

# Diamond Managed-IT Master Service Agreement

---

## Master Service Agreement

1. **Master Service Agreement:** This Master Service Agreement (“MSA”) is in conjunction with the **TERMS AND CONDITIONS FOR ALL CNS SERVICES AND PRODUCTS** “Terms”, located at <https://www.cns-service.com/agreement/>. This MSA does not replace the Terms but incorporates all the provisions and obligations set forth in the Terms. Capital Network Solutions, Inc. provides the Services described below to the standards stated in the Terms. The date for this MSA when electronically signed and accepted is the (“MSA Effective Date”) supplements the Terms and Conditions (the “Terms”) by and between Capital Network Solutions, Inc. (“CNS”) and (“Client”). This MSA consists of the terms below, the signature page, and any unique attachments to this MSA, which are all incorporated into the Terms by this reference and are made a part of the Terms by all intents and purposes. Requested Services will be provided and limited as indicated on the signed quotation. Further service offerings may only be secured via subsequent Statement of Work.
2. **Term Commitment:** The initial term of this MSA is **One-year** from the MSA Effective Date.
  - a) **Automatic One-year Renewal:** This MSA will automatically renew for another one-year term extending the Effective Date on each annual renewal. Client will receive the services included in the most current Diamond Managed IT Master Service Agreement as updated.
  - b) **Election Not to Renew:** Either party may elect not to renew this Agreement by providing written notice to the other party at least 30 days before the end of each one-year term. Client may terminate this MSA or elect to be on a month-to-month plan. Client must provide written notice at least 30 days to terminate or change to a month-to-month agreement.

## Managed IT Support Services

3. **Managed IT Setup:** For new clients, there is a one-time setup fee of **\$1,000.00**. The duration of the onboarding process can vary based on your organizational size and needs. This Managed IT Setup includes the following:
  - a) **IT Security Assessment and Environment Documentation**
    - i) Gather information and create documentation on the Client portal.
    - ii) Conduct cyber security risk assessment and Dark Web password scan.
    - iii) Present findings, recommendations, and billable scope of work for any remediations needed to meet the CNS IT Standards, as defined in this MSA section 16.
  - b) **Managed IT Deployment**
    - i) Install remote management software, antivirus and End Point Detection and Response.
    - ii) Setup and configure of CNS managed backup and firewall.
    - iii) Deploy advanced security solutions:
      - (1) Real-time email threat protection
      - (2) Configure multi-factor authentication for all users
      - (3) Endpoint encryption on laptops and manage keys
      - (4) Mobile device and application management
      - (5) Document IT Security policies

4. **Virtual Chief Information Officer (“vCIO”) Consultant:** The vCIO is responsible for developing an overall technology strategy, setting standards for computer operations, and for ensuring the computer and network infrastructure meets the organization’s needs. An annual meeting will be held working with the executive team on the organization’s long-term planning, with a specific focus on identifying opportunities, as well as designing and implementing the technology required to achieve these long-term goals.
5. **Diamond Support Overview:** This plan provides on-demand support services for a flat monthly fee. Client’s employees get direct access to the CNS Service Desk.
- a) **Service Desk Summary:** Our Service Desk provides technical assistance and support for incoming queries and issues related to computer systems, software, and hardware. The Service Desk is the first contact for all Client service requests. CNS will work remotely to troubleshoot problems, identify root causes, and resolve issues while staying within our Service Level Agreement. If necessary, CNS will act on Client’s behalf to work with technology vendors to resolve problems.
- b) **Support:** The following outlines the types of issues that the Service Desk will work to resolve:
- i) Workstation hardware issues and slowness
  - ii) Application Issues
  - iii) Network or Internet Service issues
  - iv) Application dot release updates and patching
    - (1) Excludes major version upgrades for line of business applications.
  - v) Installation of peripherals
    - (1) Includes desktop printers, desktop scanners, keyboards, mouse, monitors, external drives and other USB devices.
- c) **Onsite Support:** If the Service Desk is unable to resolve an issue remotely, CNS will provide onsite support. This onsite service is included within the Diamond Plan at no extra charge for corporate offices located within a 60-mile radius from the CNS Office (8950 Cal Center Drive, Sacramento, CA 95826). Any travel outside of this 60-mile radius will be billed hourly at 50% of Client’s billable service rate. In certain instances, a local subcontracted resource may be retained for onsite technical support.
- d) **Support Hours:** We offer support during and after business hours.
- i) Standard Support is available via email request or phone call: Monday through Friday, 7:00 a.m. to 5:00 p.m. (PST).
  - ii) After-hours Emergency Support is only available via phone call: Weekdays, 5:01 p.m. to 6:59 a.m. (PST); Weekends, 24 hours a day.
- e) **Service Level Agreement (“SLA”) and Agreement Response Times:** Every phone call, email and voicemail request received by the Service Desk will be entered into the CNS service ticketing system and assigned a priority. The table below summarizes our SLA. Urgency and impact determine the priority level, which dictates the time of response and resolution target. Response time is measured from ticket submittal until the appropriate assigned tech first replies. The auto-generated confirmation email sent to the requester does not fulfill the response time requirement. Resolution time is measured from ticket submittal until the issue is resolved.
- i) **Dispatch:** Problems are addressed remotely first. Engineers will be dispatched only if remote remediation is not possible. Time to dispatch a resource for onsite service is based on the ticket’s priority level. Actual onsite arrival times will vary for local and remote locations.
  - ii) **After-Hours:** All after-hour support requests are assumed to be a priority 1 or priority 2 issue. Calls received after-hours that are determined to be priority 3 or priority 4 will be logged into our ticketing system and addressed on the next business day.

### iii) SLA Response Timetable

Priority	Response Time	Target Resolution Time	Definitions
<b>Priority 1 "Critical"</b>	Within 1 hour of initial contact	As quickly as possible; issue worked on continuously until resolution reached; Client provided with hourly updates.	A mission-critical system down with no workaround available; affects the entire organization.
<b>Priority 2 "High"</b>	Within 2 hours of initial contact	Within 4 hours; issue worked on continuously until resolution reached; Client provided with hourly updates.	A mission-critical system down or unavailable, but with an available workaround or partial system functionality; key business personnel impacted.
<b>Priority 3 "Normal"</b>	Within 4 business hours of initial contact	Within 1 business day of initial contact	A task, service or individual impacted, with no workaround available; an important issue that does not have significant impact on productivity.
<b>Priority 4 "Low"</b>	Within 8 business hours of initial contact	Within 4 business days of initial contact	A task, service, or individual impacted, but with little or no impact on productivity.

## Management and Maintenance

The Diamond Managed IT Master Service Agreement includes a set of management and maintenance services that are included for no extra charge.

**6. System Management:** System Management includes all Server Hosts, Operating Systems, and Network Equipment. Proper maintenance and monitoring should not be neglected as it offers the best protection against preventable failures and potential security flaws. CNS maintains a technician for critical after-hours events, monitoring Client infrastructure 24 hours a day, 7 days a week. Should a problem occur in the middle of the night, Clients have the choice of being contacted immediately by CNS or waiting until the next business day to initiate a resolution.

#### a) **Deployment**

- i) Installation of new computers (desktops/laptops/virtual desktop machines)
- ii) Adding new employees to local Windows Servers and Microsoft 365.
- iii) Reassigning physical or virtual desktop computers for existing and/or new users.

#### b) **System Administration**

- i) Changes to existing user accounts and email.
- ii) Changes to Microsoft 365 subscriptions.
- iii) Security settings and privileges.

#### c) **Application Updates**

- i) Microsoft Office and Edge
- ii) VMware ESXi
- iii) Microsoft HyperV
- iv) Adobe Acrobat and Flash Plugin
- v) Google Chrome
- vi) Oracle Java

**d) Troubleshooting system related problems**

- i) 24x7 alert remediation for server hardware and machines.
  - (1) 24x7 critical alert monitoring.
  - (2) After-hours remediation of all critical alerts.
- ii) Customization of monitoring and alerting configurations (as requested)
- iii) Coordinate and assist with warranty repairs
- iv) Configuration documentation
- v) Network equipment firmware updates
  - vi) Regular backup of all network Equipment Configuration Files
- vii) Email Maintenance, Email Address and Alias Creation
- viii) Spam Management, Blacklisting and Whitelisting Domains

**7. Workstation Management:** CNS provides support and maintenance services for all company-owned desktops and laptops. Our solutions help by optimizing desktop infrastructure, improving end-user productivity, and protecting corporate assets. These support and maintenance services include:

- a) Warranty Repair Coordination and Assistance
- b) Up to-Date Configuration Documentation
- c) Anti-Virus and Malware Management
- d) Software Upgrades
  - i) Operating System service packs and feature packs.
  - ii) Standard line-of-business application updates (excludes major versioning updates).
- e) Windows Patch Management
  - i) Management of all Windows system patching.
  - ii) Weekly remediation of patch issues and application of missing patches.

**8. Security:** The Diamond Managed IT Security Services Agreement provides advanced control and protection of company data and mobile devices. For companies that must meet state or federal regulatory guidelines, CNS also offers add-on services for compliance and IT audits. The following outlines the services that are included in the Diamond plan:

- a) Annual Cyber Security Risk Assessment
- b) Annual Dark Web Password Scan
- c) Anti-Virus and Malware Protection
- d) End Point Detection and Response
- e) Firewall management
- f) National Institute of Standards and Technology (NIST) system hardening
  - i) Firewalls
  - ii) Email
  - iii) Servers

- iv) Applications
- v) Access Control
- vi) Data Loss Prevention
- vii) Windows Security Updates
- viii) Multi-Factor Authentication
- ix) Vulnerability Scan
- x) Security Awareness Training
- xi) Real-Time Email Threat Protection
- xii) Device Encryption
- xiii) Email Encryption
- xiv) Mobile Device and Application Management
- xv) Exchange Online Archiving
- xvi) IT Security Policies

**9. Add-On: Managed SOC (Security Operations Center):** For an additional monthly charge CNS offers customers a Security Operations Center as a Service. Customers with sensitive information or have the need to meet state or local government regulatory and/or Insurance regulations by retaining all event logs. CNS offers a Managed SOC service at an additional monthly charge per device. CNS will review and remediate issues detected by a 24/7 cyber security service. This provides a threat monitoring platform detecting malicious and suspicious activity across endpoints, network, and cloud platforms. Services include:

- a) Device based billing includes all workstations, laptops, and firewall appliances.
- b) 24/7 Threat monitoring and analysis
  - i) Endpoint - Windows & macOS event log monitoring, breach detection, malicious files and processes, threat hunting, intrusion detection, 3rd party NGAV integrations
  - ii) Network - Firewall and edge device log monitoring integrated with threat reputation, who-is and DNS information.
  - iii) Cloud - Microsoft 365 security event log monitoring, Azure AD monitoring, Microsoft 365 malicious logins, Secure Score.
- c) Log Monitoring - Monitor, search, alert and report on the 3 attack pillars: network, cloud and endpoint log data spanning
- d) Real-Time Investigation and Threat Hunting
  - i) Intrusion Monitoring
  - ii) Threat Isolation and Remediation
  - iii) Incident Response and Notifications
- e) Log retention
  - i) 30 Days - Online Log Data Access
  - ii) 1 Year - Archived Log Retention

**10. Data Protection:** CNS protects data in several platforms that includes Microsoft 365 data, on-premises servers, and Azure cloud machines. The following outlines what is included within our backup maintenance and recovery points.

- a) **Microsoft 365:** CNS utilizes the Barracuda Cloud to Cloud backup service to protect email and other data hosted in Microsoft 365. Workstation and laptop system backups are not included or managed. Only the File Library on such devices is protected by Microsoft OneDrive and the Barracuda Cloud to Cloud backup. Data is protected with in Microsoft 365 Exchange Email, OneDrive, SharePoint and Team Sites. Barracuda Cloud Backups are also stored in Azure across multiple zones with granular recovery points. The following

schedule and retention are configured.

- i) Maintenance includes
  - (1) Backup Alert Monitoring and Remediation
  - (2) Data Restorations
- ii) Backup Schedule
  - (1) Frequency: 1 daily backup
  - (2) Recovery Points
    - (a) Keep All Revisions: forever
    - (b) Keep Daily Revisions: forever
    - (c) Keep Weekly Revisions: forever
    - (d) Keep Monthly Revisions: forever
    - (e) Keep Yearly Revisions: forever

b) **Add-On: On Premise Server Backup:** For an additional monthly charge CNS utilizes a server backup appliance from Barracuda to manage data protection for Clients on-premise servers. The appliance will backup and keep a local copy of the Client's data, as well as replicate data to the Barracuda Cloud hosted in Microsoft Azure's cloud. CNS will configure a Server O/S agent-based backup solution for a rapid restore of individual files and databases. Plus, an image-based backup of the Windows Server will also be used to have a rapid recovery of such Windows Server machines and/or the entire server hardware host. Both are required to provide a reasonable recovery time in the event of an outage.

- i) Maintenance includes
  - (1) Creation of a custom backup schedule and/or snap shots
  - (2) Backup Alert Monitoring and Remediation
  - (3) Data Restorations
  - (4) Flat File, Folder and Drive Restorations
  - (5) Virtual Machine and Host Restorations
- ii) Backup Schedule
  - (1) Backup Frequency: 1 to 3 daily backups
  - (2) Recovery Points
    - (a) Keep Daily Revisions: 7 days
    - (b) Keep Weekly Revisions: 4 weeks
    - (c) Keep Monthly Revisions: 12 months
    - (d) Keep Yearly Revisions: 7 years
  - (3) Offsite Replication: Every 24 Hours

c) **Microsoft Azure:** Any workloads hosted in Microsoft Azure cloud is protected by the configured backup snap shots within that cloud platform. The following standard recovery and retention will be configured and managed.

- i) Maintenance includes
  - (1) Creation of a custom backup schedule and/or snap shots
  - (2) Backup Alert Monitoring and Remediation
  - (3) Data Restorations
  - (4) Flat File, Folder and Drive Restorations
  - (5) Virtual Machine
- ii) Backup Schedule
  - (1) Backup Frequency: 1 daily backup
  - (2) Recovery Points

- (a) Keep Daily Revisions: 7 days
- (b) Keep Weekly Revisions: 4 weeks
- (c) Keep Monthly Revisions: 12 months
- (d) Keep Yearly Revisions: 7 years

## Billable Services and Exclusions

- 11. Hourly Rate Charges:** CNS charges an hourly rate for requested services not covered under the Diamond Managed IT Service Agreement. Estimates of hours and pricing will be provided to the Client's designated personnel via a work authorization or project scope of work before the engagement of billable services.
- a) **Tier-3 and Professional Services Billable Time.** CNS charges **\$160.00 per hour** for the following work, but not limited to:
- i) **Remote Onsite support:** CNS includes in this MSA at no additional cost onsite services for locations within a 60-mile radius from the CNS Office. Client will be billed for onsite services outside the radius. In certain instances, a local subcontracted resource may be retained for onsite technical support.
  - ii) **Installation or re-locating**
    - (1) New Server and storage hardware.
    - (2) New Microsoft Windows Server machines on-premises or Microsoft Azure cloud.
    - (3) Networking appliances, switches, Firewalls and wireless access points.
    - (4) Unforeseen global changes to multiple locations.
    - (5) Microsoft Teams Phones and/or 3<sup>rd</sup> party phone systems, software clients and handsets.
- 12. Service Exclusions:** CNS does not provide the following services but does have partnerships with trusted local vendors:
- a) Selling, moving, configuring or management of Multifunction Printers.
  - b) Network cabling or electrical work.
  - c) 3<sup>rd</sup> party Phone Systems other than Microsoft Teams Phones.
  - d) Custom application programming or database development.
  - e) Sales of accounting software or other primary line-of-business applications.
  - f) Selling, moving, configuring or management of audio and video conferencing systems, projectors, or televisions.

## Microsoft Subscriptions

- 13. Microsoft 365 Billing:** Payments are due within 30 days of receipt of invoices. Microsoft Subscriptions will have seven (7) days from placing an order for a new Subscription, from a renewal of an existing Subscription, or from an increase of seats to an existing Subscription, to submit a cancellation request for such. Client may be able to request a total cancellation of the seat-based Subscription or a partial cancellation. If Client submits a cancellation request within the initial seven (7) calendar days period, then Client will receive a prorated refund, calculated daily, which will be displayed on its next invoice.
- a) **Limited refunds:** No refund will be provided in connection with a cancellation request submitted after the initial seven (7) days period has passed, regardless of a One Year or One Month Term subscription.
  - b) **Termination Balance Payment:** Upon cancellation of this Managed-IT Agreement a payment in full is due within 30 days for the remaining balance for all one-year term subscriptions.
- 14. Azure Billing:** CNS will provide an Azure subscription account for Client with a preset approved budget or allowance to ensure Client does not overspend. Client will be notified by email when reaching 90% of their

set approved budget. Both Client and CNS must authorize any additional spending. The invoice is based on the total consumption by Client during the last billing cycle. Payments are due within 30 days upon receipt of invoices.

**a) Reservations Terms:** These terms will supplement the Channel Authorization and will govern any rights granted to Company to purchase or resell Reservation Offers. "Reservations" means an advanced purchase of eligible Marketplace Offerings for a specified term and region (e.g. Reserved Software Instances, etc.). Reservations are purchased for specified terms of up to three years. Reservations expire at the end of the specified term. Refunds are not available for unused Reservations. Unless indicated otherwise for a Marketplace Offering, exchange and cancellation are not available. Reservation pricing will be based on the available pricing at the time of each purchase. Reserved Instances for software do not include the cost of compute

**b) Termination Balance Payment:** Upon cancellation of this Managed-IT Agreement a payment in full is due within 30 days for the remaining balance for all one-year or three-year term reservations.

## Service Conditions

**15. Diamond Plan Microsoft 365 subscription requirements:** CNS deploys and supports advanced security services which requires an additional purchase of a Microsoft 365 beyond subscription that includes Enterprise Mobility + Security E3. One of the following 1 Year subscriptions qualifies.

a) Microsoft 365 subscription options

- |   |                                |
|---|--------------------------------|
| (1) Microsoft 365 Business Premium:             | \$22.00 per User (1 Year Term) |
| (2) Microsoft 365 E3:                           | \$36.00 per User (1 Year Term) |
| (3) Add-on - Enterprise Mobility + Security E3: | \$10.60 per User (1 Year Term) |

**16. IT Standards:** To maintain the highest level of service and to ensure the Client's environment meets our minimum standards, CNS will implement specific changes. If any of these minimum requirements are not met, CNS may cancel this agreement or provide services at an hourly rate while trying to resolve issues. For services that are not elected and mutually agreed not to be used an attestation letter will be submitted to Client outlining the associated risks of not using such services and releases of liability from CNS to Client as stated in the Terms. Minimum security standards are subject to change at any time based on new threats and the external security climate.

a) Client must have a current hardware warranty and/or software maintenance support and subscription services on all systems. Client is financially responsible for paying any additional costs that may occur if the hardware, software or service provider imposes a charge to obtain support or parts.

b) All workstation and server hostnames will be changed to a standard naming convention.

c) All workstations and servers must have a CNS agent, anti-virus and End Point Detection and Response installed.

d) Minimum security standards will be implemented, including but not limited to:

- i) Password complexity
- ii) Multi Factor Authentication for Microsoft 365.
- iii) Lockout policy
- iv) Password reset frequency
- v) Firewall security services
- vi) Patch levels
- vii) Port blocking
- viii) SSL cert application

e) Client must have a functional UPS (uninterrupted power supply) for all servers and networking appliances.

- f) Client must have a supported Microsoft Server and Desktop Operating system. CNS does support operating systems that have reached Microsoft's "Support End Date." For a complete list of end-of-support deadlines, visit [support.microsoft.com/lifecycle/search](https://support.microsoft.com/lifecycle/search).

## **Billing and Payment Terms**

- 17. Billing:** There are re-occurring monthly invoices for Managed-IT and software subscriptions with automatic monthly charges. There are also one-time invoices for products purchases and out of scope hourly rate services that are paid manually as invoiced.
- a) **Automatic Monthly Charge:** For monthly Managed-IT and Software subscription bills CLIENT agrees to set up automatic payments by ACH from a checking account or by credit card. Monthly automatic payments are charged 30 days upon receipt of invoices by email.
- b) **Product Charges:** For most product purchases of hardware and software payments are due within 30 days upon receipt of invoices. In some cases, depending upon the manufacture and costs there may be a down payment required.
- c) **Hourly Rate Charges:** CNS charges an hourly rate for requested services not covered under the Diamond Managed IT Service Agreement. Invoices are due within 30 days upon receipt of invoices. Below is an itemization of these services. Please note this list is inclusive but not exhaustive. Estimates of hours and pricing will be provided to the Client's designated personnel via a work authorization or project scope of work before the engagement of billable services. CNS charges **\$160.00 per hour** for the following work:
- i) Onsite support of remote offices outside of a 60-mile radius from the CNS Office; in certain instances, a local subcontracted resource may be retained for onsite technical support.
  - ii) Installation or re-locating of networking appliances, wireless access points, and server equipment.
  - iii) Installation of new Microsoft Windows Server machines on-premises or Microsoft Azure or AWS cloud platforms.
- 18. Payment Due Date/Default:** Unpaid balances will receive a written notice within 15 days. The notice will state that the delinquent account is subject to suspension and/or termination from services listed in this agreement unless a payment is received by within 15 days. Non-payment may result in temporary suspension of Requested Services. CLIENT will have 30 days to make payment or services will be terminated until all payments are made in full.
- 19. Fee Increases:** This agreement is subject to annual rate increase of 5% to 10%. Such rate increases are to accommodate for additional technology and services added to this agreement. CNS will provide Client a 30-day notice for any change in rates.

## **Acceptance**

- 20.** This Managed-IT Diamond Agreement ("**MSA**") is made by and between either an individual or an entity ("**CLIENT**") and Capital Network Solutions, Inc. ("**CNS**"), and it shall be effective as of the date that you electronically approved this Agreement ("**Effective Date**"). By accepting this Agreement, either by indicating your acceptance, by executing or approving a quote order that references this Agreement, you agree to this Agreement and the **TERMS AND CONDITIONS FOR ALL CNS SERVICES AND PRODUCTS**, located at <https://www.cns-service.com/agreement/> . Once accepted, this Agreement is a legally binding contract between You and CNS, and it sets forth the terms that govern the services or licenses to You hereunder. CNS reserves the right in its sole discretion to modify this Agreement from time to time and will provide reasonable notice of any such modifications by posting the most up-to-date version on CNS' website. Any modifications shall apply prospectively and only after notice has been given. Your continued use of the Services and Software following modifications shall constitute Your acceptance of the modifications.