Managed Services Agreement

This Managed Services Agreement (the “Agreement”) is a legal agreement entered into by and between Secure Data Technologies, Inc. (Secure Data) and the Client identified on an order form (“Client”) and governs any Statement of Work, quote, proposal, or other ordering document executed by Client (“Order Form”) that references this Agreement. The Order Form will be issued to Client by Secure Data. This Agreement is effective on the date Client executes the Order Form or submits a matching purchase order to Secure Data (the “Effective Date”).

This Agreement permits Client to purchase Managed Services, as defined below, and which are identified in the Order Form (the “Subscribed” Managed Services), and sets forth the terms and conditions under which the Managed Services will be delivered. The Agreement consists of the terms and conditions set forth below, the Master Agreement between the parties, and any Order Forms that reference this Agreement. If there is a conflict between the terms below, the Order Form, or the Master Agreement, the documents will control in the following order: The Master Agreement, the Order form (which may from time to time contain alterations to these standard terms and conditions), then this Agreement.

BY EXECUTING, WHETHER MANUALLY OR ELECTRONICALLY, AN ORDER FORM, DELIVERING A PURCHASE ORDER OR OTHER CONFIRMATION TO SECURE DATA, OR OPERATING, DOWNLOADING, INSTALLING, REGISTERING OR OTHERWISE USING THE PRODUCTS, OR CLICKING AN "I ACCEPT” OR “CONTINUE" BUTTON ASSOCIATED WITH THIS AGREEMENT, CLIENT (OR ITS AUTHORIZED AGENT, IF APPLICABLE) EXPRESSLY AND EXPLICITLY ACKNOWLEDGES AND AGREES THAT THIS IS A BINDING AGREEMENT AND CLIENT HEREBY AGREES TO THE TERMS OF THIS AGREEMENT AND ACCEPTS THE OFFER TO PURCHASE TO THE MANAGED SERVICES PURSUANT TO THE TERMS HEREIN.

In consideration of the mutual covenants and agreements contained herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. SCOPE

1.1. Managed Services, General. Client will purchase, and Secure Data will provide the specific Managed Services as specified in the applicable Order Form. Secure Data’s Managed Services offerings are Managed Help Desk, Managed Infrastructure, Managed Continuity, and Managed Cybersecurity. The scope of each Managed Service is defined within Section 1. The parties acknowledge that Secure Data will provide only Subscribed Managed Services purchased by Client as specified in the applicable Order Form.

1.2. Managed Help Desk. In general, Managed Help Desk provides the first line of support for Client’s employees to work with when they have IT questions or need IT assistance. Secure Data provides a multi-tiered team of support engineers who are available to perform End-User and workstation support.

1.2.1. Inclusions: Secure Data will provide, and Client may receive, the following:
- Remote troubleshooting and remediation for End-Users.
- 8AM – 5 PM CST Monday through Friday support for all issues.
- 24 x 7 x 365 support for all P1 issues (see P1 definition in Section 2.2).
- Access to the Secure Data ticketing system with phone and email channels for support.
- Priority-based triaging and routing for various ticket types for fast resolution.
- Remote Monitoring and Management (RMM) agent for remote support and issue remediation.
- Password and MFA resets for End-Users.
- User moves, adds, changes according to Client-defined user onboarding procedures.
- Remote Windows PC device provisioning and deployment.
- Active Directory and Entra ID account support.
- Operating System (OS) troubleshooting and configuration for Windows and MacOS.
- Remote troubleshooting of print queue-related issues.
- VPN and Remote Desktop support.
- Remote application support, including Microsoft Office suite and common business-related applications.
- Third-party application issue escalation support (procedures to be defined by Client).
- Third-party ticket management and status updates for services such as ISPs or security vendor-related issues.

1.2.2. Exclusions: The parties agree the following are not included within the scope of this Agreement:
- On-site support at Client’s location(s) is not included, except as documented on the Order Form.
- Mobile devices (tablets and phones) are not covered for support, except for password or MFA reset requests.
- Linux and Unix operating system support.
- Client’s employees’ home office equipment.
- Client’s employees’ home networking issues.
- Support for any personally owned devices, such as an employee’s “Bring Your Own Device” (BYOD) laptop.

1.2.3. Client Responsibilities, Managed Help Desk. Client will be responsible for the following requirements for Managed Help Desk. These responsibilities are in addition to the responsibilities listed in Section 1.6.
- End-User devices must have endpoint security software installed.
- Supported devices must be under current manufacturer hardware support, or alternatively, spare equipment must be available for replacement due to hardware, software, or configuration failure.
- Applications and operating systems must be supported and under appropriate vendor maintenance agreements.

1.3. Managed Infrastructure. In general, Managed Infrastructure provides flexible monitoring and management of the Client’s network infrastructure. Secure Data utilizes a proprietary combination of tools and platforms to provide monitoring and management services and offers standard and customized alerting and remediation services based on Client’s business requirements.

1.3.1. Inclusions: Secure Data will provide, and Client may receive, the following:
- 24 x 7 x 365 monitoring of all Covered Devices.
- 24 x 7 x 365 support for all P1 issues (see P1 definition in Section 2.2).
- 8AM – 5 PM CST Monday through Friday remote troubleshooting and remediation for Covered Devices.
- Customized escalation chain alerting to Client End-Users, as required.

- Covered Device and configuration moves, adds, and changes (Client may add additional devices as Covered Devices at the per-device rate in the Order Form), including:
  - Switches: VLANs, port channels, and base configuration
  - Routers: interface changes, routing, and base configuration
  - Firewalls: security policies, and base configuration
  - Wireless access points: SSIDs, VLANs, and base configuration
  - SD-WAN controllers and appliances: base configuration, and routing configuration
  - SAN & NAS devices: base configuration, storage, LUN management, share, and permission updates
  - Servers (physical or virtual): virtualization management, physical host management and patching, and resource monitoring and alerting
  - IOT devices: base configuration, network connectivity, and application connectivity
- Internet Circuit Incident Management, including diagnosis and remote coordination between Client and internet circuit vendor to restore service as quickly as possible.
- Covered Device patching: Upon Client request, Secure Data will apply any vendor-supported network device patching (excluding major software version upgrades) within 30 days and during Normal Business Hours, dependent on Client-approved maintenance windows and Client-accepted risk of applying patches.
  - After-hours Covered Device patching and upgrades are also available, but will be billed at current after-hours or weekend rates
- Covered Device configuration backups: For supported platforms, Secure Data Technologies will maintain annual backups of Covered Device configurations. Supported platforms may vary over time, but currently includes Cisco Systems (excluding Meraki), Juniper Networks, Pure Storage, HPE and VMWare.
- Access to management software platforms used by Secure Data to monitor and manage Covered Devices.
- Documentation of all discovered devices and network topologies, including review of naming conventions and best practices, existing alerts and issues, identification of end-of-support or end-of-life devices, and identification of pre-existing vulnerabilities.
- Access to Client portal which includes access to Client's environment alerts, SNMP polling, ticket history, reporting, and default dashboards.

1.3.2. Exclusions: The parties agree the following are not included within the scope of this Agreement:
- On-site support at Client's location(s) is not included, except as documented on the Order Form.
- Remediation of changes to the network environment made by Client or a third-party that were not previously discussed or planned in coordination with Secure Data.
- Mobile Devices and End-User workstations.
- Scripting changes or patching requests to occur outside of Normal Business Hours.
- Vendor contract negotiations and vendor relationship management.
- Major software releases and version upgrades.
- Licensing configuration changes. For example, the conversion from PAK to subscription-based licensing through a Cisco SmartNet account would not be included.
- Implementation of net-new functionality provided by software releases or enhancements that were not previously implemented in the environment. An example would be a firewall update that introduces new antivirus capability. If that functionality was not previously implemented or enabled, the task of enabling and configuring the new functionality is not included.
- Storage technology conversions. For example, converting from iSCSI to Fiber Channel or changing block levels would not be covered.
- IP Address Management (IPAM). Secure Data will document known IP addresses but is not responsible for maintaining source of truth records for all addresses.
- Net-new infrastructure deployment, such as a new site, firewall, switch, cluster host, or virtual machine. If requested by Client, these services will be scoped and billed as outside the scope of this Agreement.
- Security Information Event Management (SIEM) log collecting or monitoring.
- End-User troubleshooting or assistance, such as issues connecting to a wireless access point. Secure Data will validate and work with established Client contacts to verify correct operation of Covered Devices, but direct End-User support is not included.
- Custom reporting or dashboards. A standard set of network dashboards is made available to all clients at no cost.

1.3.3. Client Responsibilities, Managed Infrastructure. Client will be responsible for the following requirements for Managed Infrastructure. These responsibilities are in addition to the responsibilities listed in Section 1.6.
- Covered Devices must be under current manufacturer hardware or service support, or alternatively spare equipment must be available for replacement due to hardware, software, or configuration failure.
- Software or firmware versions installed on Covered Devices must be under current manufacturer support.

1.4. Managed Continuity. In general, Managed Continuity provides secure, reliable, and validated backups of Client's operating systems and cloud solutions. Secure Data utilizes a proprietary combination of tools and third-party vendors to offer backup and recovery solutions that are capable of meeting Client's mean-time-to-recovery (MTTR), security, and/or compliance objectives.

Due to the highly customizable nature of Secure Data's Managed Continuity offerings, this document defines the standard inclusions and exclusions to its Managed Continuity service. See the applicable Order Form for additional inclusions, exclusions, or customized services as agreed to between the parties.

1.4.1. Inclusions: Secure Data will provide, and Client may receive, the following:
- 256-bit AES or better encryption for all data in transit using TLS (Transport Layer Security).
- 8AM – 5PM CST Monday through Friday remote support for simple file or directory restoration, or for the restoration of a single virtual machine.
- 24 x 7 x 365 monitoring of all covered continuity solutions.
- 24 x 7 x 365 phone support for any P1 outage or recovery situations (see Managed Continuity Exclusions for the billable nature of Major Incident recovery services).
- Project management to facilitate onboarding of Managed Continuity services.
- Reporting on continuity events including successful backups, errors, warnings, or informational alerts will be delivered to Client at either monthly, weekly, or daily intervals, as requested by Client.
- Daily backup checks will be performed by Secure Data during Normal Business Hours. Daily backup checks consist of reviewing internal monitoring and alerting of jobs, and addressing any issues in an error or warning state.
- Service tickets are proactively generated to alert on any issues in an error or warning state to ensure timely communication and remediation notes to Client.
- Quarterly engineer-validated verifications of backup data.

1.4.2. Exclusions: The parties agree the following are not included within the scope of this Agreement:
- File, directory, or image-based restorations outside of Normal Business Hours will constitute a billable engagement.

- Regularly scheduled backups according to the defined frequency and retention policy as defined on the Order Form are included in this Agreement. On-demand backups, or backups that are in addition to the pre-defined retention policies and frequency will constitute a billable engagement to provide such additional backups.
- Backup data that exceeds contracted data amounts (either in storage size or number of protected items, servers, or users) are billed as additions to Client's Managed Continuity agreement. For specific details on incremental costs, please refer to your Order Form.
- Major incident recovery services, such as recovery of an entire environment after a complete server hardware failure, a failure resulting from third-party vendor updates, failures caused by force majeure, theft, vandalism, etc. are not covered under this agreement and will constitute a billable engagement, both to recover the data and to rebuild or restore services.
- Data contained within a backup job that has expired or has exceeded pre-defined retention policies cannot be recovered, and Secure Data maintains no obligation to recover such data.
- Conditions outside of Secure Data's control may adversely impact the ability of Secure Data to perform successful backups or restorations. Examples of such conditions include a Client task, software, scheduled job, or other human intervention (intentional or otherwise) that renders files unavailable to Service, failure of Client software or operating system, or network connectivity issues between Client server and cloud-based hosting providers including, but not limited to, packet loss, lack of sufficient network capacity, etc. Such conditions and any remediation required to alleviate them are excluded from this Agreement.

1.4.3. Client Responsibilities, Managed Continuity. Client acknowledges and affirms that in the event of a support issue or restoration event, Client is responsible for on-site cooperative efforts with Secure Data as required to assist in the diagnosis and remediation of the issue. Client also acknowledges and affirms that Secure Data cannot guarantee compatibility with any version changes or hardware upgrades made by the Client on their network, server, OS, or application infrastructure without advanced notice and confirmation of compatibility. It is the Client's responsibility to ensure any planned version changes on their infrastructure are compatible with Secure Data's equipment and software, including cloud services. These responsibilities are in addition to the responsibilities listed in Section 1.6.

1.4.4. Ownership of Client Data. At all times, backup data stored on Secure Data hardware or in any third-party data center remains the sole property of Client. If Client chooses to terminate Managed Continuity, Secure Data will assist Client in the orderly termination of services and retention of existing data. Client agrees to pay Secure Data the actual costs of rendering such assistance. Client warrants that it is the owner or legal custodian of any data transmitted to Secure Data, and Client further warrants they have full legal authority to transmit said data and direct its disposition in accordance with the terms of this Agreement.

1.5. Managed Cybersecurity. In general, Managed Cybersecurity provides security solutions with a pre-defined set of security tools that offers effective cybersecurity protection responsive to the constantly evolving cybersecurity threat landscape.

1.5.1. Inclusions: Secure Data will provide, and Client may receive, the following:
- Provisioning and management of a comprehensive security platform including:
  - Endpoint Detection and Response (EDR)
  - Identity Threat Detection and Response (ITDR)
  - Security Information and Event Management (SIEM)
  - User Security Awareness Training (SAT)
  - Web & Content Filtering
  - Vulnerability and Dark Web Scanning
  - User Password Management
- 24x7x365 active monitoring and alerting for all components of the Managed Cybersecurity stack.
- Automated endpoint and identity isolation in the event of a detected threat event.
- Alert-based service ticket generation and notification for critical security events.
- Regular updates and patch management for deployed cybersecurity tools managed under this Agreement.
- Quarterly security summaries as part of the Quarterly Business Review (QBR) process.
- Project management and onboarding support for tool deployment and user adoption.
- Security awareness training campaign setup, monitoring, and reporting for Covered Users.

1.5.2. Exclusions: The parties agree the following are not included within the scope of this Agreement:
- Incident response beyond initial triage and alerting is not included. Full-scale incident response, forensic investigation, containment, and remediation services constitute a separate, billable engagement.
- Cybersecurity services provided for endpoints, users, or systems not explicitly defined and covered in the Client's active Order Form are excluded and will be subject to additional charges if support is requested.
- Any effort to remediate or investigate issues caused by Client-managed or third-party cybersecurity tools, configurations, or conflicting software.
- Recovery from security incidents or breaches caused by Client's failure to follow reasonable security practices (ex. use of unsupported software, failure to implement MFA, or non-compliance with recommendations from Secure Data) is not included.
- Support for regulatory compliance (e.g., HIPAA, PCI-DSS, CMMC) is not included unless specifically defined and scoped in the Order Form.
- Business email compromise (BEC), wire fraud, or other social engineering incidents are not covered under this Agreement. Education and best practices are provided via SAT, but financial restitution or recovery is outside the scope of this Agreement.
- Remediation efforts resulting from causes beyond Secure Data's control, such as power outages, natural disasters, third-party vendor outages, or internet service disruptions, are excluded from this Agreement.
- Performance issues or downtime caused by Client-side infrastructure, configurations, or failure to meet Secure Data's minimum technical requirements may be excluded from coverage or result in billable support.

1.5.3. Client Responsibilities, Managed Cybersecurity. Client agrees to maintain, at its own expense, an active cyber liability insurance policy with coverage levels appropriate to the size and nature of its business and the data it processes or stores. This policy should include, at minimum, coverage for data breaches, network security failures, business interruption, and legal or regulatory liabilities arising from cybersecurity incidents. Upon reasonable request, Client shall provide proof of such coverage to Secure Data. These responsibilities are in addition to the responsibilities listed in Section 1.6.

1.5.4. Cybersecurity Risk Acknowledgement and Indemnification. While Secure Data employs reputable tools and continuously updates its Managed Cybersecurity platform to respond to emerging threats, no cybersecurity solution can guarantee complete prevention of all cyberattacks. Accordingly, Client acknowledges and agrees that Secure Data shall not be held liable for any damages, including but not limited to loss of data, business interruption, reputational harm, or other consequential, incidental, or indirect losses arising out of or related to a cybersecurity incident. Client agrees to indemnify, defend, and hold harmless Secure Data Technologies, its officers, directors, employees, and affiliates from and against any and all claims, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or related to such incidents, except to the extent caused by Secure Data's gross negligence or willful misconduct.

1.6. Client Responsibilities. The following responsibilities apply to any Subscribed Managed Services purchased by Client. Client and Secure Data acknowledge these conditions are essential for Secure Data to successfully provide the Managed Services included in this Agreement. Therefore, Client agrees to the following:

- To provide remote network access, connectivity, and privileges to Secure Data employees as requested and in a timely fashion.
- To approve the installation of our Remote Monitoring & Management toolset.
- To provide one physical or virtual machine for use by our tools, with the following minimum specifications: Windows 11 Pro or Windows Server 2022 Standard, 2 CPU cores, 8GB RAM, 80GB hard drive space, full administrative rights.
- To provide administrative account access privileges as required to troubleshoot issues as they arise.
- To provide Secure Data as an authorized contact with ISPs, vendors, and other third parties as required to empower Secure Data to troubleshoot issues on your behalf. In some cases, Client may sign a Letter of Authorization (LOA) with the vendor to allow Secure Data access to the Client's maintenance agreements and support resources.
- For vendors where Secure Data is not listed as the reseller of record or does not have a Letter of Authorization (LOA) on file, Client will be responsible for opening vendor support cases on Secure Data's behalf.
- To provide all pertinent and requested documentation information to Secure Data in a timely manner.
- To work with Secure Data to identify appropriate escalation paths and procedures for issues as they arise.
- To appoint a primary contact that is authorized to schedule work and answer questions to resolve issues as they arise.
- To promptly notify Secure Data of any planned or active major deployments and/or infrastructure changes that could cause network issues or generate alerts from Secure Data's monitoring toolset.
- To maintain active support agreements for all hardware and line-of-business software. Any hardware or software support without an active support agreement will be provided at best effort only and is excluded from SLA guarantees or penalty calculations.

2. SERVICE LEVEL AGREEMENT AND INCIDENT DEFINITIONS

2.1. Incident. An Incident is an event that occurs where a Covered Device or Covered User issue is reported that is outside of normal operating expectations. Incident definitions included in Section 2.2 and the related Service Level Agreements (SLAs) will be applied to all Incidents. Secure Data will make the initial classification of all Incidents based on information reported to it by the tools, ticketing systems, Covered Users, or assigned Client personnel.

2.2. Service Level Agreements.

Classification	Incident Definition	SLA	Support Channels
Priority 1 (P1) CRITICAL	▫Network or service is down for all users ▫Critical impact to Client's business operations *Examples:* ▫Firewall failure/site inaccessible ▫Ransomware security incident ▫Phone system failure	▫Support available 24x7x365 ▫Contact Client within 30 minutes of incident report ▫Begin work within 60 minutes ▫Client and Secure Data will commit resources 24x7 as needed to resolve the Incident	**PHONE ONLY** 618-726-4040 *P1 issues should not be reported via email or portal, as these are not monitored 24x7x365.*
Priority 2 (P2) High / VIP	▫Operation of existing network or service impaired, but most business functions remain operational ▫Users designated on the VIP list (limit: 5 per Client) that have an issue preventing them from performing daily task, work, or other business operation *Examples:* ▫Primary device failure, but backup device running ▫Degraded performance or features that impact a significant percentage of users	▫Responses provided during Normal Business Hours ▫Phone contact with Client within 2 hours of Incident report ▫Begin work within 2 business hours ▫Client and Secure Data will commit necessary resources full time during Normal Business Hours to resolve the Incident	**Phone or Email** 618-726-4040 support@securedatatech.com
Priority 3 (P3) Standard	▫Operation of a service or device is not optimal, or a move, add, or change is requested ▫Issues or outages that affect a single user or small subset of users ▫Overall functionality is intact. Impact and severity are normal Examples: ▫Move, add, or change ▫Single user or small branch application issue ▫Single workstation failure	▫Responses provided during Normal Business Hours ▫Contact Client within 2 business hours through the ticketing system or phone ▫Begin work within 48 hours ▫Client and Secure Data will commit resources during Normal Business Hours to resolve the Incident ▫Secure Data will triage tickets in order of relative severity and urgency	**Phone or Email** 618-726-4040 support@securedatatech.com
Priority 4 (P4) Low	▫Issue is an inconvenience or annoyance but there are clear workarounds or alternatives ▫Overall impact is limited to one user *Examples:* ▫Voicemail password reset ▫Chat or email connectivity issues	▫Responses provided during Normal Business Hours ▫Contact Client within 4 business hours through the ticketing system or phone ▫Client and Secure Data will commit resources during Normal Business Hours to resolve the issue ▫Secure Data will triage tickets in order of relative severity and urgency	**Phone or Email** 618-726-4040 support@securedatatech.com
NOTE: Under no circumstances can resolution times be guaranteed, as involvement from third party vendors, product manufacturers, etc. may be required and are not entirely within Secure Data's control. Secure Data will make its best effort to resolve every Incident as quickly as possible. Instead, these SLAs provide response and work in progress times.			

2.3. Escalations. If Secure Data's initial classification of an Incident does not meet the Client's needs, an Incident may be escalated in multiple ways. To escalate an Incident's priority classification, the Client may take the following steps: To escalate a P3 or P4 Incident to a P2, Client can email support@securedatatech.com or call 618-726-4040 to request an increase in the priority level; or to escalate a P2 Incident to a P1, Client must call the support number at 618-726-4040.

3. SERVICE LEVEL AGREEMENT MEASUREMENT AND PENALTY

3.1. SLA Penalty. If an SLA is not achieved, a penalty in the form of a credit may applied to the Client's next invoice. SLA penalties may only be applied in relation to the Client's Subscribed Managed Services. Priority 4 (P4) Incidents are not eligible for SLA penalty calculations. Penalties will be applied according to the following calculations:

- Failure to successfully respond to 75% of P1-P3 Incidents within the SLA a calendar month qualifies for a Service Credit of 5% of the Client's monthly recurring charge.
- Failure to successfully respond to 60% of P1-P3 Incidents within the SLA in a calendar month qualifies for a Service Credit of 10% of the Client's monthly recurring charge.
- Failure to successfully respond to 50% of P1-P3 Incidents within the SLA in a calendar month qualifies for a Service Credit of 20% of the Client's monthly recurring charge.
- If Secure Data fails to successfully respond to 50% of P1-P3 Incidents for 4 or more months in a contract period, the Termination for Convenience fee outlined later in this document will be fully waived.

3.2. Service Credit Request. Service credits are the Client's sole and exclusive remedy for any failure to meet any Service Level. To request a service credit, the Client's account must be in good standing. Client may contact finance@securedatatech.com to report SLA failure(s). Such notice must be received within 30 calendar days of the conclusion of the month in which the SLA failure(s) occurred. Client waives any right to credits not requested within 30 days. Credits will be issued once validated by Secure Data and applied towards the Client's invoice no later than two (2) months following the service credit request. Client may not request credit if the Agreement term is 12 months or less. Any unused credits existing upon termination of the Agreement shall lapse without reimbursement to the Client. Client may not claim SLA violations for any Managed Services which Client is not Subscribed.

4. TERM AND TERMINATION

4.1. Initial Term and Renewals.

4.1.1. Onboarding. The Onboarding Term will begin on the Effective Date. During the Onboarding Term, Secure Data will perform the setup of the Subscribed Managed Services, and Client will provide information and access to its systems to complete such setup. The Onboarding Term will end at the earlier of (1) the date the setup of the Subscribed Managed Services is complete, or (2) 45 days after the Effective Date.

4.1.2. Initial Term. Notwithstanding anything contrary on the Order Form and any terms set forth therein, the Initial Term of this Agreement will commence upon the conclusion of the Onboarding Term and will continue for the term specified in the Order Form (the "Initial Term"). If not specified in the Order Form, the parties agree to an Initial Term of thirty-six (36) months.

4.1.3. Renewals. After the Initial Term, this Agreement will automatically renew, in its entirety, for the same duration as the Initial Term, inclusive of a 10% increase in the monthly contract amount, and subject to the then-current terms at the time of renewal. If either party would like to opt out of automatic renewal or reduce the scope of the Subscribed Managed Services, then such party must notify the other party no less than sixty (60) days prior to the expiration of the then-current Term.

4.2. Termination for Cause. This Agreement may be terminated by either party upon written notice if the other party: (a) becomes insolvent; (b) files a petition in bankruptcy; (c) makes an assignment for the benefit of its creditors; or (d) breaches any of its obligations under this Agreement in any material respect, which breach is not remedied within thirty (30) days following written notice to such party.

4.3. Termination for Convenience. Client may terminate this agreement for any reason ("Termination for Convenience"). If Client terminates this Agreement for any reason other than described above, the parties agree to a Termination for Convenience fee equal to 80% of the remaining Managed Services contract amount in the current Term.

4.4. Effect of Termination. Upon Termination of this Agreement, Secure Data will assist Client in the orderly termination of Subscribed Managed Services, including timely transfer of services to another designated provider as requested by Client. Client agrees to pay Secure Data the actual costs of providing such assistance.

5. ADDING, REMOVING, AND MODIFYING SERVICES. Secure Data scopes and bills for Subscribed Managed Services based on the number of Covered Devices and Covered Users in the Client's environment. Client's environment will be reviewed quarterly to ensure alignment between services rendered and billing provided to the Client. Bills will be incrementally adjusted to account for the true amount of users and devices in an environment as evaluated each quarter. No retroactive billing will be applied for increased device or user counts, and similarly no credits or refunds shall be provided for decreased device or user counts. Decreased device or user counts are subject to the Minimum Commitment outlined below.

6. MINIMUM COMMITMENT. Client agrees to a minimum commitment of eighty percent (80%) of the monthly contract amount included in the signed Order Form. If, as a result of adding, removing, or modifying services during the Term, the monthly billing would drop below eighty percent of the monthly contract amount included in the signed Order Form, Secure Data will bill Client for eighty percent of the original monthly contract amount. Exclusions to minimum commitment are Managed Cybersecurity, Managed Continuity, Managed Communication (as separately defined), and Managed Print (as separately defined), as the tools required to provide these services cannot be decreased during the contracted term.

7. OUT OF SCOPE SERVICES. Any services requested by Client that are not included within the scope of a Subscribed Managed Service will be considered Out-of-Scope Services and will be billed to Client as Time and Expense Matters at Secure Data's current published rates (see Schedule A).

8. UPDATES. Should Secure Data modify the terms and conditions in this Agreement, including updates related to the scope of its Managed Services offerings, Secure Data will post the amended terms at www.securedatatech.com/defaultterms and will update the "Last Updated Date" within the specific terms and provide notification of the change to Client. By continuing in its relationship with Secure Data, Client is indicating that it agrees to be bound by such updated terms. If any change is not acceptable to Client, Client must notify Secure Data within 30 days after the effective date of the change, at which time Client and Secure Data will remain governed by the terms in effect immediately prior to the change until the end of the then-current Agreement term. Any renewal of the Agreement will be renewed under the then-current terms, unless otherwise agreed in writing.

9. ATTORNEY'S FEES. Secure Data will have the right to collect from the Client its reasonable costs and necessary disbursements and attorneys' fees incurred in enforcing this Agreement.

10. DEFINITIONS. Capitalized terms and critical throughout this Agreement will be defined in the following priority: (1) as defined throughout this Agreement, (2) as defined below within this Section 9, or (3) or based on the most common IT industry understanding of such term.

Covered Device: Covered Device means any Client IT infrastructure equipment, appliance, gear, hardware, whether physical or virtual, which Client provides to Secure Data through onboarding checklists, access to network monitoring, or additions during the contract term. Covered Devices are generally identified by the device's IP address. At Client's request, devices may be excluded from coverage. The default classification of all devices known to Secure Data will be that of Covered Device unless Client directs Secure Data to remove a device from coverage. Client is responsible for informing Secure Data of any new or changed devices so that Secure Data may apply coverage for any subscribed services appropriately.

Covered User: Covered User means any Client employees or IT users. Covered Users are generally identified by the user's inclusion in Client's Active Directory. The default classification of all employees and IT users known to Secure Data will be that of Covered User unless Client directs Secure Data to remove a user from coverage. Client is responsible for informing Secure Data of any new or changed users so that Secure Data may apply coverage for any subscribed services appropriately.

End-Users: End-User means Client employees or IT users who use a assigned laptop, computer, workstation, or other devices provided by Client's IT team to perform their work function.

SCHEDULE A. Service Rates for Out-of-Scope Services

The following rates will apply for work that is requested outside the scope of Client's subscribed services with Secure Data. Secure Data will always seek authorization from a Client prior to performing work that falls outside the scope of this Agreement. Normal Business Hours in this Agreement are recognized as Monday through Friday, 8AM to 5PM, Central Standard/Daylight Time.

Work Description	Hourly Rate
Normal Business Hours: Pre-Scheduled	$250 Per Hour
Normal Business Hours: Emergency Response	$330 Per Hour
Outside Normal Business Hours: Pre-Scheduled	$275 Per Hour
Outside Normal Business Hours: Emergency Response	$375 Per Hour
Holiday Response (See Schedule B)	$500 Per Hour

Note: The rates above are current as of June 1, 2025.

SCHEDULE B. Secure Data Holidays

Secure Data observes the following holidays. During these days, Secure Data schedules minimal staff to meet the anticipated work and service requirements of maintaining 24x7x365 service for its managed services clients, while also permitting a maximum number of staff to observe the holiday. Accordingly, any Out-of-Scope Services which Client requests on a holiday listed below will be billed at the Holiday Response rate.

Secure Data affirms that the staffing and tools required to provide the applicable 24x7x365 coverage(s) included in Client's Subscribed Managed Services will not be impacted during these observed holidays.

- New Year's Day
- Memorial Day
- Independence Day
- Labor Day
- Veteran's Day
- Thanksgiving Day
- Day After Thanksgiving ("Black Friday")
- Christmas Day