Exhibit A: Managed Service Specifications

This exhibit describes the IT service and support that CA will deliver to the Client under the terms and conditions of the Master Service Agreement (MSA) and a Managed Service Order (MSO). The specific Services, Term Length, Non-Recurring and Recurring Charges will be designated, quantified, and described on a Managed Service Order (MSO). CA offers flexible Managed Service support options to Clients and the scope can vary per Client agreement. The descriptions below are intended to provide a comprehensive listing of all available Products and Services, however, the specific Products and Services provided will be designated in an MSO. CA will provide the following services in alignment with the MSO:

- **Managed IT Services**: Managed IT services are provided by technical service teams comprised of Service Desk, Remote Operations Center (ROC), and Managed Service Engineering support teams. CA has the ability to monitor, manage, and maintain the Client's IT infrastructure including servers, network devices, storage devices, backup systems, certain cloud services, and applications. CA has the ability to provide remote and onsite technical support, troubleshooting, and problem resolution for the Client's IT infrastructure. CA will use best practices and industry standards to ensure the availability, performance, security, and reliability of the Client's IT infrastructure. The scope of Managed IT Services and Products supported will be governed by the entitlements provided within an Order. The definition of support entitlements will be outlined in this Managed Service Specifications Exhibit.
- **Managed Security Services:** Managed Security services are provided by technical service teams comprised of Remote Operations Center (ROC), Security Analysts, Security Operations Center (SOC), and Security Engineering teams. CA has the ability to provide solutions designed to protect the Client's IT infrastructure from cyber threats, such as malware, ransomware, phishing, denial-of-service attacks, and unauthorized access. CA can also provide security awareness training, vulnerability assessment, penetration testing, incident response, and disaster recovery services for the Client's IT infrastructure. CA will use advanced tools and techniques to detect, prevent, and mitigate cyber threats. The scope of Managed Security Services and Products supported will be governed by the entitlements provided within an Order. The definition of support entitlements will be outlined in this Managed Service Specifications Exhibit.
- **Supported Client IT Infrastructure:** CA will provide support to all currently installed and functioning IT infrastructure within the entitlements in Managed IT Services. CA will provide support for all back-end systems and IT infrastructure including, but not limited to:
    - Servers, Storage, Backup, Virtualization, Hypervisor, and Universal Power Supply
    - Firewalls, Switches, Wireless Controllers, Access Points, SD WAN, Load Balancers, Routers
    - E-mail Platform, Archiving, Backup, Encryption, Anti-Spam, Phishing Protection, and Filtering
    - Endpoints such as Desktops, Laptops, Mobile devices, and Tablets
        - Windows Operating Systems – with active and current support from Microsoft
        - Mac Operating Systems – with active and current support from Apple
            - Operating systems that do not have an active and current support agreement will be supported on a best effort basis; support and remediation services may be limited.
        - Microsoft 365 – Productivity, Modern Work and Security
        - PC Hardware and Peripherals

        - Email and Mobility
    - Cloud Infrastructure, Storage, Backup, and Disaster Recovery
    - Phone Systems - Microsoft Teams, 3CX, and NEC
    - Connectivity (if procured and authorized through CA)

- **Not Supported Client IT Infrastructure:** CA is not obligated to provide support on the defined technology solutions:
    - Printers and Copiers
        - Rollers, Cleaning, Toner and/or General Maintenance
    - Phone Systems – All other
    - Programming or Coding
        - .net, JAVA, SQL DBAs
    - Line of Business Applications administration
        - CRM, ERP, CLM, Etc.
    - Software Development
- **Professional Services**: Outside of the scope of Managed Services Agreement and entitlements, CA can provide assessments, architectural design, Advisory Services, and Professional Services for the Client. Professional Service projects such as hardware and software procurement, installation, upgrades, or replacement; assessments, testing, or remediation; backup or disaster recovery planning or implementation; cloud migration or optimization; policy and plan creation; or any other project-based work will be scoped, quoted, and invoiced outside of the scope of the Managed Services Order and Agreement. CA will invoice the Client for these services based on the agreed upon scope, timeline, and budget and will be documented within a Statement of Work (SOW) or Service Order (SO).
    - Any New IT infrastructure, equipment, devices, and software will require a SOW or SO with Professional Services which will be scoped and delivered to the Client for approval.
    - Once New IT infrastructure, equipment, devices, and software is implemented, it will be supported within the Managed IT Service entitlements.
    - If the New IT infrastructure, equipment, and devices require additional software tools, security tools, or Managed IT support hours a Managed Service change order will be generated and delivered to the Client for approval.

Service Specifications for Managed IT Services

This section describes the Managed IT services that CA will deliver to the Client under the terms and conditions of the Master Service Agreement (MSA) and a Managed Service Order (MSO). The specific Managed IT Services will be designated, quantified, and described on a Managed Service Order (MSO). CA will provide the following services in alignment with the MSO:

- **Service Desk**: CA will provide multi-channel (Phone, Email, Chat) support and triage to Client and Client's end users. Service Desk is the initial service team for rapid response, resolution, and escalation. CA will use best practices and industry standards to ensure support requests are received, classified, and documented.
    - **Service Desk Services Include:**
        - Microsoft Windows, Office, Microsoft 365 support
        - End User computer (PC – Windows or Mac) support
        - Mobile device support
        - Network access and connectivity support
        - Rapid response, triage, and escalation
        - Active Directory and user administration
        - Windows file sharing administration and privileged access
- **Remote Operations Center (ROC)**: CA will monitor the IT infrastructure including servers, network devices, storage devices, backup systems, cloud services, anti-virus\EDR\MDR\XDR, and applications. CA will use best practices and industry standards to ensure the availability, performance, security, and reliability of the Client's IT infrastructure. CA will apply approved Microsoft updates and patches and Third-Party patches after they are released. CA and our patching solution provider review and validate the patches before implementing them across all supported devices.
    - **ROC Service Includes:**
        - Up-time/Down-time reporting
        - Event Log monitoring
        - Hardware performance
        - Drive space monitoring
        - Asset management and auditing
        - Monitoring, Alerting, and Notification
        - Microsoft Patching
        - Specific Third-Party Patching (horizontal business applications; not specific vertical applications)
- **Managed Service Technical Support**: CA will provide remote and onsite technical support, troubleshooting, and problem resolution for the Client's IT infrastructure. CA will monitor, manage, and patch the Client's IT infrastructure, including servers, network devices, storage devices, backup systems, cloud services, and applications. CA will also provide guidance to the Client's staff on how to use and maintain the Client's IT infrastructure. CA will also provide documentation and monthly reporting of the Client's IT infrastructure and assets under management.
    - **Managed Service Technical Support Includes:**
        - Active Directory and user administration
        - Windows file sharing administration and privileged access
        - Network Infrastructure troubleshooting, administration, and configuration.
        - Server and Storage Infrastructure troubleshooting, administration, and configuration.
        - Connectivity troubleshooting, administration, and configuration.
        - Microsoft Application and OS troubleshooting, administration, and configuration.
        - Cloud Application (horizontal business applications, not vertical applications) troubleshooting, administration, and configuration.
        - Backup Management and Testing
        - End user support, onsite and remote engineering, and Vendor engagement.
        - Third Party application support (horizontal business applications).
        - Third Party application assistance for Line of business applications (triage request and escalate to software Vendor, must have active support agreement with software Vendor).

- Third Party connectivity assistance for internet connections (triage request and escalate to ISP, must have active support agreement with service provider).
- Software tool reporting and analysis.
- Technology Roadmap and Lifecycle Management
- Technology Business Reviews

Service Specifications for Managed Security Services

This section describes the Managed Security services that CA will deliver to the Client under the terms and conditions of the Master Service Agreement (MSA) and a Managed Service Order (MSO). The specific Managed Security Services will be designated, quantified, and described on a Managed Service Order (MSO). CA will provide the following services in alignment with the MSO:

- **Security Tools and Software**: CA will provide a portfolio of Cyber Security tools, software, and hardware solutions to be utilized in the Client's IT Infrastructure.
    - **Security Tools and Software Include:**
        - Anti-Virus and Endpoint Detection Response
        - Security Awareness and Training
        - End User Phishing, Smishing and Vishing Simulation
        - Multifactor Authentication
        - Web and DNS Filtering
        - Spam Filtering
        - Managed and Monitored Network Infrastructure
        - IDS/IPS
        - Managed Backup and Disaster Recovery
        - Password Management
        - Email Encryption
        - Device Encryption
        - Email Archiving
        - Managed Detection Response
        - Security Incident and Event Management
        - Dark Web Monitoring
        - Vulnerability Scanning
        - Network Access Control
        - Mobile Device Management
        - Zero Trust Network Access
        - Secure Access Services Edge
        - Compliance Management
        - Threat Hunting
        - Cloud Access Security Broker
        - Data Loss Protection and Prevention
- **Managed Security Service Technical Support**: CA will provide remote and onsite technical support, troubleshooting, and problem resolution for the Client's cyber security tools and software. CA will respond to the Client's requests and incidents within the agreed service level goals (SLG). CA will also provide guidance to the Client's staff on how to use and maintain the Client's cyber security tools and software.
    - **Managed Security Service Technical Support Includes:**
        - Tool administration
        - Reporting and analytics
        - Tool and Software provisioning and configuration
        - Assessments, Reporting, and Scanning
        - Risk identification
- **Security Operations Center (SOC)**: SOC Service provides monitoring, detection, investigation, escalation, and incident support for incidents within the current support toolset and visibility of the managed services. CA will provide remote and onsite technical support, troubleshooting, and problem resolution for the Client's subscribed security solutions within the Service Order. CA will respond to the Client's requests, Vendor requests, and incidents within the agreed service level goals (SLG). CA will provide monitoring, alerting and technical response to validated alerts from the Security Operations Center (SOC). CA will coordinate response and remediation with Client and Clients designated authorized contacts or representatives.
    - **SOC Service Includes:**
        - Detecting, preventing, investigating, and responding to cyber threats
        - Managed Detection and Response

- Event and System Log monitoring
- Tool and software administration, access control, and reporting
- Network monitoring
- Threat detection and Threat intelligence
- Incident investigation and technical response
- Incident Response rapid engagement and remediation
- Detailed reporting
- Risk and Compliance Management
- Responsibility for all people, processes, and technologies needed to enable these services and provide 24/7/365 support.

- **Incident Investigation and Response**
  - The SOC will provide monitoring, detection, investigation, escalation and incident support for all incidents within the current supported toolset and visibility of the managed services.
  - The SOC is responsible for incident monitoring, detection, analysis, investigation, escalation, and incident support. The SOC will be responsible for remote incident analysis and investigation to determine if alerts or security events warrant incident classification. If an event is classified as an incident by the SOC, the SOC will track the incident with You. The SOC will perform incident triage to include determining threat scope, urgency, potential impact and make recommendations designed to allow for remediation.
  - The SOC will remotely investigate initial security events identified by the SOC and escalate as appropriate in accordance with the established and agreed upon Service Level Goals (SLGs). Events and incidents will be analyzed and investigated using the SOC's standard process and procedures. Escalations will follow established escalation paths and utilize contact information collected during onboarding and documented by SOC.
  - For incidents that are assigned to the Client after analysis, the Client is responsible for escalating incidents back to the SOC that require action or analysis by the SOC.
  - The SOC will be the collection point for additional group inputs for classification of security incidents. The potential exists for other entities to notify the SOC of possible events. In these relatively rare cases, the SOC will ensure outside sources of information are incorporated into established SOC workflow procedures. As events are pulled into the SOC Workflow, it is the SOC's responsibility to create and classify incidents. As the SOC is responsible for incident escalation and response, only the SOC has the authority to classify events or alerts as incidents to ensure due diligence of event investigation and accountability in reporting.
- **During incident investigation the SOC may perform the following activities:**
  - Perform analysis on client assets / traffic, document results noting attacker profiles.
  - Assist in identifying potential impact of incidents on client systems and using available CA security tools to assist client in determining if data was exfiltrated.
  - Document and track events (false positives and false negatives, blacklists, whitelists) within the CA security toolset.
  - Escalate incidents to identified client contacts for further remediation.

- **Testing of Monitoring and Response Capabilities**

- The Client may test SOC monitoring and response capabilities by staging simulated or actual reconnaissance activity, system, or network attacks, and/or system compromises. Such activities may be initiated directly by Client or by a contracted third party. Client shall notify the SOC testing email at least fourteen (14) days in advance of testing with the expectation that analyst activities will not be notified of testing. Testing performed on newly added (within 60 days) assets or data feeds should be communicated to the SOC via advance electronic or written notice to ensure SOC personnel have properly onboarded new information and that all monitoring and response capabilities are working properly. SLGs will not apply during the period of staged or testing activities.

- **Scheduled and Emergency Maintenance**
  - Scheduled maintenance means any maintenance that is performed during a scheduled maintenance window or in which Client is notified at least one day in advance. Notice of scheduled maintenance will be provided to the Client's Authorized Point of Contact. Emergency maintenance means any non-scheduled, non-standard maintenance required by SOC. No statement in the section of any Services entitled "Service Level Objectives" shall prevent SOC from conducting emergency maintenance if it is critically necessary for the integrity and security of the Services. During such emergency maintenance, Client's Authorized Point of Contact will receive notification of initialization of the emergency maintenance, and of the completion of the emergency maintenance. The SOC will be relieved of its obligations under the applicable SLGs during scheduled and emergency maintenance.

- **File Sample Submissions**
  - The EDR and SIEM SOC services may detect suspicious or malicious executable files on endpoints. Sometimes it is necessary to perform additional investigations to understand an attack. In these cases, CA may retrieve file samples of suspicious or malicious files from an endpoint to perform additional analysis.
  - By allowing sample submissions, our analysts are enabled to provide more in-depth analysis and context to their investigations of potential incidents, as well as enhancing the detection and prevention of future incidents that may involve the same file(s).
  - Part of this process may require our analysts to automatically request samples of files, scripts or other source detected in Client or End Client environments to perform further analysis. In addition to our own in-house analysis, CA may use outside services including but not limited to:
    - VirusTotal
    - Opswat MetaDefender
    - Joe Sandbox
  - Unless the Client opts-out of File Analysis Submissions, the SOC will request samples from an endpoint and upload potentially malicious files for analysis as needed.
  - By allowing permission for the SOC to upload unknown binaries, SOC Analysts will either manually or automatically upload unknown binaries to outside analysis services:

        - Sample binary or its hash representation will be submitted to the appropriate analysis service.
    - Terms of Service and Privacy Policy for each service will apply.
    - The SOC shall not be responsible for this submission or for any act or omission by any online service.
    - You are hereby advised some / most analysis services make the file metadata publicly available, along with scan results from numerous anti-virus products. Service providers may also make the files samples available for download to partners.

- **Host Isolation Terms**
    - With our EDR offerings, CA SOC has the ability to isolate machines on a Client or End Client's network that have an agent installed. The SOC uses host isolation to prevent the spread of malicious code by preventing a compromised machine from communicating to other network devices on the Internet or the Client or End Client's network. The isolated machine will maintain connectivity to SOC and allow our analysts to continue investigation without risking other network devices to malicious code or active attacks.
    - Unless the Client opts-out, CA will isolate potentially compromised machines. CA will manually isolate the machine using the installed Endpoint Agent and notify the client of the isolation via an incident for escalation. The machines will remain in isolation until the threat has been remediated or the client has specifically said they accept the risk and request the SOC to remove the isolation.
    - The client commits to identifying production impacting servers and assets that are NOT to be isolated unless the client has given written authorization. Client recognizes they assume all risk for non-isolated machines and the spread of any attack profile due to this.
    - The SOC commits to isolating machines that are NOT on the unauthorized list only to prevent the spread of malicious code and lateral movement by suspected attackers.
    - The SOC will escalate all incidents that require isolation to the client for their visibility and active feedback on the incident.
    - Clients are hereby advised that the SOC has the functionality to isolate machines on your network or End Client's network with installed CA EDR offerings, that the SOC has the ability to use this function to protect the network, and that the isolated machines will lose all connectivity to all other devices on the network.

- **Automated Remediation**
    - Some incidents can be remediated by the CA EDR agents. These remediation actions are visible in the endpoint console. Clients can opt-out of allowing SOC Analysts to execute the automated remediation actions on affected endpoints. The current remediation actions that can be performed are, but are not limited to:
        - Kill Process
        - Quarantine Files
        - Remediate Threat
        - Rollback Threat

- Clients are hereby advised that the SOC has the functionality to remediate machines on your or your End Client's network, that the SOC has the ability to use this function to protect the network, and that the SOC is not liable for downtime as the result of remediation actions that were taken.

Additional Terms and Conditions

- CA can only support equipment that has a valid and current warranty and/or support agreement from the manufacturer or Vendor. The Client is responsible for renewing and maintaining such warranty and support agreements for all equipment that is covered by the Managed IT and/or Managed Security services. CA will not be liable for any failure or damage to equipment that is caused by an expired or invalid warranty or support agreement.

- CA will offer a la carte Managed IT and Managed Security services for Clients and expressly provides Products and Services defined in the Client approved Managed Service Order. The Client can opt in or opt out of these services based on their needs and preferences. By opting out of Managed Security Services, Client is willingly and knowingly accepting the risk associated with not implementing industry defined (NIST CSF) Cyber Security best practices.

- The Client may also bring their own solution for any type of Product or equipment that is not supported within CA' approved solution portfolio (Exhibit C). CA will provide best effort support for this equipment but will not guarantee any SLG (Exhibit B) or quality of service in remediation. CA will provide services in a good and skillful manner in effort to reduce or resolve any Client incidents.

- The Client may request changes to their service options at any time by notifying CA in writing. CA will provide a change order and adjust services as agreed upon in a signed MSO. CA will provide a change order and adjust services if agreed upon in a signed MSO.

- The Client will pay CA a monthly fee based on the number of users and devices that are covered by the Managed IT and Managed Security solutions. CA will allow variance of approximately ten percent (10%) of the monthly recurring charges without incurring and enforcing a change order. CA will invoice the Client monthly, and payment is due on the due date. The first month of service will be invoiced along with onboarding charges post implementation and service activation date. Sales Tax is not charged upfront on services, but when applicable taxable services occur in a month, you will receive an invoice to pay for those taxable services. You may review the Minnesota Department of Revenue Sales Tax Fact Sheet 134 for further clarification. At the conclusion of each month, time and services are reviewed by CA, and if services beyond the contract occur, an invoice will be sent accordingly. Questions regarding your invoice or any related billing issues can be resolved by reaching out to the finance department by emailing finance@cyberadvisors.com.

- CA reserves the right to suspend or terminate any or all of the Services if the Client fails to pay the invoices on time or breaches any of the terms and conditions of the MSA. CA will notify the Client in writing before taking any such action and will give the Client five (5) calendar days to remedy the situation.

- CA provides monthly reporting on all subscribed services per the MSO, this can include Backup, Server, Active Directory, Storage, Email, Network cabling, Network Infrastructure, Remote Management, workstations, security solutions, and Cloud applications. Reporting will indicate quantities, deployment, health, status, risk, and action items.

- CA performs Vendor due diligence on all third-party manufacturer solutions, including hardware and software. Additional diligence information is available upon Client request. CA will assist the Client in requesting, gathering, and delivering all relevant due diligence information from the Vendor. By using our services, Client agrees to comply with the third-party terms and conditions, acceptable use policy and end user license agreements. The Client acknowledges that they have read and understood the terms and conditions of these agreements and accepts them. You also agree to indemnify and hold CA harmless from any claims, damages, or losses arising out of Clients breach of these agreements.

Exhibit B: Service Level Goals (SLG)

This exhibit describes the Service Level Goals that CA will deliver to the Client under the terms and conditions of the Master Service Agreement (MSA). CA will provide the following Service Level Goals:

METRIC	DESCRIPTION	PERFORMANCE GOAL
Availability of Service Desk	Hours of Service Desk operation	24x7x365
Availability of Contact Center	Hours of Contact Center operation	24x7x365
Email Response Time	The amount of time it takes for the Service Desk to respond to a Client email or voicemail request	Goal = 85% of email requests are responded to in less than 4 business hours.
Phone Call Response Time	The amount of time it takes for the Service Desk to answer a Client phone call	Goal = 85% of calls received are answered within 90 seconds.
Call Abandonment	The percent of Client calls that are hung-up or disconnected before Service Desk responds	Goal = Less than 10% abandonment rate.
Open Service Desk Tickets Status	The number of open tickets on weekly review queue that include current status. Actionable tickets are when there are no delays in waiting on Client collaboration and availability.	Goal = 100% of actionable open tickets have status updates within the last 24 hours.
Escalation Time	The amount of time it takes for the Priority Alerts to get escalated.	Goal = 95% of alerts are triaged, escalated, and assigned in less than 2 hours.
EDR Initial Threat Analysis	The amount of time to identify an endpoint related threat (must have EDR agent installed).	Completed within 1 hour of alert and incident created if necessary.
SIEM Initial Threat Analysis	The amount of time to identify an infrastructure related threat (must have SIEM agent installed).	Completed within 2 hours of alert and incident created if necessary.
Client Created Security Alert	The amount of time to respond to a Client created ticket regarding security services.	Varies by priority (Low – 4 hour, Medium – 4 hour, High – 2 hour, Urgent – 1 hour)
SOC Voicemail Response	The amount of time to respond to a Client created voicemail regarding a security incident.	All voicemails to the SOC are classified as Urgent tickets with a 1 hour initial response goal

Exhibit C: Approved Solutions List

This exhibit describes the Approved Solutions List that CA will support in alignment with the SLG provided in Exhibit B. This list is subject to change at any time at CA' sole discretion. Products or equipment manufacturers not on the Approved Solution List will be supported in a best effort manner. CA will use commercially reasonable efforts to support, repair and maintain Products that are not on the Approved Solution List.

Approved Solution List:

Equipment	Supported Manufacturers
Servers	Dell
	HPE
	Lenovo
	SuperMicro
Server OS	Windows Server 2019 or later
Hypervisor	Microsoft Hyper V
	VMware ESXi
Storage	Dell EMC
	HPE
Backup Systems	Veeam
	Dell EMC
	Datto
	Axcient
	SkyKick
	Acronis
	DropSuite
	Arcserve
Client PC	Dell
	HPE
	Lenovo
	Apple
	Microsoft
Client PC OS	Windows 10, 11 or newer
	MacOS
Phone System	Microsoft Teams
	3CX
Cloud Service	Microsoft Azure (IaaS, PaaS, SaaS)
	Microsoft 365 Suite
Applications	Microsoft SQL Server 2017 or later
	Microsoft Exchange Server 2019 or later
Networking	Fortinet

	Sophos
	HPE Aruba
	Cisco Meraki
	SonicWall
	WatchGuard
	Dell
	Auvik
Patching	ConnectWise
	PatchMyPC
	Microsoft InTune
AntiVirus/EDR	Sophos
	SentinelOne
	Microsoft Defender
	ESET
Email Security	Securence
	Barracuda
	Sophos
	Microsoft Defender
	Zix (Webroot)
Security Awareness	KnowBe4
	Arctic Wolf
Web Filtering	Cisco Umbrella
	DefensX
IDS/IPS	Perch (ConnectWise SIEM)
MFA	Microsoft
	Cisco DUO
MDR	Sophos
	SentinelOne
	Arctic Wolf
	Perch (ConnectWise SIEM)
Dark Web Monitoring	IDAgent
	Keeper
Password Management	LastPass
	Keeper
	Passly