follows industry best practices (ITIL framework) to prioritize and execute recovery as efficiently as possible. CJS will consult with your organization to define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) appropriate to your business needs — contact us to discuss.*

© 2026 CJS Associates, LLC. Confidential.

2.7 IT Vendor Management

CJS manages your technology vendor relationships on your behalf as part of the MSP — Company service. When a vendor issue arises — whether with your internet provider, hardware manufacturer, software vendor, or any other IT-related third party — CJS acts as your point of contact and advocate.

- **General vendor management:** Coordination with ISPs, hardware manufacturers, software vendors, and any other IT service providers that support your business environment.
- **Line-of-business application vendors:** For organizations using cloud-hosted line-of-business applications managed by a third-party vendor, CJS can provide an additional level of managed vendor engagement — supporting your users' access to the application and coordinating with the vendor when technical issues arise. This is quoted as a company-level service where applicable.

Note: *IT Vendor Management is included as part of the CJS managed service relationship and is not a separate quoted line item for standard vendor coordination. Fees charged by third-party vendors for warranty service, OEM support, or similar work are passed through to the client at cost per the MSA.*

2.8 Security Operations Center (SOC)

CJS provides *Security Operations Center (SOC)* support as a standard component of the managed service. The *SOC* is the monitoring and response layer that operates behind your managed security tools — reviewing alerts, investigating anomalies, and escalating confirmed threats for remediation.

SOC support covers your entire managed environment at the company level, not individual users or devices in isolation. When a security event is detected — whether at the endpoint, identity, or network level — the *SOC* is the team that evaluates it and determines the appropriate response.

- **Alert monitoring and triage:** Security alerts generated across your managed environment are reviewed and prioritized by SOC analysts.
- **Threat investigation:** Suspicious activity is investigated to determine whether it represents a genuine threat or a false positive, reducing noise and ensuring your team is only contacted when action is genuinely required.
- **Escalation:** Confirmed threats are escalated for remediation through the appropriate channel — help desk, senior engineering, or direct client notification depending on severity.

Note: *SOC support operates on the data available from your managed security tools. The Managed SIEM add-on (Section 4.2) expands the scope of what the SOC can monitor by centralizing and correlating security event data across your entire environment. Organizations with elevated security requirements or compliance obligations may benefit from adding Managed SIEM to their plan.*

© 2026 CJS Associates, LLC. Confidential.

3. Microsoft 365 Licensing

CJS manages your Microsoft 365, Azure, and Entra licensing as a Microsoft Cloud Solution Provider (CSP). Microsoft licensing is billed as a variable line item connected to your user count and may change as users are added or removed.

3.1 Licensing Management

CJS handles the procurement, assignment, and ongoing administration of Microsoft 365 and related licenses for your organization, including:

- **License procurement and user assignment:** Licenses are purchased and assigned to the right people on your team.
- **License adjustments:** As your team grows or changes, CJS updates your licensing to match.
- **Microsoft Entra ID administration:** Management of your Microsoft identity and access environment.
- **Microsoft Intune tenant management:** Device enrollment and security policy management for your organization.
- **Microsoft coordination:** CJS works with Microsoft on licensing disputes, renewals, and technical escalations on your behalf.

3.2 Microsoft Licensing Models — NCE

Microsoft 365 licenses are governed by Microsoft's New Commerce Experience (NCE) licensing model. Three commitment structures are available:

Model	Commitment	Payment	Cancelable Mid-Term?
Annual / Annual	1 year	One annual payment	**No**
Annual / Monthly	1 year	Monthly payments	**No**
Monthly / Monthly	Month to month	Monthly payments	**Yes**

Note: *Only the Annual commitment models (Annual/Annual and Annual/Monthly) are non-cancelable once purchased. If you choose an annual commitment, you are responsible for the full license cost for the entire term regardless of the reason for termination. Adding users mid-term creates new licenses at the then-current rate for a new term. Removing users mid-term does not reduce fees for the current term.*

© 2026 CJS Associates, LLC. Confidential.

3.3 M365 Backup & Archive

CJS provides backup and archiving for your Microsoft 365 environment. *M365 Backup* covers two scopes — per user and tenant-wide — both operating on the standard 90-day retention period described in Section 2.6.

- **M365 User Backup:** Backup of each covered user's mailbox and OneDrive.
- **M365 Tenant Backup:** Backup of tenant-level data including SharePoint sites and shared resources.

> **Note:** *M365 Backup is a separate service from the workstation backup described in Sections 1.2 and 2.6.2. Tenant backup covers the full Microsoft 365 environment at the organizational level, not just the standard backup scope configured on individual user devices.*

3.4 Non-Microsoft Licensing

CJS manages non-Microsoft software and service licensing on behalf of clients where applicable. This includes procurement, renewal coordination, and license assignment for third-party business software included in your Quote. Specific terms for non-Microsoft licenses are governed by the respective provider and will be referenced in your Quote.

© 2026 CJS Associates, LLC. Confidential.

4. Optional Add-Ons

The services in this section are not included in a standard managed service plan. They are available as optional additions to your agreement and will appear in your Quote if applicable.

4.1 Voice Over IP (VoIP)

CJS provides *Voice Over IP (VoIP)* phone service as an optional add-on. *VoIP* replaces traditional phone lines with internet-based calling, enabling features such as call routing, voicemail-to-email, multi-location phone systems, and more. CJS coordinates *VoIP* provisioning, configuration, and ongoing management through a third-party *VoIP* provider.

> **Note:** *Important: VoIP services may affect the reliability of emergency 911 (E911) calls. See Section 6.4 — VoIP E911 Notice for the full disclosure and acknowledgment. CJS strongly recommends that all VoIP clients maintain at least one cellular device capable of independently dialing 911.*

4.2 Advanced Cybersecurity — Managed SIEM

Managed SIEM (Security Information and Event Management) is an optional add-on that expands the scope and depth of your organization's security monitoring. While standard managed services include endpoint, identity, and network-level security monitoring, *SIEM* centralizes and correlates security event data from across your entire environment — enabling the *SOC* to detect threats that individual tools operating independently may not catch.

Managed SIEM is a company-level service billed per device.

- **Centralized log collection:** Security event data from covered devices, servers, network components, and cloud services is aggregated into a single platform for unified analysis.
- **Correlation and threat detection:** *SIEM* analyzes patterns across data sources to identify threats that only become visible when events from multiple systems are examined together — such as a credential attack that touches identity, endpoint, and network simultaneously.
- **Enhanced SOC Visibility:** With *SIEM* in place, the SOC has a broader and more detailed view of your environment, enabling faster and more accurate threat identification.

> **Note:** *Managed SIEM builds on the SOC support included in your standard managed service plan (Section 2.8). It does not replace endpoint EDR, identity ITDR, ISPM, or ESPM — it complements them by adding a unified view across all security layers.*

4.3 Advanced Email Filtering

Advanced Email Filtering is an optional add-on for organizations experiencing excessive spam volume or recurring email-based security threats. It provides an additional layer of filtering and threat analysis beyond the standard email protection included in the *MSP Managed User* plan.

This service is recommended for environments where standard email protection is insufficient due to the nature of the organization's industry, public-facing exposure, or history of email-based incidents. Contact CJS to discuss whether advanced email filtering is appropriate for your environment.

© 2026 CJS Associates, LLC. Confidential.

4.4 Employee Security Awareness Training (ESAT)

Employee Security Awareness Training is a company-level add-on that provides ongoing cybersecurity education to your team. It helps reduce the risk of human-error security incidents — the most common cause of breaches — by training your employees to recognize and respond correctly to phishing, social engineering, and other threats.

- **Ongoing training:** Regular, automatically updated training modules delivered to your team on a scheduled basis.
- **Simulated phishing campaigns:** Controlled phishing simulations test your team's awareness and identify individuals who may need additional training.
- **Reporting:** CJS provides reports on your organization's training completion and simulated campaign results so you can track improvement over time.

4.5 Dark Web Monitoring

Dark Web Monitoring continuously scans dark web sources — underground forums, credential marketplaces, and breach databases — to identify whether your organization's credentials or sensitive data have been exposed. When a match is found, CJS is alerted and will notify you so that you can take action before the exposure causes further damage.

- **Coverage:** Monitoring for your organization's email domains, usernames, and credential data across dark web sources.
- **Alerting:** CJS receives alerts on your behalf and notifies you of any confirmed exposures with recommended remediation steps.

4.6 NIST Risk Assessment

CJS can perform a *NIST Cybersecurity Framework (CSF)* risk assessment for your organization. This assessment evaluates your current IT environment against the NIST CSF — a widely recognized standard organized around five functions: Identify, Protect, Detect, Respond, and Recover.

A *NIST Risk Assessment* produces a documented evaluation of your current security posture and a prioritized list of recommended improvements. This service is scoped and quoted on a per-engagement basis and is not part of a standard managed service plan.

> **Note:** *A NIST Risk Assessment documents your security posture at a point in time. It is not a guarantee of compliance with any regulatory framework. Per the MSA, CJS services are not intended as a full compliance solution unless expressly stated in your Quote.*

4.7 Privileged Access Management (PAM / PIM)

Privileged Access Management (PAM) — referred to as *Privileged Identity Management (PIM)* within the Microsoft environment — controls and monitors access to sensitive systems and administrative functions. *PAM* ensures that elevated permissions are granted only when needed, to authorized individuals, for a defined period of time.

This service is available as an optional add-on for organizations with elevated security requirements or compliance obligations. It is scoped and quoted on a per-engagement basis.

© 2026 CJS Associates, LLC. Confidential.

4.8 Penetration Testing / Vulnerability Assessment

A *Penetration Test (Pen Test)* is a controlled, authorized security assessment in which a qualified third party attempts to identify and exploit vulnerabilities in your environment before a malicious actor can. CJS coordinates *Penetration Testing* engagements through independent qualified third-party security specialists.

CJS's role in a *Penetration Testing* engagement includes:

- **Scoping:** Working with you and the testing vendor to define the scope, rules of engagement, and timeline for the assessment.
- **Authorization coordination:** Ensuring the test is properly authorized and that CJS-managed systems are not disrupted during the assessment.
- **Results review:** Reviewing findings with you and providing context and prioritized remediation recommendations.

Note: *CJS does not perform penetration tests directly. This service is coordinated through a vetted third-party security specialist. Costs for the testing vendor are in addition to CJS coordination fees and will be included in your Quote.*

4.9 Hardware as a Service (HaaS)

Hardware as a Service (HaaS) allows your organization to receive business-grade workstations and devices under a managed hardware model, rather than purchasing equipment outright. *HaaS* is typically introduced when a client is due for a hardware refresh or workstation upgrade.

- **Procurement and deployment:** CJS procures, configures, and deploys hardware appropriate to your environment.
- **Billing:** *HaaS* hardware is billed monthly as a separate line item on your MSP invoice — not as a separate invoice. The total cost of the hardware is divided across the term of the lease.
- **Warranty coordination:** CJS coordinates manufacturer warranty and repair services for *HaaS*-covered hardware.
- **End of term:** Hardware return terms at the end of a *HaaS* agreement are governed by the MSA and your Quote.

Note: *Hardware provided under a HaaS agreement remains CJS property. See your MSA for the full terms governing equipment return, damage, and early termination.*

4.10 Compliance Program

CJS can support your organization's compliance efforts as a project-based engagement. *Compliance Programs* are scoped based on the specific regulatory framework applicable to your business — such as HIPAA, SOC 2, or applicable state-level data privacy regulations.

A *Compliance Program* engagement typically includes an assessment of your environment against the applicable framework, identification of gaps, and a prioritized remediation roadmap. Remediation work is scoped and quoted separately.

Note: *Compliance programs support your compliance efforts but do not guarantee regulatory compliance or certification. Per the MSA, CJS services are not intended as a full compliance solution unless expressly stated in your Quote.*

© 2026 CJS Associates, LLC. Confidential.

4.11 Professional Services

Professional Services covers IT work that falls outside the scope of your standard managed service plan. This includes project work, one-time configurations, system migrations, technology implementations, and any other engagement scoped and quoted individually.

- **Per-project:** Scoped and quoted on a fixed or estimated basis for a defined deliverable.
- **Hourly:** Billed at the applicable CJS hourly rate for work performed. Refer to your Quote for the applicable rate.

Note: *Professional Services are performed during standard business hours (Monday through Friday, 8:00 AM to 5:00 PM PT) unless otherwise agreed. Work performed outside standard hours is billed at the applicable after-hours rate. See Section 5.1 for coverage hours and rate guidance and Section 6.1 for After-Hours coverage.*

© 2026 CJS Associates, LLC. Confidential.

5. Service Standards

5.1 Coverage Hours

Coverage Type	Hours
Help Desk — Tier 1 & 2	24 hours a day, 7 days a week, 365 days a year including all holidays
Escalated / Senior Engineering	Monday through Friday, 8:00 AM to 5:00 PM PT, excluding CJS-observed holidays
After-Hours & Not-Covered Emergency Support	Available by request. After-hours work is billed at the applicable rate. Refer to your Quote for current rates.
Scheduled Maintenance	Performed outside standard business hours unless otherwise authorized. Minimum 24-hour advance notice provided.

5.2 Response Times

CJS responds to support requests based on the priority level of the issue. A response means an acknowledgment that your issue has been received and is being evaluated — not that the issue has been resolved. Resolution time depends on the nature of the issue and cannot be guaranteed within a fixed timeframe.

Response time targets follow ITIL best practices and represent CJS's standard operating commitments on a best-effort basis. They are not binding SLAs.

Priority	Definition	Target Response	How to Reach Us
Critical	Complete outage or active security incident affecting the entire organization or a critical system	Within 1 hour	Phone / Help Desk
High	Significant issue affecting multiple users or a key business function — work cannot continue as normal	Within 2 hours	Phone / Help Desk
Medium	Issue affecting a single user or non-critical system — a workaround is available	Within 4 business hours	Help Desk / Email
Low	General question, minor issue, or scheduled request with no immediate business impact	Within 1 business day	Help Desk / Email

Note: *New service onboarding: For the first 60 days following the start of any new service, and during any service transition or off-boarding period, response time targets do not apply. These periods involve significant environment changes and unexpected delays may occur. This exception is defined in your MSA.*

© 2026 CJS Associates, LLC. Confidential.

5.3 On-Site Support

On-site support is available for issues that cannot be resolved remotely. CJS technicians will come to your location when on-site access is needed to resolve a problem.

- **Within 50 miles of CJS offices:** On-site labor is included within the standard managed service — no additional travel fee applies.
- **Beyond 50 miles:** Travel beyond 50 miles is billed at cost. CJS will notify you before incurring travel expenses.
- **After-hours on-site:** On-site support performed outside standard business hours (M–F, 8:00 AM – 5:00 PM PT) is billed at the applicable after-hours rate. Refer to your Quote for current rates.

5.4 Minimum Requirements

To receive managed services from CJS, your environment must meet the following minimum requirements. CJS reserves the right to exclude from coverage any device or component that does not meet these requirements.

- **Device age:** Covered workstations and servers must be no more than 3 years old at the time of enrollment. CJS may, at its discretion, cover devices up to 5 years old on a case-by-case basis. Devices older than the applicable threshold may be designated as end-of-life and excluded from managed coverage.
- **Operating system:** All covered devices must run a currently supported version of their operating system with vendor security updates available. End-of-life operating systems are excluded from managed coverage.
- **Software licensing:** All software in the managed environment must be genuine and properly licensed. Unlicensed software must be remediated before managed services can begin.
- **Physical environment:** Covered equipment must be maintained in a suitable physical environment including temperature control, protection from moisture, and physical security measures as required by your MSA.
- **Power protection:** All on-premises servers and primary network equipment must be protected by a UPS. All other managed hardware must be protected by a surge protector at minimum. *See Section 2.3.5.*

5.5 Exclusions — What Is Not Covered

The following are explicitly outside the scope of CJS managed services unless expressly listed in your Quote:

- Support for personal devices (BYOD) not enrolled in *MDM*
- Support for software outside the managed service scope
- Recovery from a cybersecurity breach or data loss event — this is a separate engagement, investigated and quoted individually
- Remediation of issues caused by unauthorized modifications to the managed environment
- Services required to bring a non-compliant environment up to Minimum Requirements
- Any service not listed in your Quote
- Work performed while your account has unpaid, undisputed balances

> **Note:** *CJS strongly recommends that all clients carry cyber liability insurance. Even in a best-practice managed environment, security incidents can occur. Insurance provides financial protection that managed services alone cannot guarantee.*

© 2026 CJS Associates, LLC. Confidential.

5.6 Third-Party Scanning and Testing

Clients may not authorize or conduct third-party security scans, vulnerability assessments, or penetration tests against any portion of the managed environment without prior written authorization from CJS. Unauthorized scans can disrupt managed services, trigger false incident alerts, and interfere with monitoring systems.

If you wish to have your environment assessed by a third party, contact CJS in advance. We will coordinate with the testing party to ensure the assessment is conducted safely and without disruption to your managed services. *See Section 4.8* for CJS-coordinated penetration testing.

5.7 Hardware and Software Obsolescence

CJS may designate any hardware or software as end-of-life (obsolete) when the manufacturer or vendor no longer provides security updates or support. Obsolete devices and software represent a security and operational risk that CJS cannot effectively manage within a standard managed service agreement.

When a device or software application is designated as end-of-life, CJS will notify you and provide a recommendation for replacement or upgrade. The affected device or software may be removed from managed coverage until remediated. CJS is not responsible for issues arising from continued use of end-of-life hardware or software.

5.8 Appropriate Use — Help Desk

Help desk access is provided for legitimate business IT support needs related to covered devices and services. Appropriate use means requests are related to covered devices and services, are made by or on behalf of covered users, and reflect genuine operational needs.

CJS reserves the right to address patterns of use that place a disproportionate burden on help desk resources. In these situations, CJS will work with you to identify and resolve the underlying cause before taking any further action.

© 2026 CJS Associates, LLC. Confidential.

6. Additional Terms

6.1 After-Hours Support

Non-Help Desk after-hours support is available outside of standard business hours (Monday through Friday, 8:00 AM to 5:00 PM PT) by request. After-hours work is billed at a rate above the standard hourly rate, with a minimum billing increment per engagement. Holiday support is billed at a separate holiday rate.

Note: *Current after-hours and holiday support rates are listed in your Quote. Rates are subject to change at the time of contract renewal per the annual adjustment terms in Section 6.5.*

6.2 New and Replacement Workstation Setup

Setup, configuration, and deployment of new or replacement workstations is billed at a flat rate per machine. This includes imaging, software installation, security configuration, and enrollment in the managed service platform. The flat setup rate also includes standard delivery within 50 miles of CJS offices. Delivery beyond 50 miles is billed at cost.

Note: *The flat workstation setup rate is listed in your Quote. After-hours or expedited deployment is available at the applicable after-hours rate.*

6.3 Contract Renewal

Your service term is stated in your Quote. Renewal is a conversation CJS initiates, not a deadline you are responsible for tracking. CJS will contact you in writing before the end of your current term to schedule a renewal review, covering your scope, user counts, rates, and anything that has changed in your environment. If your Quote states renewal terms specific to your account, those terms apply.

- **Starting a new term:** A new Quote is what changes your agreement. Any change to your term length, scope, plan structure, or line items takes effect only upon signature and acceptance of a new Quote.
- **Continued coverage:** If renewal is not concluded by the end of your term, your coverage continues as your Quote describes for two months following the end of your term.
- **Ending service during continued coverage:** During those two months, either party may end services with 30 days' written notice. Because your term has already expired, no early termination fee applies. All other aspects of ending service, including your obligations at the end of service and any transition assistance, are governed by your MSA.
- **After two months:** If renewal has still not been concluded, CJS will notify you in writing of one of the following: your coverage continues month to month at your then-current rates until a renewal is concluded; your agreement continues for a 12-month term on your existing line items, with any annual rate adjustment included in your renewal notice applied, per *Section 6.5*; or, where CJS has attempted to schedule a renewal review at least three times over a period of no fewer than 30 days without a review being scheduled, CJS ends coverage with 30 days' written notice. A continuation under this section is always 12 months, regardless of the length of your previous term, and does not change your scope, plan structure, or line items. A new term of any other length requires your signature.

© 2026 CJS Associates, LLC. Confidential.

Except as described above, termination is governed by your MSA, including any termination fee that applies to ending services before the natural expiration of your term.

Note: *Amendments are governed by the Amendment provision in Section X of your MSA. An amendment must be provided to you in writing, must identify the document being amended, and takes effect only when both parties affirmatively accept it in writing. Email or electronic signature is sufficient. CJS cannot amend your agreement without your acceptance.*

6.4 VoIP — E911 Notice and Acknowledgment

VoIP phone services operate differently from traditional telephone lines. Before activating *VoIP* service, you must understand and acknowledge the following:

- **E911 location:** *VoIP* E911 calls may not automatically transmit your physical location to the emergency dispatcher. You are responsible for registering your service address with your *VoIP* provider and keeping that address current if your location changes.
- **Power and internet dependency:** *VoIP* service — including the ability to dial 911 — may be unavailable during a power outage or internet outage. Traditional phone lines and cellular devices are not affected by these outages.
- **Your responsibility:** CJS recommends that all *VoIP* clients maintain at least one cellular device capable of independently dialing 911.
- **Acknowledgment:** By activating *VoIP* service through CJS, you acknowledge these limitations and agree that CJS is not liable for any inability to complete an emergency call through the *VoIP* service.

6.5 Annual Rate Adjustments

CJS may adjust managed service rates at the time of contract renewal. Annual rate adjustments will not exceed 7% above the prior year's rate. You will be notified of any planned rate adjustment prior to the renewal date.

Rate adjustments resulting from third-party vendor price increases — referred to as Pass-Through Increases in your MSA — are not subject to the 7% cap and may occur outside of the annual renewal cycle. CJS will provide as much advance notice as reasonably possible when a pass-through increase applies.

6.6 Microsoft NCE Licensing Terms

By accepting a Quote that includes Microsoft 365 licensing, you agree to the following terms governing Microsoft's New Commerce Experience (NCE) licensing model:

- Per-seat licenses under annual commitment models cannot be canceled once purchased and cannot be transferred to another customer.
- Licenses require a definite term — monthly or annual — and must be paid in full for the entire term regardless of the reason for termination of managed services.
- If you transition to a different managed service provider, licenses under annual commitments may continue to be used until expiration, provided they are paid in full.
- Adding users mid-term results in new per-seat licenses at the then-current rate for a new term.
- Removing users mid-term does not reduce fees for the current term.

© 2026 CJS Associates, LLC. Confidential.

6.7 HaaS — Equipment Return

Upon termination of a *HaaS* agreement for any reason, you are required to return all CJS-provided hardware within 10 days. Hardware must be returned in the same condition as delivered, normal wear and tear excepted.

CJS will coordinate the return process and provide instructions for scheduling pickup or drop-off. Hardware that is not returned within 10 days, or that is returned in a damaged condition beyond normal wear and tear, will be invoiced at full replacement value.

Note: *Full equipment return terms — including rights of access to retrieve equipment — are governed by your MSA.*

6.8 IT — Acceptable Use

CJS manages your email hosting and security on your behalf. CJS recommends that all clients maintain a written Acceptable Use Policy governing how email and company data may be used by employees. A written policy protects your organization and sets clear expectations for your team.

As a condition of CJS managing your email environment, your organization agrees that company email will not be used for transmitting spam, malware, phishing content, or communications that violate applicable law or your email hosting provider's terms of service. Violations that affect the managed email environment may result in suspension of email services.

© 2026 CJS Associates, LLC. Confidential.

7. Glossary

The following definitions apply to terms used in this Services Guide and in your Quote. If a term appears in your Quote that is not defined here, contact CJS for clarification.

Term	Plain-Language Definition
BDR / MBDR	Backup and Disaster Recovery. A managed service that backs up your data on a schedule and enables recovery if that data is lost, corrupted, or encrypted by ransomware.
Dark Web	A part of the internet not indexed by standard search engines, accessible only through specialized software. It is frequently used by cybercriminals to buy and sell stolen credentials and data.
Dark Web Monitoring	A service that continuously scans dark web forums and credential databases for your organization's usernames, passwords, or other sensitive data that may have been exposed in a breach.
DKIM	DomainKeys Identified Mail. A digital signature added to your outgoing email that allows the receiving mail server to verify the message genuinely came from your domain — and has not been tampered with in transit.
DMARC	Domain-based Message Authentication, Reporting, and Conformance. A policy that tells receiving mail servers what to do with email that fails authentication checks, and provides reporting back to you on email activity for your domain.
EDR	Endpoint Detection and Response. Security software running on your computer that monitors in real time for malicious activity — viruses, ransomware, malware — and responds automatically to contain threats.
ESPM	Endpoint Security Posture Management. Continuous monitoring of how well your devices are configured for security, checking for gaps, misconfigurations, or policy violations across all managed endpoints.
Firewall / Gateway	A device or service that sits between your internal network and the internet, controlling what traffic is permitted in and out. Think of it as the front door and security checkpoint for your network.
HaaS	*Hardware as a Service*. A model where CJS provides business hardware — typically workstations — under a recurring billing arrangement rather than a one-time purchase.
High Availability (HA)	A network or infrastructure design where redundant systems are in place so that if a primary component fails — a server, a network connection — a backup automatically takes over with minimal or no interruption to your business. Common examples include dual-WAN internet connections.
IDS / IPS	Intrusion Detection System / Intrusion Prevention System. Security tools that monitor your network for suspicious activity or known attack patterns. IDS detects and alerts; IPS actively blocks the threat.
ISPM	Identity Security Posture Management. Continuous monitoring of how user identities and access permissions are configured — identifying accounts with excessive access, weak policies, or signs of compromise.

© 2026 CJS Associates, LLC. Confidential.

Term	Plain-Language Definition
ITDR	Identity Threat Detection and Response. Monitors your Microsoft 365 user accounts for signs of unauthorized access or credential-based attacks, such as suspicious login locations or unusual account activity.
ITIL	Information Technology Infrastructure Library. A widely adopted framework of best practices for IT service management. CJS uses ITIL principles as the basis for how we prioritize and respond to support requests.
MDM	*Mobile Device Management*. Software that allows CJS to manage and enforce security policies on mobile devices — smartphones and tablets — remotely
MFA	Multi-Factor Authentication. A security requirement that verifies your identity using two or more methods — typically your password plus a code sent to your phone — before granting access to an account.
NCE	New Commerce Experience. Microsoft's current licensing model for Microsoft 365 and related products. Licenses under annual NCE commitments are non-cancelable once purchased.
NIST CSF	NIST Cybersecurity Framework. A voluntary framework developed by the National Institute of Standards and Technology that provides guidance for managing cybersecurity risk, organized around five functions: Identify, Protect, Detect, Respond, Recover.
PAM / PIM	*Privileged Access Management* / Privileged Identity Management. Controls that limit and monitor who has administrative access to critical systems, ensuring elevated permissions are used only when necessary, by authorized people, for a defined time.
RMM	Remote Monitoring and Management. The platform CJS uses to monitor the health of your devices, servers, and network, and to perform maintenance and management tasks remotely — often resolving issues before you notice them.
RPO	Recovery Point Objective. The maximum acceptable amount of data loss measured in time. For example, a 90-day RPO means data from the last 90 days can be recovered. CJS establishes RPOs collaboratively with each client based on their business needs.
RTO	Recovery Time Objective. The target time within which systems or services should be restored after an outage. CJS establishes RTOs collaboratively with each client based on their business needs and environment.
SIEM	Security Information and Event Management. A system that collects and analyzes security-related data from across your environment — devices, servers, network — to detect threats that individual tools might miss.
SOC	Security Operations Center. A team of security analysts who monitor alerts from *SIEM* and other tools, investigate potential threats, and escalate confirmed incidents for response.
SPF	Sender Policy Framework. An email authentication method that identifies which mail servers are authorized to send email on behalf of your domain, helping prevent spoofing.
UPS	Uninterruptible Power Supply. A battery backup device that keeps your equipment running during a power outage long enough to save work and shut down safely — protecting against data loss and hardware damage from sudden power loss.

© 2026 CJS Associates, LLC. Confidential.

Term	Plain-Language Definition
VLAN	Virtual Local Area Network. A way of dividing a physical network into separate logical segments. VLANs allow CJS to isolate sensitive systems — such as servers or security cameras — from general office traffic, reducing risk if one segment is compromised.
VoIP	Voice Over Internet Protocol. A phone system that routes calls through your internet connection rather than traditional phone lines, enabling features like call routing, voicemail-to-email, and multi-location phone systems.
VPN	Virtual Private Network. An encrypted connection between a device and your business network — used to allow remote employees to securely access company resources as if they were working in the office.

Pricing Reference — For Quote Template

The following items are referenced in this Services Guide as 'see your Quote for current rates.' Check your quote for specific rates including:

- Standard hourly rate
- Architecture / senior engineering hourly rate
- After-hours support rate and minimum billing increment
- Holiday support rate
- Flat workstation setup fee (per machine, including delivery within 50 miles)
- Shared Workstation base rate
- Shared Workstation per-user add-on rate
- Second Machine add-on rate
- HaaS hardware rates
- MBDR rates (server, workstation, M365 tenant)
- After-hours on-site travel policy (beyond 50 miles)

cjsassociates℠
IT Solutions for the Office and Cloud

© 2026 CJS Associates, LLC | IT Solutions for the Office and Cloud
This document is confidential and intended for use by CJS Associates clients only.