1. Purpose

This Attachment B Service Level Agreement ("Agreement" or "SLA") is made between DYOPATH, LLC ("DYOPATH"), a Delaware limited liability company with its principal place of business at 1801 S. Meyers Rd, Suite 10, Oakbrook Terrace, Illinois 60181 and the Client pursuant to the terms and conditions of the Managed Services Agreement ("MSA") and applicable Attachment A entered into by Client and DYOPATH. DYOPATH and Client may be collectively referred to herein as the "Parties" and each may be referred to as a "Party".

1.1 Goals and Objectives

The purpose of this Agreement is to identify the Client's expectations and service performance levels ("Service Levels" or "SL") that will be provided by DYOPATH to the Client and the metrics or performance indicators by which the Service Levels will be measured. The Parties hereto may amend Attachment B from time to time upon written agreement of both Parties.

This Agreement defines the levels of service expected and delivered for IT Managed Services including Service Desk, Network Operations Center (NOC), Server and Storage Operations, Networked Device Monitoring, Reporting Requirements, Audit Support, Managed Security, Security Operations Center (SOC) Depot Services. It outlines response and resolution targets, and key performance indicators (KPIs) to ensure service quality and client satisfaction.

2. Service Level Targets

Metric	Target
Service Desk First Call Resolution	≥ 60%
Service Desk Incident and Service Request Compliance	≥ 90%
Service Desk Client Satisfaction	≥ 80%
Service Desk Average Speed to Answer Phone Calls	≥ 80% within ≤ 60 Seconds
Service Desk Abandon Rate for Phone Calls	≤ 6% after 60 seconds wait time

3. Service Level Management (SLM)

3.1. Service Request

A Service Request is a request from a user for access to IT services or information that does not involve unplanned service disruption.

Service Request Metrics

Priority	Description	Response Time	Resolution Time
1 – Critical	A request that impacts a core business function or many users, where delays or failure could lead to major disruption, financial loss, or regulatory risk.	30 mins	4 hours
2 – High	A request impacting important non-core functions or a limited group of users.	30 mins	8 hours

3 – Medium	Not urgent; mostly involves application access or hardware replacement.	2 hours	2 days
4 – Low	A request to change a minor configuration or add a new category.	4 hours	5 days

3.2. Incident Management Severity Levels & Response/Resolution Times

Severity	Description	Response Time	Resolution Time
1 – Critical	Business-critical outage or major system failure	30 mins	4 hours
2 – High	Significant issue affecting multiple users or services	30 mins	8 hours
3 – Medium	Single-user or non-urgent issues	2 hours	2 days
4 – Low	General inquiries or minor issues	4 hours	5 days

3.3.1 Vulnerability Severity Levels and Remediation Schedule (External Facing Devices)*

Severity	CVSS Score	Remediation
Critical	9.0 – 10.0	≤ 15 Days
High	7 – 8.9	≤ 30 Days
Medium	4 – 6.9	During the next scheduled patching cycle
Low	1 – 3.9	During the next scheduled patching cycle

3.3.2 Vulnerability Severity Levels and Remediation Schedule (Internal Facing Devices)*

Severity	CVSS Score	Remediation
Critical	9.0 – 10.0	≤ 15 Days
High	7 – 8.9	During the next scheduled patching cycle
Medium	4 – 6.9	During the next scheduled patching cycle
Low	1 – 3.9	During the next scheduled patching cycle

3.4. Proactive Default Patching Details*

Description/Category	Details
Monthly	Servers
Quarterly	Host, Edge Devices (Firewalls, SDWAN, etc.)
Semi-Annual	Routers, Switches, Load Balancers, SAN Switches, Wireless LAN Controllers, and Wireless Access Points
Patch Timing	10:00 PM local equipment time (unless otherwise stated)
Patch Version Policy	Vendor-designated stable versions only; no cutting-edge releases, only minor versions are included in service, major releases are handled as a project
Backup Verification	DYOPATH ensures latest backup is successful before patching
Pre-Patch Communication	DYOPATH communicates recommended patch level in advance
Post-Patch Validation	DYOPATH performs system health checks; client performs application-level testing

Post-Patch Support	DYOPATH provides next business day support for issues discovered in production

*** Requires patching service subscription on the devices to be patched**

3.5 Response, Resolution, and Priority Definitions:
For the most efficient and timely assistance, we advise reporting all critical and high-priority service requests or incidents by phone. This approach guarantees prompt engagement and ensures the quickest possible response.

The Incident and Request Response Time SL tracks the time elapsed from when an incident is reported and initially routed to a DYOPATH support group until it is assigned to an individual within the group. At this point, the assigned individual begins the processes of categorization, prioritization, and initial diagnosis of the incident.

The Incident and Request Resolution Time SL tracks the total time an incident remains assigned to a DYOPATH support group until it is resolved. This SL functions as a continuous timer throughout the lifecycle of an incident.

DYOPATH shall respond to and contain cybersecurity incidents within 2 hours of the response time listed above. Containment is defined in alignment with the SANS Incident Handling Process* as the implementation of short-term and recommendations for long-term strategies to limit the immediate impact of an incident and prevent further damage. Short-term containment includes isolating affected systems, blocking malicious activity, and stopping unauthorized access, while long-term containment involves advising on the application of measures such as patching vulnerabilities and securing compromised accounts to ensure the environment is stabilized. DYOPATH will provide documentation of containment measures taken in the ITSM and collaborate with the client to ensure effective communication and resolution of the incident.

Resolution indicates that the SOC has effectively contained the incident, but no further activities are in scope (eradication, remediation, etc.). For more in-depth Incident Response (IR), such as forensic investigation, malware analysis, hands-on support, onsite support, threat actor negations, etc., additional services or projects are required.

* SANS Incident Handling Process
- Preparation
- Identification
- Containment
- Eradication
- Recover
- Lessons Learned

Priority of an incident is derived based on two factors:

1) Impact – how extensive is the impact of the error or outage (individual, group, or company-wide)
    1 – Widespread: Enterprise-wide, entire business unit, or critical business service for entire organization

2 – Significant: Multiple departments, sites, or locations
3 – Moderate: Entire building/location or department wide if only one location
4 – Localized: Single or multiple users

2) Urgency – what is the urgency behind this incident (typically driven by the criticality of a system)
   1 – Critical: Multiple services affected or single critical service, no workaround available
   2 – High: Single service, no workaround available
   3 – Medium: Single service, workaround exists
   4 – Low: No impact to the availability of the service, redundancy, or acceptable workaround in place

Priority Matrix Table		**Impact**			
		1 – Widespread	2 – Significant	3 – Moderate	4 - Localized
Urgency	1 – Critical	Critical	Critical	Critical	High
	2 – High	Critical	High	High	Medium
	3 – Medium	High	Medium	Medium	Medium
	4 – Low	Medium	Low	Low	Low

3.6 Exceptions:
The incident and request resolution SLM will be paused under the following conditions:

- The ticket is assigned to a support group that is not managed by DYOPATH.
- The ticket is assigned to a DYOPATH-managed support group, but its status is set to 'pending', indicating that the support group is awaiting information or action from the customer, client staff, or an unmanaged third-party resource (e.g., a client vendor).

The incident and request resolution SLM will be excluded from reporting under these circumstances:

- The ticket is assigned to and resolved by a support group that is not managed by DYOPATH.

4. Client Requested Changes
All requests for moves, adds, changes, or deletions in the existing environment_are to be submitted to DYOPATH via a Service Request (via phone or e- Mail). The Service Desk will coordinate with appropriate resources to obtain an estimate of level of effort including time, materials, and potential costs dependent upon the applicable Attachment A. Once the approval has been received from the Client, the change will be scheduled and the Client notified of the planned completion date.

5. DYOPATH Infrastructure Changes
DYOPATH will use commercially reasonable efforts to minimize the impact of any change control and, when possible, schedule the change control to eliminate or minimize impact to the Client's Service.

DYOPATH will provide the Client with at least five (5) business days prior written notice before performing scheduled maintenance. For high impact changes, e.g., changes requiring an outage or service disruption, DYOPATH will provide the Client with at least ten (10) business days prior to written notice. All changes should occur during the agreed maintenance window (Example: Saturdays from 11:00 PM through Sunday 1:00 AM) unless previously agreed in writing by Client. If DYOPATH detects an issue within its infrastructure that could cause a disruption of service or significant degradation in service, DYOPATH will notify the Client of an Emergency Change (a change that must be implemented urgently to resolve a critical issue or prevent a significant business impact), that needs to be applied to the DYOPATH infrastructure. DYOPATH will provide the Client with as much notice as possible when performing Emergency Change controls. However, DYOPATH reserves the right to proceed with any change control if it is determined, by DYOPATH in its sole discretion, that a change control is necessary to maintain overall integrity of the Services.

6. Onboarding Timeline

Limiting SLs during the onboarding process helps ensure a smooth transition and enables DYOPATH to effectively adapt to the new environment. The following timelines take effect starting on the Commencement Date as defined in Section 1.16 of the MSA.

- 30 Days: Baseline data collection and SL planning.
- 60 Days: Fine-tuning of processes based on initial results.
- 90 Days: Full SL implementation and steady-state operations.

7. DYOPATH Standard Toolsets

DYOPATH standard toolset:

- RingCentral
- BMC Helix ITSM
- Auvik
- NinjaOne
- RADAR
- Managed Security Tools
    - SIEM Solution
    - Email Security Platform
    - Security Awareness, Training, and Darkweb Platform
    - Host Based Vulnerability Management Platform
    - Autonomous Pentesting
    - File Level Encryption and Data Management Platform

If Client does not use DYOPATH's standard toolset solutions with our default configuration, SL metrics may not apply.
If nonstandard DYOPATH toolsets solutions are used by Client, SL will be defined in the applicable Attachment A and DYOPATH must approve measurements, logic, reporting, and SLs.

8. Non-Standard Solutions
Nonstandard solutions that fall outside of the SLA Scope require custom Attachment A/SOW language. If there is a separate SLA in place, the agreement will supersede this SLA.

9. Contacts and Volume
Monthly Total Contact Volume: The Monthly Total Contact Volume is the agreed-upon number of tickets or contacts per month.

Normal Volume Variance: Normal Volume Variance is defined as being less than or equal to 6% of the calculated Monthly Total Contact Volume per day and less than or equal to 0.9% of the calculated Monthly Total Contact Volume per hour. If daily or hourly contacts exceed Normal Volume Variance, Service Level Agreements may be impacted for that month on a Best Effort basis.

- Example: Service Desk pricing is based on 300 contacts per month.
- Maximum Daily Contact Volume: 18
- Maximum Hourly Contact Volume: 3
- If Maximum Contact Volumes are exceeded within that time frame, SL will be “Best Effort” during those periods.