This Statement of Work ("SOW") is by and between Technology Information Group, a Pellera company ("SERVICE PROVIDER") and City of Medina ("CLIENT") and is subject to the terms and conditions of the **Master Services Agreement** dated January 29, 2026, which are incorporated herein by reference and made a part hereof (the "Agreement").

1. Services to be performed

A. SERVICE PROVIDER will provide CLIENT the subscription Services described in the attached Exhibit(s) in accordance with the terms set forth below.

B. Dependencies: SERVICE PROVIDER's performance of this SOW depends on CLIENT's timely performance of certain responsibilities listed in the attached Exhibit(s). In the event CLIENT or CLIENT's vendor(s) fail to perform the CLIENT responsibilities in a timely manner, SERVICE PROVIDER may charge CLIENT additional fees associated with schedule delays and the change control procedure may be invoked to adjust the delivery schedule and pricing.

2. Term of Service

A. The Term of this Service is identified in the **Pricing Summary** section below. If CLIENT does not wish to renew this SOW, CLIENT shall provide written notice of non-renewal to SERVICE PROVIDER at least sixty (60) days prior to the end of the Term. In the event CLIENT has not provided timely notice of non-renewal, upon completion of the Term, this SOW shall automatically renew for the same duration as the initial Term (each a "Renewal Term"). Fees for Services during each Renewal Term shall be equal to one hundred and five percent (105%) of the Service fees during the prior term. This SOW shall continue to automatically renew in accordance with the foregoing until CLIENT provides written notice of non-renewal. In the event CLIENT fails to issue payment during any Renewal Term, SERVICE PROVIDER reserves the right to terminate the SOW for non-payment upon written notice to CLIENT and seek collection for Services performed. **CLIENT acknowledges and agrees that the initial Term as well as any Renewal Terms are subject to the Termination requirements as outlined in the Master Services Agreement.**

B. Unless otherwise mutually agreed to, this SOW shall commence on the first business day of the month immediately following the date of the last party's execution and continue until CLIENT provides timely notice of non-renewal.

C. **NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT, THIS SOW IS NON-CANCELLABLE AND CLIENT SHALL NOT BE PERMITTED TO TERMINATE THIS SOW FOR CONVENIENCE. CLIENT SHALL ONLY BE PERMITTED TO TERMINATE THIS SOW WITHOUT CAUSE AFTER CLIENT PROVIDES PRIOR WRITTEN NOTICE TO SERVICE PROVIDER AND AFFORDS SERVICE PROVIDER A THIRTY (30) DAY PERIOD TO CURE THE DEFECT.**

3. Pricing Summary

A. The fees for the Services are set forth in the table below. Please see **Master Services Agreement** (referenced above) for details on definitions and calculation of charges. Pricing is valid for sixty (60) days from the date set forth in the header above and subject to applicable taxes:

Item #	Product Description	Term	Qty	Unit
1	MIS, 24x7 IOC Service 03-02-01-01-001-01	12	1	Included
2	MIS, Networking Services, Premium, Firewall, NGFW (Palo Alto) 03-02-03-01-179-01	12	1	Device
3	MIS, Networking Services, Premium, Switch 03-02-03-01-184-01	12	5	Device
4	MIS, Networking Services, Premium, WAP 03-02-03-01-187-01	12	4	Device

5	MIS, Physical Compute, Premium, x86 Type 1 Hypervisor Host 03-02-04-01-049-01	12	3	Device
6	MIS, Virtual Compute, Premium, VM 03-02-05-01-044-01	12	15	VM
7	MIS, Virtual Compute, Premium, Management Console 03-02-05-01-047-01	12	1	Instance
8	MIS, Operating System, Premium, Windows 03-02-09-01-043-01	12	12	Instance
9	MIS, Operating System, Premium, Linux 03-02-09-01-048-01	12	5	Instance
10	MIS, Database, Premium, MSSQL Server 03-02-10-01-047-01	12	2	Instance
11	MIS, Physical Compute, Premium, x86 (backup servers) 03-02-04-01-048-	12	2	Device
12	MIS, Data Protection Service, BUR, BYOL, Veeam 03-01-22-01-058-01	12	17	Device
13	MIS, Public Cloud, Azure, Foundation, Small 03-02-08-01-003-01	12	1	Environment
14	ECS, MSD, 24x7 Ticket Management Service [<=100], Shared-MX 01-01-02-03-004-01	12	50	Ticket
15	ECS, DDM Service, RMM (Patch and Application Deployment Only) [100-500] 01-01-04-01-083-01	12	55	Device
16	ECS, Microsoft Modern Workplace, Productivity, M365 + Hybrid Identity, Full User 01-01-11-01-006-01	12	55	User
17	MSS, Platform, EDR, BYOL, Managed, Sophos 02-03-02-01-028-01	12	1	Platform
18	MSS, Email Security, Mimecast, BYOL, Managed 02-01-07-01-037-01	12	1	Platform
19	MSS, Platform, SWG, Cisco, BYOL, Managed, Umbrella 02-03-02-01-139-01	12	1	Platform
20	MSS, MDR, Sophos, BYOL, Enhanced MDR Security Response By Pellera 02-03-02-01-157-01	12	55	Endpoint

	Total NRC	**Total Recurring**	**Total CV**
	$0.00	**$9,856.15**	**$118,273.80**

B. In the event of any cost increase (such as third party vendor increases in software or operating system licenses) that materially increases costs of delivering the Services to CLIENT, SERVICE PROVIDER will endeavor to provide written notice to CLIENT thirty (30) days and CLIENT shall then have ten (10) days from the date of the notification to dispute the cost increase, which the Parties agree to resolve in good faith. CLIENT shall then have thirty (30) business days from the date of SERVICE PROVIDER notice to dispute the cost increase in writing, and the Parties agree to resolve the dispute in good faith. No increase shall take effect and SERVICE PROVIDER shall not invoice at the increased rate unless

and until the Parties resolve the dispute in writing or CLIENT approves the increase in writing through the applicable change order process.

C. Notwithstanding anything to the contrary in Section 2. Term of Service - All funds for payment under this SOW are subject to the availability of any annual appropriation. In the event of non-appropriation of funds under the SOW, CLIENT may terminate the SOW, without termination charge or liability, on the last day of the then-current fiscal year or when the appropriation made for then-current year for the services/items covered by this Contract is spent, whichever occurs first. This non appropriation provision applies to the initial term and any renewal term. Termination under this provision is effective upon written notice from CLIENT as required in the Master Services Agreement and shall not be subject to any early termination fee, minimum contracted quantity charge, or other termination charge.

D. **CLIENT's execution of this SOW below authorizes SERVICE PROVIDER to invoice CLIENT for all fees contemplated in the table above, any additional fees incurred when utilizing the Service, and any automatic Renewal Term fees, and CLIENT agrees to pay such invoices in accordance with the terms specified herein, regardless of whether CLIENT has issued a corresponding Purchase Order ("PO") for such charges. CLIENT payment obligations are subject to CLIENT lawful procurement and payment requirements. SERVICE PROVIDER shall include any required purchase order or contract reference information on invoices if requested by CLIENT.**

4. Invoicing

A. Fees for the subscription are invoiced in accordance with the following:
   a. Non-Recurring Charges ("NRC") shall be invoiced in advance upon signature of the SOW.
   b. Recurring Charges shall be invoiced monthly in advance.

B. Services are to be performed remotely. Should onsite work be required, CLIENT and SERVICE PROVIDER will agree in advance of travel expenses being incurred. All travel and living expenses will be invoiced for actual expenses as incurred in accordance with the Agreement.

5. Additional Terms

The following terms apply to these Services and shall prevail over any conflicting terms or provisions in the attached Exhibit(s):

A. CLIENT agrees and acknowledges that SERVICE PROVIDER may subcontract a Service, or any part of it, SERVICE PROVIDER provides to CLIENT to SERVICE PROVIDER's affiliates, subsidiaries, or third party subcontractors selected by SERVICE PROVIDER.

B. **Notwithstanding anything in the Agreement to the contrary, CLIENT acknowledges and agrees that SERVICE PROVIDER may utilize resources from outside the United States to deliver the Services described herein. CLIENT's execution of this SOW below constitutes CLIENT's prior written consent to SERVICE PROVIDER's use of such resources unless otherwise stated herein.**

C. **SERVICE PROVIDER acknowledges that CLIENT is subject to the Washington Public Records Act, RCW chapter 42.56, and that records created, received, used, or retained by SERVICE PROVIDER in connection with the Services, including without limitation tickets, correspondence, logs, reports, security alerts, and invoices, may be public records. SERVICE PROVIDER shall promptly provide such records to CLIENT upon request in a usable format and shall reasonably cooperate with CLIENT to enable CLIENT to respond to public records requests and other lawful disclosure obligations. If SERVICE PROVIDER receives any public records request, FOIA request, subpoena, or other demand that references CLIENT or CLIENT records, SERVICE PROVIDER shall notify CLIENT promptly and shall not produce records absent CLIENT's written direction unless legally required. SERVICE PROVIDER shall not destroy, delete, or alter records relating to the Services that are subject to a CLIENT legal hold or retention requirement. SERVICE PROVIDER may identify information it believes is exempt from disclosure, but any confidentiality designation by SERVICE PROVIDER does not control CLIENT's disclosure determinations.**

D. **SERVICE PROVIDER shall reasonably cooperate with and support audits, inspections, and requests for information by CLIENT, the Washington State Auditor, and any other governmental auditor with jurisdiction, including by providing timely access to relevant records, reports, and documentation relating to the Services. This cooperation is not limited to one request per calendar year. SERVICE PROVIDER may require reasonable confidentiality protections for**

proprietary information, but such protection shall not unreasonably delay or prevent an audit. Audit cooperation under this section is included in the Services and shall not be billed as a separate fee unless CLIENT approves in writing in advance. For clarity, the SOC 2 report frequency limit as referenced in any other Pellera Terms applies only to SOC 2 reports and does not limit CLIENT audit rights or access to records.

6. Data Security

A. CLIENT acknowledges and agrees that no processing, creation, receipt, transmission, storage, or maintenance of personal data, including personal data of European Economic Area data subjects, is required for this SOW. Notwithstanding the foregoing, SERVICE PROVIDER remains responsible for actions taken with SERVICE PROVIDER's credentials to CLIENT systems in accordance with the Agreement. No category 3 or high data was defined in policy established in accordance with RCW 43.105.054 will be shared and thus, no data sharing agreement is required pursuant to RCW 39.26.340.

B. CLIENT is responsible for the overall security, content, and integrity of the information technology infrastructure including servers, databases, and backups and ensuring compliance with applicable regulatory requirements. CLIENT is also responsible for the access and security controls, backup and recovery procedures, and security procedures necessary to safeguard the integrity and content of databases and systems and prevent unauthorized access. SERVICE PROVIDER shall follow CLIENT information security policies and procedures provided in writing when accessing and managing CLIENT infrastructure components that are in scope for the Services. All support staff must be CJIS-certified through the Medina Police Department.

7. Tools

A. SERVICE PROVIDER may utilize various third party tools to perform the Services described herein, which may include hardware tools and/or software tools ("Third Party Tools"). With respect to SERVICE PROVIDER's use of Third Party Tools, CLIENT acknowledges and agrees that:

i. SERVICE PROVIDER will be using the Third Party Tools solely to facilitate the performance of Services;

ii. No right, title, or interest in, nor any license under, any copyright, patent, trade secret, trademark, mask work protection right, or any other intellectual property right is either granted to CLIENT or implied by the use of the Third Party Tools at CLIENT's facility or otherwise pursuant to this SOW. CLIENT acknowledges that the Third Party Tools used for the Services contain valuable, confidential information and trade secrets which CLIENT agrees to protect;

iii. No right is granted to CLIENT to make any copies of the Third Party Tools in any form;

iv. CLIENT will not modify, reverse assemble, reverse compile, or otherwise obtain or attempt to obtain the source code of the Third Party Tools, in whole or in part;

v. Upon completion or termination of SERVICE PROVIDER's services requiring the Third Party Tools, SERVICE PROVIDER will remove all copies of the Third Party Tool from CLIENT's systems; and

vi. In the event SERVICE PROVIDER utilizes hardware Third Party Tools, CLIENT shall bear all risk of loss or damage to the Third Party Tool, reasonable wear and tear excepted, upon delivery to the installation site until the Third Party Tool is returned to SERVICE PROVIDER's custody and control.

vii. CLIENT ACKNOWLEDGES AND AGREES THAT THE THIRD PARTY TOOLS ARE PROVIDED "AS IS" WITHOUT WARRANTY, INDEMNITY, MAINTENANCE, OR SUPPORT OF ANY KIND. NOTWITHSTANDING ANYTHING IN THE AGREEMENT TO THE CONTRARY, SERVICE PROVIDER DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED AND STATUTORY, WITH RESPECT TO ANY THIRD PARTY TOOLS ASSOCIATED WITH THIS SOW, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, COMPLETENESS, ERROR-FREE SERVICE, UNINTERRUPTED SERVICE, NON-INFRINGEMENT, TITLE AND NON-INTERFERENCE.

IN WITNESS HEREOF, CLIENT and SERVICE PROVIDER have caused this SOW to be executed by their duly authorized signatories.

City of Medina		Technology Information Group, a Pellera company	
Signature:	_____	Signature:	_____
Print Name:	_____	Print Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

Please Return Entire Document (All Pages) to:	Presented by:
Services Contracts Administrator Technology Information Group, a Pellera company EMAIL: jeff.bass@pellera.com	Dave Densley dave.densley@pellera.com Prepared by: Jeff Bass

Exhibit 1:

MANAGED SERVICE DESK (MSD)
SERVICE DESCRIPTION

REV 2025-10-30

1. SERVICE OVERVIEW

a) Managed Service Desk Services ("Level 1 Service" or "this Service") is a service line of Service Provider's End-User Client ("ECS") service family.

b) This Service provides 24x7 IT Service Desk management consisting of:

i. Minimum Monthly Quantity of tickets to be created by Client end users and managed by Service Provider.

ii. Service Provider's Level 1 supporters who resolve in-scope Level 1 tickets initiated by Client end users or Client systems. Such "Level 1 Resolvable" tasks shall be defined during the Transition-in Phase.

iii. Service Provider's Level 1 supporters who dispatch Service Desk non-resolvable Level 1 tickets for resolution to designated Level 1 supporters at Client location(s).

iv. Service Provider's Level 1 supporters who dispatch Level 2 tickets to Service Provider's Level 2 supporters when the resolution is in scope of "Level 2 Services" purchased from Service Provider by Client. A Level 2 Service shall have its own Service Description in a separate SOW.

v. Service Provider's Level 1 supporters who dispatch Level 2 tickets to Client's Level 2 supporters for resolution when out of scope of Level 2 Services.

vi. Service Provider can deliver this Service via a shared or a dedicated ITSM Tool owned by Service Provider or Client. See *Addendum MSD-1* for the specific choices for delivering this Service.

vii. Incident and Service Request Management processes are owned and managed by Service Provider. All other ITSM processes are owned by Client, unless mutually agreed to be in scope of this Service.

c) Client-specific details are defined in *Addendum MSD-1*:

i. Client Locations: list of Client's offices and plants where Service Provider is expected to deliver this Service to Client end users.

ii. Service Hours of Operation: times when this Service is available.

iii. Languages: list of languages to use to deliver this Service.

iv. Tools: list of tools from Service Provider and/or Client, which Service Provider shall need to deliver this Service.

v. Standard Hardware and Software End User Support List: list of standard Client end user hardware and software to be supported by this Service.

vi. Custom Hardware and Software End User Support List: list of custom Client end user hardware and software to be supported by this Service.

vii. Custom Service Levels: list of custom Client changes to or additions to Service Provider's ITSM Tool standard definitions, reporting, service levels, and other capabilities in this Service Description.

d) The detailed Steady State Service Responsibilities Matrix is defined in *Addendum MSD-2*.

e) The detailed Service Transition Management Responsibilities Matrices are defined in *Addendum MSD-3*.

f) Collectively, "this Service", "Level 1 Services" and "Level 2 Services" shall be referred to as "the Services."

g) Whenever Client purchases *Managed Service Desk Services*: (i) the content of this *Managed Service Desk Services Description* shall replace entirely the content of any *ITSM Foundation Services Description* addendum attached to existing Service Provider SOWs presented to Client, and/or (ii) the use of the term *"ITSM Foundation Services Description"* in any service description addendum attached to existing Service Provider SOWs presented to Client, shall be replaced with, *"Managed Service Desk Services Description"*.

2. SERVICE DELIVERY GOVERNANCE

a) Service Provider shall name one main point of contact ("Client Success Manager" or "CSM") and Client shall name one main point of contact ("Partner Success Manager" or "PSM") for the Services. The Client PSM and Service Provider CSM and shall deal with contract management, Client satisfaction, and service delivery escalations but not for day-to-day service management of the Services.

b) Service Provider shall name one technical lead ("Service Provider TL") and Client shall name one technical lead ("Client TL") who shall deal with the on-going ("Steady State") technical service management of the Services. Client TL reports to PSM and Service Provider TL reports to Service Provider CSM.

c) Client PSM, Service Provider CSM, and Client and Service Provider TLs are available during Normal Business Hours; however, they shall be available outside Normal Business Hours for escalations.

d) Depending on the nature and scope of the Services, one named person may be assigned more than one of the above roles or is responsible for more than one Service. This shall be determined during the Transition-In Phase.

e) During the Transition-In Phase, Client PSM and Service Provider CSM may mutually establish a "Services Review Meeting", the frequency and duration of which shall be proportional the scope of the Service purchased (e.g., weekly, monthly, quarterly). Client TLs and Service Provider TLs may mutually establish a "Service Delivery Meeting", the frequency and duration of which shall be proportional the scope of the Level 2 Services purchased by Client. Ad-hoc meetings shall be arranged and mutually agreed upon between Client PSM and Service Provider CSM or between Client TLs and Service Provider TLs according to urgency and need.

f) To mitigate risk and ensure audit and security compliance, and when Client is responsible for authorizing access to its network(s), systems, and applications to deliver the Services, Client shall establish individual user accounts for Service Provider supporters with sufficient administration privileges to perform the obligations under the Services. If Client is unwilling or unable to configure its network(s), systems, and applications as required, Client thereby accepts all liability resulting from misuse of shared user accounts.

3. SUPPORTER DELIVERY MODELS

a) This Service shall be performed using one of the following supporter delivery models, according to what is specified in the *Pricing Summary*. All Level 2 Services purchased by Client leverage (i) or shall be defined in the applicable SOW for that Service.

i. Remote (onshore or nearshore) shared and unnamed: Service Provider supporter is shared, unnamed, and located in Service Provider office to work on this Service non-exclusively. Available when ticket volume is less than 500 tickets per month.

ii. Remote (onshore or nearshore) shared and named: Service Provider supporter is shared, named, and located in Service Provider office to work on this Service non-exclusively. Available when ticket volume is equal to or greater than 500 tickets per month.

iii. Remote (onshore or nearshore) dedicated and named: Service Provider supporter is dedicated, named, and located in Service Provider office to work on this Service exclusively.

4. SERVICE TRANSITION MANAGEMENT

a) Transition-In:

i. The objective of the Transition-In Management is to either: (1) perform a greenfield or new implementation of the Services; or (2) perform a brownfield implementation by replacing Client's existing IT services with Services Provider's Services.

ii. The scope of the Services, including any outsourced business processes (e.g. password resets) shall be mutually agreed upon prior to executing the Transition-In Plan.

iii. Service Provider shall come up with a Transition-In Plan including key deliverables, milestones, a transition team who has knowledge of specific technologies, applications, and business processes required to take over support and to create or enhance existing documentation as appropriate. Transition shall be done remotely and/or on-site, as mutually agreed upon. Client must ensure the key contacts, knowledgeable subject matter experts and any business process documentation for Client's existing IT services are made available during the Transition-In Phase to ensure successful Go Live. Transition Management consists of four (4) phases: (1) Planning; (2) Knowledge Acquisition and Integration; (3) Shadow/Test; and (4) Steady State.

iv. Client shall coordinate and provide all available documentation and process information required to support the implementation of the Services, including shadowing & knowledge sharing session(s). Client shall cooperate actively and comprehensively in a UAT ("User Acceptance Test"). For a brownfield implementation, the Transition-In project assumes Service Provider shall be able to interact and transition in a collaborative way from the existing service provider or Client IT supporters, as applicable.

v. Client's internal ITSM processes may require alignment during Client Transition-In Phase with Service Provider's ITSM processes.

vi. Additional detail for Level 2 Services purchased by Client, if any, shall be found in the applicable SOWs.

b) Transition-Out:

i. The detailed Transition-in and Transition-out Responsibilities Matrices for this Service are defined in *Addendum MSD-3*.

ii. Additional detail for Level 2 Services purchased by Client, if any, shall be found in the applicable SOWs.

5. KNOWLEDGE MANAGEMENT

a) Client and Service Provider shall mutually build and maintain, as needed, a "Client Knowledge Management Repository" in the ITSM Tool or other designated system containing Client-specific documentation, processes, learnings, work instructions, and other related artifacts ("Knowledge Articles") related to delivering the Services. All Knowledge Articles, and revisions thereto, shall be approved by Client.

b) Service Provider documentation for delivering the Services that is not specific to Client are intellectual property and cannot be shared with Client.

c) If Service Provider is the ITSM Tool Owner, at its sole discretion, may publish Knowledge Articles through its ITSM Tool web-based portal for the purpose of providing self-service support to Client.

d) If Client is the ITSM Tool Owner, at its sole discretion, may publish Knowledge Articles through its ITSM Tool web-based portal for the purpose of providing self-service support to its end users.

6. ESCALATION MANAGEMENT

a) Ticket escalation shall be as follows: (i) if a ticket has not been responded to in a timely fashion, ticket initiator shall first escalate by requesting an update from assigned supporter via the ticket itself or directly with the assigned supporter; (ii) ticket initiator shall escalate to Client TL who shall then escalate to Service

Provider TL; (iii) Client TL shall escalate to Client PSM who shall escalate to Service Provider CSM; and (iv) Client PSM shall escalate to their manager who shall escalate to the manager of Service Provider CSM.

b) Managerial Escalation shall be as follows: The Client PSM can escalate to Service Provider CSM directly to establish direct communication until a ticket or Service issue is resolved without following the escalation process defined in paragraph a) above.

c) Major Incident Management is a subprocess combining Incident Management with Escalation Management and deals with the management of a P1 Incident that is having a major business impact on Service Provider or Client. Service Provider performs this process for all P1 Incidents generated from the Services. However, this process does not extend to include P1 Incidents generated by Client's IT assets and services that are not in scope of the Services, unless mutually agreed upon. Client PSM and Service Provider CSM shall align their respective Major Incident Management subprocesses during the Transition-In Phase.

7. PROBLEM MANAGEMENT

a) Whenever there is a P1 Incident or a repetitive Incident impacting the delivery of the Services, Service Provider shall initiate a Root Cause Analysis ("RCA"), the progress and results of which shall be communicated to Client in the form of corrective action(s) and a timeline for implementation. If the root cause is determined to be a Client responsibility, Client shall follow up internally and ensure corrective actions are promptly performed.

8. CHANGE MANAGEMENT

a) Service Provider performs this process for changes impacting the delivery of the Services. However, this process does not extend to change management activities related to Client's IT assets and services that are not in scope of those Services, unless mutually agreed upon. Furthermore, Client TL is responsible for obtaining the necessary change request information from Service Provider to follow its own change management processes. Service Provider PSM and CSM shall align their respective IT processes during the Transition-In Phase.

b) There are three types of change: (i) "**Contractual Change**" adds a new Service, decommissions an existing Service, or modifies contractual terms. This type of change shall be initiated pursuant to Client and Service Provider's sales order processes; (ii) a "**Standard Change**" refers to a low risk and low impact change to an existing Service for which the approach has an accepted and documented procedure and is pre-approved; (iii) a "**Normal Change**" refers to a change that must follow the complete change management process. Normal changes are often categorized according to risk and impact to the business. A "**Minor Normal Change**" is a low risk and low impact change, a "**Significant Normal Change**" is medium risk and medium impact change, and a "**Major Normal Change**" is high risk and high impact change. All Normal Changes shall proceed through all steps of the change management process and those that are categorized as a Significant or Major Normal Change shall be reviewed by Client and Service Provider respective **Change Advisory Boards (CAB's)**. An "**Emergency Change**" is a Normal Change that must be implemented before the next regularly scheduled CAB meeting due to its high risk and high impact on the security and/or availability of a Service. A "**Maintenance Change**" is a planned Normal Change that is periodically initiated by Service Provider to ensure the ongoing security and/or availability of a Service. Client shall be informed of the Maintenance Change in advance via "Maintenance Notices". When a Maintenance Change requires that a Service, or portion thereof, to be orderly turned off to perform the maintenance, it is referred to as a "**Standard Maintenance Downtime**". When a Maintenance Change is reactive, unplanned, critical, and urgent and requires that a Service, or portion thereof, to be orderly turned off to perform the maintenance it is referred to as a "**Emergency Maintenance Downtime**".

c) Normal Changes require coordination between Client and Service Provider and may include but is not limited to: (i) change risk and business impact assessment; (ii) execution, validation, and communication plan; (iii) cancellation, rollback, and reschedule plan; (iv) approvals/authorization by relevant stakeholders; and (v) date, start time, and expected duration.

d) Client-initiated Standard Changes and Service Provider- or Client-initiated Normal Changes shall be documented via the creation of a Service Request ticket in the ITSM Tool. Thereafter, a formal Service Provider Change Request ticket will be created to document approval and execution.

e) A change to a Service is assumed to be performed during Normal Business Hours, unless the change risk and business impact assessment indicates that the change must be performed outside Normal Business Hours.

f) If a change is complex, requiring the coordination of multiple resources over an extended period (i.e., weeks and months), Service Provider CSM may assign a Service Provider Project Manager ("Service Provider PM"). The Service Provider PM shall manage the project delivery details in coordination with Service Provider CSM and Client PSM. This may include the establishment of a one regular project meeting, the frequency and duration of which shall be proportional to the scope of the project.

9. CONTINUAL SERVICE IMPROVEMENT

a) Continual service improvement for the delivery of the Services shall be implemented by Service Provider's Quality Assurance Program in conjunction with its Problem Management process.

b) Client is responsible for the continual service improvement of any processes and tools owned by Client and are used by Service Provider to deliver the Services.

c) Service Provider uses "Shift-Left Best Practices" for the delvery of the Services. This means Service Provider's Level 2 support activities may be shifted to Service Provider's Level 1 support, and to Level 0 support (self-service). Shift-Left reduces ticket resolution times and increases Client satisfaction.

d) Shifting Client's out-of-scope Level 2 support activities to Service Provider's Level 1 support requires a detailed analysis of which Level 2 support tickets meet the mutually agreed upon definition of "Level 1 Resolvable". Client shall then provide work instructions for Service Provider to follow as well as sufficient training and privileges to resolve such tickets.

e) Service Provider may record all inbound and outbound phone calls for quality assurance purposes. Client may submit a request to review one or more individual call recordings. However, the total number of individual call recordings for review per calendar month that are included in the Service shall be 5% of the minimum contracted monthly ticket count per calendar month, with no less than 25 and no higher than 100 ("Included Individual Call Recording Review Count"). Any individual call recordings for review that are more than the Included Individual Call Recording Review Count per calendar month shall be separately billable

according to the rate card documented in the *Pricing Summary*, or according to the current rate at the time of the request, when not documented in the *Pricing Summary*.

10. SERVICE DESK MANAGEMENT

a) By default, Service Provider is the "ITSM Tool Owner" and provisions the Service Desk ticket management tool and the associated Communication Channels (collectively "ITSM Tool"), unless otherwise defined in *Addendum MSD-1*.

b) If Service Provider is the ITSM Tool Owner, Service Provider's ITSM Tool functionality, including the defined ticket states, priorities and service levels are accepted as-is.

c) If Service Provider is the ITSM Tool Owner, user license types assigned to Client end users shall be billed back to Client if defined as such in the *Pricing Summary*. There are three (3) ITSM Tool user license types: (i) "**Regular Users**" who manage only their tickets (i.e. create, view, and update tickets, including change the ticket state from 'With Client' to 'In Progress' or request a change in the state of the ticket via a ticket update); (ii) "**Key Users**" who can view and manages all tickets for Client; and (iii) "**IT Users**" who can view all tickets, assign to support groups, and resolve tickets. The assignment of ITSM Tool user license types to Client and Service Provider supporters shall be defined during the Transition-in Phase.

d) If Client is the ITSM Tool Owner, as defined in *Addendum MSD-1,* Service Provider's standard definitions, reporting, service levels, and other capabilities, as detailed in Section 11 (Incident and Service Request (Ticket) Management) and Section 12 (Service Level Management) shall be adjusted to document what can be fully supported by Client's ITSM Tool. Any configuration or development changes to Client's ITSM Tool to support Sections 11 and 12 are separately billable and not included in this Service

e) The ITSM Tool Owner shall be responsible for all ITSM Tool licensing, accessibility, availability, continual service improvement, and overall maintenance of the ITSM Tool. If the ITSM Tool is replaced or is subject to a major upgrade, ITSM Tool Owner shall be responsible for all project-related costs to effect the change.

f) Where supported by the ITSM Tool, Client may specify which of its end users are "VIP". This alerts Service Provider Level 1 supporters to provide 'white glove' treatment to a VIP end user with the necessary attention and urgency above that provided for Regular Users. Client shall provider a list of VIP users.

10.1. SERVICE HOURS

a) "24x7" or "Service Hours" shall be defined as 24 hours for every day of the year.

b) "9x5" or Normal Business Hours" shall be defined as Monday-Friday from 8AM to 5PM CT, excluding Client and Service Provider holidays for the delivery of Level 1 and Level 2 Services.

c) Any Service-, zone-, or region-specific "Normal Business Hours" in-scope for Client shall be defined in *Addendum MSD-1*.

10.2. COMMUNICATION CHANNELS

a) Service Provider supporters shall be contacted by Client end users using one or more of the following four ITSM Tool "Communication Channels": (i) toll-free phone number; (ii) self-service portal; (iii) support email; and (iv) support chat. If at least one channel is available, Service shall be considered available.

b) The ITSM Tool Owner shall be responsible for the Communication Channels. Client and Service Provider shall integrate Communication Channels during the Transition-In Phase so that Service Provider supporters can work effectively with Client end users.

c) Client end users shall only interface with Service Provider supporters using the defined Communications Channels. All Incidents and Service Requests shall be documented via a ticket inside the ITSM Tool. Service Provider supporters cannot manage ticket communication or control and measure service level performance when communication is outside the defined Communication Channels.

d) Client end users may request direct contact with the assigned Service Provider supporter ticket owner if needed or by calling the toll-free phone number.

11. INCIDENT AND SERVICE REQUEST (TICKET) MANAGEMENT

11.1. INCIDENT TICKET DEFINITION

a) A ticket created for the Services when it is no longer functioning as expected due to an unplanned or unexpected issue is called an "Incident". This is also known as a "break/fix" issue.

11.2. SERVICE REQUEST TICKET DEFINITION

a) A ticket created for a Service to request: (i) information about a Service; (ii) to perform a task that is included in a Service (i.e., no additional billing if Client's contractual limits have not been reached); or (iii) to perform a task that is not included in a Service (i.e., billable), and shall be called a "Service Request". A Service Request that requires a Contractual Change or is billable (which is not already contractually pre-approved) shall be subsequently referred to as a "Billable Service Request". The Service Provider CSM shall follow up with Client PSM prior to any execution. A Service Request that is a non-billable Standard Change shall continue to be referred to as a Service Request. It shall be documented and executed using the existing Service Request ticket. A Service Request that is a non-billable Normal, Maintenance, or Emergency Change shall be referred to as a "Change Request". It shall be documented, approved, and executed using a Change Request Ticket that implements Service Provider's formal change management process.

b) Service Requests, which are Standard Changes, are pre-approved by Client for delivery and subsequent additional billing when contractual quantity maximums, if defined the applicable SOW, are exceeded.

c) Service Requests that are also Normal Changes require Client approval prior to delivery and subsequent additional billing when contractual quantity maximums are exceeded, if defined in the applicable SOW.

11.3. TICKET VOLUMES

11.3.1. LEVEL 1 SERVICE TICKET VOLUMES

a) The Minimum Monthly Quantity shall be defined as the minimum total count of tickets included in this Service without additional fees. The Minimum Monthly Quantity and the additional fee per ticket above the Minimum Monthly Quantity shall be documented in the *Pricing Summary*.

b) The Actual Monthly Quantity consumed each calendar month shall be calculated as follows:

i. Tickets handled by Service Provider Level 1 supporters which are: (i) in scope of this (Level 1) Service for resolution; or (ii) dispatched to Client's Level 2 supporters for follow up and resolution are included.

ii. If Service Provider is the ITSM Tool Owner, the maximum total count of tickets included in the Service Fee that may be created per calendar month and handled entirely by Client Level 2 supporters without any interaction with Service Provider Level 1 or Level 2 supporters shall be equal to the total number of active Resolver User Licenses assigned to Client supporters in each calendar month multiplied by two hundred and fifty (250). If this actual ticket count exceeds two hundred and fifty (250), the difference is included.

iii. Tickets handled by Service Provider Level 1 supporters in support of Service Provider Level 2 Services are not included.

iv. Tickets generated automatically by systems (e.g., alert tickets) whether by Client or Service Provider are not included. However, such tickets may be subject to the limitations and additional billing requirements as detailed in paragraph (b)(ii) above; or according to limitations and additional billing requirements detailed the service descriptions of the Level 2 Services purchased by Client.

c) Service Overage and Fee Calculations. The following method shall be used to determine whether a Service Overage and Fee applies or not. The Service Overage is equal to the Actual Monthly Quantity measured over three (3) consecutive calendar months minus the Minimum Monthly Quantity x 3. If the Service Overage is negative or zero, no Service Overage Fee shall be invoiced. If the Service Overage is greater than zero, the Service Overage Fee shall be the calculated as the Service Overage multiplied by the additional fee per ticket in the *Pricing Summary*.

d) Minimum Monthly Quantity Adjustments. The Minimum Monthly Quantity in the *Pricing Summary* was estimated based on information provided by Client to Service Provider prior to delivery. Service Provider bases its capacity and resource planning on those quantities to ensure the delivery and performance of this Service. The Minimum Monthly Quantity shall not be reduced for the initial three (3) calendar months after delivery. However, if the Service Overage during the initial three (3) calendar months after delivery is greater than zero, Client shall pay the resulting Service Overage Fee. Thereafter, the parties agree to review the Service Overage for each subsequent three (3) calendar month period. If the Service Overage is consistently 10% above or below the Minimum Monthly Quantity, both parties agree to adjust (up or down) this Service's ongoing Minimum Monthly Quantity to best reflect the expected monthly consumption of this Service going forward. If an adjustment needs to be made that will increase the Minimum Monthly Quantity, and Client does not agree to it, the Service Level Credits shall be waived until the adjustment is agreed to.

11.3.2. LEVEL 2 SERVICE TICKET VOLUMES

a) The number of tickets created automatically via Service Provider's monitoring tool in support of Level 2 Services purchased by Client are included in this Service.

b) The number of tickets manually created by Client to request support for Level 2 Services purchased by Client are included in this Service, unless limitations are documented in the Service Descriptions for those Level 2 Services.

c) The number of autogenerated tickets by Client are not included in this Service and are billed separately, unless mutually agreed upon.

11.4. TICKET PRIORITY

a) Definitions

State	Definition
P1 - CRITICAL	Service unavailable; high business disruption; no workaround
P2 - HIGH	Service partially available; high business disruption; possible workaround Service unavailable; medium business disruption; possible workaround
P3 - MEDIUM	Service mostly available; high business disruption; possible workaround Service partially available; medium business disruption; possible workaround Service unavailable; low business disruption; possible workaround
P4 - LOW	Service mostly available; medium business disruption; possible workaround Service mostly available; low business disruption; possible workaround Service partially unavailable; low business disruption; possible workaround

b) Ticket initiator shall establish the priority of each ticket. A Service Provider supporter may engage with the ticket initiator to mutually agree to adjust the priority to align with the above definitions or to align with the current urgency of the ticket during its lifecycle.

c) P1 and P2 tickets are reserved for Incidents only.

d) For P3 and P4 tickets, the Service Level Clock is paused outside Normal Business Hours when the ticket is in the 'In Progress' state.

e) P1 and P2 tickets shall be subject to the Major Incident Management subprocess. Client shall always use the toll-free phone number to create such tickets to reduce the delay in the creation and processing of the ticket. If a P1 or P2 Incident ticket is submitted by any other method, it shall be treated as a P3 ticket until the priority is adjusted using the toll-free phone Communication Channel. The ticket initiator (or their assigned delegate) shall be available for callbacks and follow-ups from a Service Provider supporter to ensure smooth handling and communication concerning the Incident after it is reported.

f) Service Request tickets shall be assigned a P4 by default. Urgent Service Request tickets may be assigned a P3 and then escalated separately by Client TL to Service Provider TL to determine if a quicker response time or delivery time can be met or not.

11.5. TICKET STATES

a) Definitions

State	Definition	Service Level Clock
Open	Ticket has been created but has not been assigned to a Service Provider or Client supporter for resolution	Running
Assigned	Ticket has been assigned to a Service Provider or Client supporter for resolution	Running
In Progress	Ticket has been assigned to Service Provider and the assignee is actively working towards its resolution	Running
With Client	Ticket has been assigned to Client end user for further input or validation	Paused
With Vendor	Ticket requires further input or validation from vendor	Paused
Postponed	Ticket is placed on hold until a future date and time when it makes the most sense to continue processing the ticket	Paused
Solved	Ticket is solved based on feedback from Client end user; but can be reopened if needed before it is permanently closed	Stopped
Closed	Ticket is closed and can't be reopened. This is automated and occurs after ticket has been solved	Stopped
Canceled	Ticket is canceled because it is no longer needed	Stopped

b) Each ticket may have nine (9) possible states, depending on its lifecycle towards resolution. The Service Level Clock is used to measure the processing time of Service Provider supporters.

12. SERVICE LEVEL MANAGEMENT

12.1. SERVICE LEVEL TYPES

a) A Service Level Agreement ("SLA") is an external Service Level that is central to the measurement and maintenance of quality. They are reported via the Standard Monthly Service Level Report. Whenever an SLA Service Level is not met, Client PSM shall initiate a Service Level Credit Claim and a Service Level Credit shall be issued to Client. This ensures a financial incentive to Service Provider to meet or exceed the SLA Service Level.

b) A Service Level Object ("SLO") is an external Service Level that is considered very important to the measurement and maintenance of quality. They are reported via the Standard Monthly Service Level Report. No Service Level Credit is issued when the SLO Service Level is not met.

c) A Key Performance Indicator ("KPI") is an internal Service Level that indirectly supports the quality-of-service measurements for SLA and SLO Service Levels. They are not reported via the Standard Monthly Service Level Report. No Service Level Credit is issued when the KPI Service Level is not met.

d) For SLA and SLO Service Levels that have not been met, the Problem Management process shall be initiated to determine the root cause and corrective actions, if any. The root cause and corrective actions for SLA and SLO Service Level Targets that have not been met shall be communicated by Service Provider CSM to Client PSM.

12.2. SERVICE LEVELS

12.2.1. CLIENT SATISFACTION RATE

a) Definition

Service Level	Value	Target	Service Hours	Type	Incident Ticket	Request Ticket	Calc. Method	Met Criteria
Client Satisfaction Rate	Satisfied	98%	24x7	SLO	Yes	Yes	Rate	Above

b) Client Satisfaction Rate is a default Service Level for all Service Provider Level 1 and Level 2 Services.

c) Client Satisfaction per ticket is measured when the ticket initiator responds to the ticket satisfaction survey with "satisfied" or "dissatisfied". The ticket initiator may also provide additional written comments. If the ticket initiator does not provide a ticket satisfaction survey response, the survey response is assumed to be "satisfied".

d) Client Satisfaction Rate is measured as a percentage based on the total tickets where the survey response is defined as "satisfied" in the Reporting Period divided by total tickets multiplied by 100.

e) The Client PSM shall periodically encourage ticket initiators to provide a service rating for each ticket to ensure representative feedback. Service Provider's Quality Assurance Program is used to review all comments with follow up with the ticket owners for additional information on negative comments. A summary is provided to Service Provider CSM who may discuss with Client PSM, as needed.

12.2.2. LEVEL 1 SERVICES

a) When the Minimum Monthly Quantity of Tickets in the SOW is greater than five hundred (500) and the Service Level Type is SLO, the type shall change to SLA.

b) In any given month, if the Actual Monthly Quantity exceeds the Minimum Monthly Quantity by more than 500 tickets, or if it exceeds the Minimum Monthly Quantity by more than 10%, the Service Level Agreement (SLA) will convert to a Service Level Objective (SLO) for that month.

12.2.2.1. LEVEL 1 TICKET RESPONSE TIME BY PRIORITY

a) Definitions

Service Level	Value <=	Target	Service Hours	Type	Incident Ticket	Request Ticket	Calc. Method	Met Criteria
P1 – CRITICAL Response Time	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P2 – HIGH Response Time	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P3 – MEDIUM Response Time	4 hours	90%	24x7	SLO	Yes	Yes	Value	Above
P4 – LOW Response Time	8 hours	90%	24x7	SLO	Yes	Yes	Value	Above

b) Level 1 Ticket Response Time by Priority is a default Service Level for Level 1 Services only.

c) Level 1 Ticket Response Time by Priority is measured automatically per Level 1 Incident ticket (P3 to P4) and per Level 1 Service Request ticket (P3 and P4) based on its initial priority from creation date and time of the ticket until the date and time the ticket is first moved from 'Open' state to 'In Progress' state - which occurs upon the ticket's first assignment to the relevant Level 1 supporter.

d) If a response time is desired that is less than the Service Level Value above, ticket initiator shall use the toll-free phone number Communication Channel.

12.2.2.2. LEVEL 1 TICKET UPDATE INTERVAL BY PRIORITY

a) Definitions

Service Level	Value <=	Target	Service Hours	Type	Incident Ticket	Request Ticket	Calc. Method	Met Criteria
P1 – CRITICAL Update Interval	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P2 – HIGH Update Interval	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P3 – MEDIUM Update Interval	24 hours	90%	24x7	KPI	Yes	Yes	Value	Above
P4 – LOW Update Interval	24 hours	90%	24x7	KPI	Yes	Yes	Value	Above

b) Level 1 Ticket Update Interval by Priority is a default Service Level for Level 1 Services only.

c) Ticket Update Interval by Priority is measured automatically per Level 1 Incident ticket (P3 to P4) and Level 1 Service Request ticket (P3 to P4) as the average of the interval times between ticket updates for all Service Provider supporter updates to the ticket while in 'In Progress' state.

d) Level 1 supporters proactively request updates from the Level 1 supporters currently assigned to a ticket.

12.2.2.3. LEVEL 1 TICKET RESOLUTION TIME BY PRIORITY

a) Definitions

Service Level	Value <=	Target	Service Hours	Type	Incident Ticket	Request Ticket	Calc. Method	Met Criteria
P1 – CRITICAL Resolution Time	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P2 – HIGH Resolution Time	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P3 – MEDIUM Resolution Time	4 hours	90%	24x7	SLO	Yes	Yes	Value	Above
P4 – LOW Resolution Time	16 hours	90%	24x7	SLO	Yes	Yes	Value	Above

b) Level 1 Ticket Resolution Time by Priority is a default Service Level for Level 1 Services only.

c) Level 1 Ticket Resolution Time by Priority is measured automatically per Level 1 Incident ticket (P3 to P4), Level 1 Service Request ticket (P3 to P4) based on each ticket's initial priority as the sum of the Service Level Clock times recorded for each ticket.

d) Level 1 tickets are those that are in scope of this Service to be resolved by Level 1 supporters. All other tickets are dispatched to Level 2 Support Teams (see next Service Level).

12.2.2.4. LEVEL 1 CALL ANSWER PERFORMANCE & ABANDONMENT RATE

a) Definitions

Service Level	Value <=	Target	Service Hours	Type	Incident Ticket	Request Ticket	Calc. Method	Met Criteria
Call Answer Performance	30 seconds	85%	24x7	SLO	Yes	Yes	Value	Above
Call Abandonment Rate	N/A	5%	24x7	SLO	Yes	Yes	Rate	Below

b) Call Answer Performance is a default Service Level for Level 1 Services only.

c) Call Answer Performance is automatically measured as a percentage based on the total inbound calls received by the Automatic Call Distributor (ACD) system until when a live Service Provider supporter talks to a caller below the given Value. This includes the time each caller spends on the phone waiting, either while the phone rings or while in a queue (a.k.a. while being on hold). However, the time that the caller spends interacting with an Interactive Voice Response (IVR) system is not included.

d) Call Abandonment Rate is automatically measured as a percentage based on the total inbound calls that were abandoned before speaking to a Service Provider supporter in the Reporting Period divided by total inbound calls multiplied by 100.

12.2.2.5. LEVEL 1 GROSS FIRST CONTACT RESOLUTION RATE

a) Definitions

Service Level	Value	Target	Service Hours	Type	Incident Ticket	Request Ticket	Calc. Method	Met Criteria
Gross First Contact Resolution Rate	N/A	60%	24x7	SLO	Yes	Yes	Rate	Above

b) This is a default Service Level for Level 1 Service only.

c) Gross First Contact Resolution Rate is measured automatically as a percentage based on the total number of tickets in the Reporting Period for all Level 1 tickets resolved correctly on the first attempt divided by the total number of total tickets received in the Reporting Period multiplied by 100. This Service Level provides a measurement for determining Shift-Left success over time because the percentage should increase as more IT activities are moved from Client or Service Provider Level 2 to Level 1. Moving Level 1 tasks to Level 0 tasks should reduce tickets counts, thus allowing Service Provider supporters to deal with more Level 2 support activities.

12.2.2.6. ADDITIONAL LEVEL 1 SERVICE LEVELS

a) None. Additional Service Levels, if any, shall be documented here.

12.2.3. LEVEL 2 SERVICES

12.2.3.1. LEVEL 2 TICKET RESPONSE TIME BY PRIORITY

a) Definitions

Service Level	Value <=	Target	Service Hours	Type	Incident Ticket	Request Ticket	Calc. Method	Met Criteria
P1 – CRITICAL Response Time	15 minutes	95%	24x7	SLA	Yes	N/A	Value	Above
P2 – HIGH Response Time	30 minutes	95%	24x7	SLA	Yes	N/A	Value	Above
P3 – MEDIUM Response Time	4 hours	90%	24x7	SLO	Yes	Yes	Value	Above
P4 – LOW Response Time	8 hours	90%	24x7	SLO	Yes	Yes	Value	Above

b) Level 2 Ticket Response Time by Priority is a default Service Level for Level 2 Services only.

c) Tickets are dispatched by a Level 1 supporter to a Level 2 supporter for resolution when in scope of a Level 2 Service; and to a Client Level 2 supporter for resolution when not in scope of a Service Provider Level 2 Service.

d) When a Level 2 ticket is dispatched to a Client Level 2 supporter, the Level 2 Incident ticket (P1 and P2) Service Level Type is SLO.

e) Level 2 Ticket Response Time by Priority is measured automatically per Level 2 Incident ticket (P1 to P4) and per Level 2 Service Request ticket (P3 to P4) based on its initial priority from creation date and time of the ticket until the date and time the ticket is first moved from 'Open' state to 'In Progress' state - which occurs upon the ticket's first assignment to the relevant Level 2 supporter.

f) If a response time is desired that is less than the Service Level Value above, ticket initiator shall use the toll-free phone number Communication Channel.

12.2.3.2. LEVEL 2 TICKET UPDATE INTERVAL BY PRIORITY

a) Definitions

Service Level	Value <=	Target	Service Hours	Type	Incident Ticket	Request Ticket	Calc. Method	Met Criteria
P1 – CRITICAL Update Interval	30 minutes	95%	24x7	KPI	Yes	N/A	Value	Above

P2 – HIGH Update Interval	60 minutes	95%	24x7	KPI	Yes	N/A	Value	Above
P3 – MEDIUM Update Interval	24 hours	90%	24x7	KPI	Yes	Yes	Value	Above
P4 – LOW Update Interval	24 hours	90%	24x7	KPI	Yes	Yes	Value	Above

b) Level 2 Ticket Update Interval by Priority is a default Service Level for Level 2 Services only.

c) Ticket Update Interval by Priority is measured automatically per Level 2 Incident ticket (P1 to P4) or Level 2 Service Request ticket (P3 to P4) as the average of the interval times between ticket updates for all Service Provider supporter updates to the ticket while in 'In Progress' state.

d) Level 1 supporters proactively request updates from the Level 2 supporter currently assigned to a ticket.

12.2.3.3. LEVEL 2 TICKET RESOLUTION TIME BY PRIORITY

a) Definitions

Service Level	Value <=	Target	Service Hours	Type	Incident Ticket	Request Ticket	Calc. Method	Met Criteria
P1 – CRITICAL Resolution Time	4 hours	95%	24x7	KPI	Yes	N/A	Value	Above
P2 – HIGH Resolution Time	8 hours	95%	24x7	KPI	Yes	N/A	Value	Above
P3 – MEDIUM Resolution Time	24 hours	90%	24x7	KPI	Yes	Yes	Value	Above
P4 – LOW Resolution Time	40 hours	90%	24x7	KPI	Yes	Yes	Value	Above

b) Level 2 Ticket Resolution Time by Priority is a default Service Level for Level 2 Services only.

c) Ticket Resolution Time by Priority is measured automatically per Level 2 Incident ticket (P1 to P4) or Level 2 Service Request ticket (P3 to P4) based on its initial priority as the sum of the Service Level Clock times recorded for each ticket.

12.2.3.4. ADDITIONAL LEVEL 2 SERVICE LEVELS

a) Additional Level 2 Service Levels, if any, shall be documented in the applicable SOW for that Level 2 Service.

12.2.4. SERVICE LEVEL REPORTING

a) The Service Level Reporting period is a calendar month ("Reporting Period") for the purposes of determining if SLA or SLO Service Levels have been met or not. The Standard Service Level Report shall also be issued weekly during the Reporting Period to facilitate trend analysis during the current month as well as on a month-to-month basis to facilitate trend analysis, whereby negative trends are subject to Problem Management and Continuous Service Improvement for a rolling twelve (12) month period.

b) The first Standard Monthly Service Level Report shall be issued in the second or third calendar month after the Go Live Date of a Service and shall cover the first whole calendar month after a Service Go Live Date. The "Service Go Live Date" is the date when the Steady State phase for a Service commences, which is the date after the Transition-In Phase terminates. During the first three (3) calendar months after Service Go Live Date, Service Level Credits shall not apply.

c) Service Level Measured % Calculation ("Calc. Method"):

i. Availability: For each system contributing to the Service Level during the Reporting Period, the per system Service Level Measured% is equal to (the number of minutes in the Reporting Period minus the Unplanned Downtimes that are the responsibility of Service Provider) divided by the number of minutes in the Reporting Period multiplied by 100. Therefore, Planned Downtimes and Unplanned Downtimes that are the responsibility of Client are not considered downtimes for the purposes of the calculation. The availability measurement is performed each minute. If there is more than one system contributing to the Service Level, the final Service Level Measured% shall be the average of Service Level Measured% of all the systems measured.

ii. Average: For all items measured during the Reporting Period, the Service Level Measured Value is equal to the average of all the actual values for all items relevant to the Service Level. If the Service Level Measured Value is less than or equal to the Service Level Value, then the Service Level Measured% is equal to 100. Otherwise, the Service Level Measured% is equal to (100 minus (Service Level Measured Value minus Service Level Value)) divided by the Service Level Value multiplied by 100.

iii. Rate: For all items measured during the Reporting Period, the Service Level Measured % is equal to the number of items relevant to the Service Level divided by the number of all items multiplied by 100. If the number of all items for a Service Level equals zero, the Service Level Measured % shall be marked as 'N/A'.

iv. Value: For all items measured during the Reporting Period, the Service Level Measured % is equal to the number of items relevant to the Service Level that are equal to or less than the Service Level Value divided by the number of all items, multiplied by 100. If the number of all items for a Service Level equals zero, the Service Level Measured % shall be marked as 'N/A'. If the number of relevant call items or P3 or P4 ticket items is less than ten (10), then the Service Level Measured % is reported but shall be considered 'Insufficient' for the purposes of determining whether the Service Level Target was met or not.

d) Service Level Measured % Met Determination ("Met Criteria"):

i. Above: For Service Levels where the Service Level Measured% is expected to be equal to or greater than the Service Level Target%, then if a Service Level Measured% is greater than or equal to the Service Level Target%, the Service Level shall be considered met or exceeded.

ii. Below: For Service Levels where the Service Level Measured% is expected to be less than or equal to the Service Level Target%, then if a Service Level Measured% is less than or equal to the Service Level Target%, the Service Level shall be considered met or exceeded.

e) If the SLA and SLO Service Level Measured% is not met or is trending negatively over two (2) consecutive calendar months, or more than one Service Level is not met in a calendar month, Client PSM shall initiate a discussion with Service Provider CSM to consider additional Problem Management and Continual Service Improvement.

f) All SLA and SLO Service Levels shall be reported via the Standard Monthly Service Level Report within seven (7) Business Days after the end of the calendar month.

g) Custom Reporting: shall be any reporting which Client requests that is beyond what is provided in the Standard Monthly Service Level Report. Custom Reporting requests shall be submitted as Service Request tickets. The feasibility of the request and any additional fees, if applicable, to implement it shall be discussed between Client PSM and Service Provider CSM.

12.2.5. SERVICE LEVEL CREDITS

a) The Service Provider CSM shall inform Client PSM if any Service Levels are not met and whose type is "SLA". Then Client PSM may initiate a Service Level Credit Claim ("Claim") for those Service Levels that were not met. The Claim must be made to Service Provider CSM in writing prior to the publishing of the next Standard Monthly Service Level Report.

b) Service Level Credit Calculations:

i. Above Met Criteria Failed for Value and Rate Calculation Methods: For each Service Level Measured % that was not marked as 'N/A' or 'Insufficient', the Service Level Credit shall be 1% for each 1% the Service Level Measured % is below the Service Level Target % up to a maximum Service Level Credit of 15%. The specific formula shall be: IF (Service Level Target % > Service Level Measured % THEN Service Level Credit % = MIN (CEILING (Service Level Target % – Service Level Measured %, 1) / 1, 15) ELSE Service Level Credit % = 0.

ii. Below Met Criteria Failed for Value and Rate Calculation Methods: For each Service Level Measured % that was not marked as 'N/A' or 'Insufficient', the Service Level Credit shall be 1% for each 1% the Service Level Measured % is above the Service Level Target % up to a maximum Service Level Credit of 15%. The specific formula shall be: IF (Service Level Measured % > Service Level Target % THEN Service Level Credit % = MIN (CEILING (Service Level Measured % - Service Level Target %, 1) / 1, 15) ELSE Service Level Credit % = 0.

iii. Above Met Criteria Failed for Availability Calculation Method: For each Service Level Target % that is not met in a calendar month, the Service Level Credit shall be 1% for each 0.1% the Service Level Measured % is below the Service Level Target % up to a maximum Service Level Credit of 15%. The specific formula shall be: IF (Service Level Target % - Service Level Measured %) > 0 THEN Service Level Credit % = MIN (CEILING (Service Level Target % – Service Level Measured %, 0.1) / 0.1, 15) ELSE Service Level Credit % = 0.

c) The Total Service Level Credits %'s for an impacted Service in the Reporting Period shall not exceed 30%.

d) The Total Service Level Credit Amount shall be equal to the Total Service Level Credit %'s multiplied by the total of all the monthly recurring Service fees (excluding one-time fees) for the impacted Service in the Reporting Period.

e) A Service Level Credit Claim shall not be considered a contractual material breach.

f) Service Level Credit Calculation Examples:

i. Client Satisfaction Rate
- Reporting Period = Dec 2023
- Met Criteria = Above. That is, Service Level Measured% needs to be less than or equal to the Service Level Target% of 98%
- Number of items with a value less than or equal to Service Level Target% = 4
- Number of items with a value greater than Service Level Target% = 96
- Service Level Measured% = 96 / (4 + 96) * 100 = 96%
- Service Level failed because Service Level Measured% of 96% is not >= Service Level Target% of 98%

a. Service Level Penalty% = 2%. That is, 1% for every 1% below 98% Target up to a maximum of 15%

ii. **Level 1 Call Answer Performance**
- Reporting Period = Dec 2023
- Service Level Measured Value needs to be less than or equal to Service Level Target Value of 30 seconds.
- Met Criteria = Above**.** That is, Service Level Measured% needs to be greater than or equal to the Service Level Target% of 85%
- Number of items with a value less than or equal to Service Level Value = 200
- Number of items with a value greater than Service Level Value = 38
- Service Level Measured% = 200 / (200 + 38) * 100 = 84%
- Service Level failed because Service Level Measured% of 84% is not > = Service Level Target% of 85%
- Service Level Credit% = 1%. That is, 1% for every 1% below 85% Target up to a maximum of 15%

iii. **Level 1 Call Abandonment Rate**
- Reporting Period = Dec 2023
- Met Criteria = Below. That is, Service Level Measured% needs to be less than or equal to the Service Level Target% of 5%
- Number of items with a value less than or equal to Service Level Target% = 20
- Number of items with a value greater than Service Level Target% = 180
- Service Level Measured% = 20 / (20 + 180) * 100 = 10%
- Service Level failed because Service Level Measured% of 10% is not < = Service Level Target% of 5%
- Service Level Penalty% = 5%. That is, 1% for every 1% above 5% Target up to a maximum of 15%

iv. **Level 2 Ticket Response Time by Priority (P1 – CRITICAL Response Time)**
- Reporting Period = Dec 2023
- Service Level Measured Value needs to be less than or equal to Service Level Value of 15 minutes.

- Met Criteria = Above. That is, Service Level Measured% needs to be greater than or equal to the Service Level Target% of 95%
- Number of items with a value less than or equal to Service Level Value = 180
- Number of items with a value greater than Service Level Value = 20
- Service Level Measured% = 180 / (180 + 20) * 100 = 90%
- Service Level failed because Service Level Measured% of 90% is not > = Service Level Target% of 95%
- Service Level Credit% = 5%. That is, 1% for every 1% below 95% Target up to a maximum of 15%

MSD-1: CLIENT-SPECIFIC DETAILS

1. CLIENT LOCATIONS

List of Location details to be finalized in operational documentation created as part of the Transition-In Phase.

Address	State	Country	# Employees	Office Type/Purpose	Hours of Operation	Normal Business Hours
1.						

2. SERVICE HOURS OF OPERATION

	Hours of Operations	Time	Included	Comments
1.	Level 1 Service Normal Business Hours	Mon to Fri, 6am CT to 6pm CT including weekends and holidays		X
2.	Level 1 Service Outside Business Hours	Mon to Fri, 6pm CT to 6am CT including weekends and holidays	X	

3. LANGUAGES

	Language	Comments
1.	English	
2.	Spanish	

4. TOOLS

List of Tools to be finalized in operational documentation created as part of the Transition-In Phase.

	Tool Name	Service Provider	Client
1.	ITSM Tool		X
2.	Knowledge Management Repository		X
3.	Self-Service Portal		X
4.	Contact Center (ACD/IVR)	X	
5.	Remote End-User Device Access Tool		X
6.	Jump Server/VDI within Client's environment installed with applications and tools to deliver the Service		X
7.	VPN		X

5. STANDARD HARDWARE AND SOFTWARE END USER SUPPORT LIST

List to be finalized in operational documentation created as part of the Transition-In Phase and maintained during the Steady State Phase in the Knowledge Management Repository.

6. CUSTOM HARDWARE AND SOFTWARE END USER SUPPORT LIST

List to be finalized in operational documentation created as part of the Transition-In Phase and maintained during the Steady State Phase in the Knowledge Management Repository in the Knowledge Management Repository.

MSD-2: STEADY STATE RESPONSIBILITIES MATRIX

1. MSD RESPONSIBILITIES MATRIX

a) The *Responsibilities Matrix* covers the overall steady state ITSM lifecycle tasks to deliver a Service.

b) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in a Service.

c) An 'X' in the *Client* column means Client is responsible for the task.

d) A '(*)' denotes that there is a clarification of: (i) the task details; (ii) the division of task responsibilities between Service Provider and Client; or (iii) task is billable.

No.	General Tasks	Service Provider	Client	Clarifications
1.	Provide single point of contact and coordination for all Incident and Service Requests for information and activities in areas covered in this Service Description	X		
2.	Use ITSM Tool to document all incoming Tickets and manage the life cycle of Ticket	X		
3.	Provide expert Level 1 support and look for opportunities to Shift-Left from Level 1 to Level 0 and from Level 2 to Level 1 for Incidents and Service Requests and inquiries on Services in the scope	X		
4.	Manage the Incident Resolution and close-out process (e.g., provide Level 2) including escalating to the third party (vendor management)	X		
5.	Provide Service Provider supporters that clearly communicate and are proficient in the supported languages and that are appropriately trained to meet Client requirements	X		
6.	Perform Root Cause Analysis for any managed service sold by Service Provider to Client on recurring and Priority 1 and 2 Incidents as applicable to Service Desk	X		
No.	**ITSM Tools**	**Service Provider**	**Client**	**Clarifications**
7.	Set up and maintain ITSM Tool environment for Service Desk services (Incident and Service request only)	X		
8.	Provide users with ITSM Tool access and to view status to Incident and Service Request tickets	X		
9.	Provide Self-service Portal that's part of or integrated with the ITSM Tool	X		
10.	Train Service Desk agent to use ITSM Tool	X		
11.	Train Client trainer to use ITSM Tool	X		Trainer must have resolver access to the ITSM Tool. Service Provider shall create the content and Client and Service Provider to agree on the training material.
12.	Train end users on using ITSM Tool for Service Desk Services		X	
13.	Create/Delete/Add/Modify Resolver Groups for Service Desk Services (Incident and Service request only)	X		
14.	Create/Delete/Add /Modify Categorization/prioritization for Service Desk Services	X		

15.	ITSM Tool user creation/deletion/updates for Service Desk Services	X		
No.	**User Administration**	**Service Provider**	**Client**	**Clarifications**
16.	Receive, track and process requests for user account additions (onboarding), changes (update, delete) and terminations (offboarding) according to documented Client procedures. If no documented procedures exist, Service Provider will work with Client to create one.	X		
17.	Perform password resets, account unlocks according to documented Client procedures. If no documented procedures exist, Service Provider will work with Client to create one.	X		
No.	**Automatic Call Distributor, Interactive Voice Response (IVR)**	**Service Provider**	**Client**	**Clarifications**
18.	Provide software, equipment, and implement and manage Interactive Voice Response [IVR], Automatic Call Distribution [ACD] needed to collect, track, and manage Service Incidents and Service Requests received over the phone by the Service Desk	X		
19.	Support in-scope language and options	X		
20.	Record all calls for quality and training purposes	X		
21.	Transfer calls to Level 2 supporters where applicable	X		
No.	**Incident & Service Request Management**	**Service Provider**	**Client**	**Clarifications**
22.	Create and record Incident, and Service Request priority types, Response, Update, and Resolution targets for Incidents and Service Requests	X		
23.	Document all troubleshooting steps in the ITSM Tool	X		
24.	Monitor, track and own Incidents and Service Requests and escalate according to documented procedures when applicable.	X		
25.	Verify acceptance of delivered Services by contacting the user to confirm results and level of satisfaction through Client satisfaction survey	X		
26.	Ensure that recurring Incidents for any Services purchased by Client are reviewed using the Root Cause Analysis procedure (Problem Management)	X		
27.	Document solutions and update Knowledge Management Repository regularly	X		
28.	Utilize remote control tools to manage and update in-scope desktop system Software, and to maintain configuration and inventory information	X		
29.	Recommend Service Provider Standard Incident and Service Request Ticket Management Services procedures	X		

30.	Resolve Incidents or implement workaround at Level 1 using approved, remote tools; otherwise escalate to appropriate Level 2 supporter as required, in accordance with documented Client procedures and SLA	X		
No.	**Major Incident Management**	**Service Provider**	**Client**	**Clarifications**
31.	Facilitate technical bridge calls during Major Incidents and coordinate with all responsible participants, including third parties, in accordance with documented Client procedures	X		
32.	Develop escalation process	X		
33.	Review and approve escalation process		X	
34.	Issue broadcasts or other notices to provide status updates as required for planned and unplanned events		X	
No.	**Software Installation**	**Service Provider**	**Client**	**Clarifications**
35.	Determine if software is standard, in scope of support or requires additional approval	X		
36.	If approval required, follow the documented process to obtain approval from Client	X		
37.	Utilize remote control tools to manage and update in-scope desktop system Software using Client's software update process, and to maintain configuration and inventory information	X		
38.	Test and provide application install package		X	
No.	**Knowledge Management and Training**	**Service Provider**	**Client**	**Clarifications**
39.	Develop, document, and maintain Service Desk runbook or manual for this Service	X		
40.	Provide a comprehensive Knowledge Management Repository	X	X	
41.	Train new Service Provider supporters on ITSM Tools, process, and methods	X		
42.	Review and approve recommended Service Desk solutions as applicable		X	
43.	Review and approve Service Desk operational procedures as applicable		X	
44.	Support and/or provide documentation on business functions and features for all supported environments to Service Provider		X	
No.	**Reporting**	**Service Provider**	**Client**	**Clarifications**
45.	Report on Service Desk statistics and trends based on the Service Level Agreements, Service Level Objectives and Key Performance Indicators and share with Client	X		
46.	Identify and report on trends in Service Requests, Incidents, and Problems, and identify those that could be addressed through Service Desk improvements (e.g., training, self-service tools, Shift-Left) and share with Client	X		
47.	Report on phone statistics as defined in the Service Level Management and share with Client	X		

48.	Identify opportunities to increase speed to resolution, increases Client satisfaction and reduces the numbers of contacts per user per month	X		
No.	**Client Satisfaction**	**Service Provider**	**Client**	**Clarifications**
49.	Develop, conduct, and execute procedures for conducting Client Satisfaction Surveys in accordance with the Service Level Management	X		
50.	Review, participate and approve procedures for conducting Client Satisfaction Surveys		X	
No.	**ITSM Self-Service Portal (Level 0 Support)**	**Service Provider**	**Client**	**Clarifications**
51.	Apply Shift-Left approach to maintain ITSM Self-service Portal content by creating regular documentation (Knowledge Management Articles) and educating Client to use ITSM Self-service Portal when available or applicable	X	X	
52.	Monitor and report on effectiveness of ITSM Self-service Portal and make necessary adjustments to increase its usage	X	X	
No.	**Out of Scope Service Management**	**Service Provider**	**Client**	**Clarifications**
53.	Maintain and document out of scope request service procedures	X		
54.	Route tickets to Client defined contacts for out-of-scope Services	X		
55.	Identify, recommend, and implement conversion of the out-of-scope requests to in scope Services	X		
56.	Review, participate and approve out of scope requests to become in scope services for Level 1 support		X	
No.	**Continual Service Improvement**	**Service Provider**	**Client**	**Clarifications**
57.	Identify, recommend, and implement Continuous Service Improvement, which is a component of a broader, integrated IT Service operations, which includes a Knowledge Management Repository and ITSM Self-service Portal capabilities, that best meet Client's business needs and service level expectations	X		
58.	Perform operational planning for Service Desk capacity and Service Provider supporter performance	X		
59.	Obtain regular feedback from key Client stakeholders (who frequently interact with the Service Desk) to identify the appropriate sets of skills, training, and enhancements needed by Service Provider Level 1 supporters	X	X	
60.	Recommend Service Provider standard procedures for this Service	X		
61.	Understand Client's business, and work with Client to implement new solutions periodically that have a positive impact to Client and/or end users to bring in operational and financial efficiency	X	X	

No.	Shift-Left Level 0 and 1 Task Management	Service Provider	Client	Clarifications
62.	Identify, recommend, and enhance Level 0 ITSM Self-service Portal through Continuous Service Improvement and application of Shift-Left approach	X		
63.	Identify, recommend, and enhance Level 1 tasks as needed through Continuous Service Improvement and application of Shift-Left approach	X		
64.	Review, participate and approve enhancements to Level 0 ITSM Self-service Portal and Level 1 tasks as recommended by Service Provider through Continuous Service Improvement and application of Shift-Left approach		X	

MSD-3: TRANSITION MANAGEMENT RESPONSIBILITIES MATRICES

1. TRANSITION-IN MANAGEMENT RESPONSIBILITIES MATRIX

No.	Planning	Service Provider	Client	Clarifications
1.	Establish detailed Transition-In plan and finalize templates	X		
2.	Identify and agree with Client to key milestones and deliverables	X		
3.	Identify transition team members including executive sponsor of the program	X		
4.	Establish governance, communication structure and frequency of the reports or status	X		
5.	Identify any infrastructure, ITSM portal or access required, if necessary, to support the transition	X		
6.	Identify and validate in-scope applications and technologies	X		
7.	List access and documentation of in scope applications and technologies required to execute the transition	X		
8.	Establish travel schedule and location of the travel	X		
9.	Establish detailed transition plan and finalize templates	X		
10.	Assign Key member(s) or subject matter experts to work with Service Provider		X	
11.	Agree on transition plan and deliverables		X	
12.	Agree on governance, communication structure and frequency		X	
13.	Procure appropriate license where applicable for tools or applications/technologies for in scope Services		X	
14.	Agree on travel schedule and location		X	
15.	Sign off on planning phase		X	
No.	**Knowledge Acquisition and Integration**	**Service Provider**	**Client**	**Clarifications**
16.	Agree that all open tickets prior to Service Provider taking over Services shall not be subject to SLA's		X	
17.	Align, enhance, or implement Incident, Change, Problem Management processes	X		
18.	Set up Service Provider infrastructure necessary to support Client	X		
19.	Travel to Client location(s) if necessary	X		
20.	Get access to in-scope applications and technologies	X		
21.	Set up meeting and conduct knowledge transfer of in scope applications and technologies	X		
22.	Create and update Client specific business function documents	X		
23.	Identify any gap(s) or risk(s) and communicate to Client	X		

24.	Identify any scope change(s) and communicate to the sponsor(s) (Client and Service Provider)	X		
25.	Share knowledge with supporters	X		
26.	Ensure everyone in team has access to the applications, technologies, and documents	X		
27.	Understand the enhancement process and tools and schedules	X		
28.	Set up ITSM Tool and ITSM Self-service Portal access and training		X	
29.	Ensure subject matter experts or key contacts are available and participate in the knowledge sharing process		X	
30.	Share any existing process documentation		X	
31.	Share any ongoing and future changes that may impact overall transition		X	
32.	Grant access to in-scope application and technologies		X	
33.	Work with Service Provider to manage gaps or risks		X	
34.	Work with Service Provider to include or exclude any scope changes or updates		X	
35.	Sign off knowledge acquisition and integration phase	X	X	
No.	**Shadow**	**Service Provider**	**Client**	**Clarifications**
36.	Review resolved tickets	X		
37.	Review any application/technology enhancement or development process	X		
38.	Resolve tickets if applicable	X		
39.	Perform minimal impact changes or tasks	X		
40.	Carry out or execute on service requests if applicable	X		
41.	Update Client on the readiness to take over Services	X		
42.	Communicate any critical milestones or deliverables that may prevent us from taking over services	X		
43.	Review ticket or enhancement task and provide feedback		X	
44.	Communicate internally to the team and sign off to start this Service		X	
No.	**Steady State**	**Service Provider**	**Client**	**Clarifications**
45.	Manage open tickets prior to Service Provider taking over services, but no SLAs shall apply to those tickets	X		
46.	Service Provider takes over support for in-scope applications	X		
47.	All tickets are processed in accordance with the established ITSM Processes during the transition acquisition and integration phase and all the information must be entered in the ITSM Tool as a ticket	X		
48.	Governance and cadence are established to share regular updates with Client and reports as described in the service level management section	X		

2. TRANSITION-OUT MANAGEMENT RESPONSIBILITIES MATRIX

No.	General Tasks	Service Provider	Client	Clarifications
1.	Write a detailed Transition-Out plan		X	
2.	Review and align the Transition-Out plan with Client	X		
3.	Advise Client where applicable in designing risk contingency and mitigation plans	X		
4.	Assign resources and identify the physical locations requirements from Client, if applicable, to support Service Provider's activities	X		
5.	Identify, communicate, and take appropriate action on Service Provider's security requirements with respect to; (i) Service Provider Data residing on Client owned Assets; (ii) Client requests to access Service Provider's physical location and systems by Client or Client's third party (if applicable) including Confidentiality obligations		X	
No.	**Software Transition**	**Service Provider**	**Client**	**Clarifications**
6.	Provide a list of Service Provider users who access Client owned software	X		
7.	Remove and delete Service Provider users and access configuration and data from Client owned software at the end of transition		X	
No.	**Hardware Transition**	**Service Provider**	**Client**	**Clarifications**
8.	Provide a list of Client owned hardware used by Service Provider used to provide this Service	X		
9.	Return to Client all Client owned hardware and transfer any lease or warranty from Service Provider to Client, if applicable	X		
10.	Pay for all costs associated with such transfer including transfer of license, warranty, and applicable fees, if applicable		X	
No.	**Knowledge Transfer and Documentation**	**Service Provider**	**Client**	**Clarifications**
11.	Provide all Client specific documents including runbooks, operational manual and any technical information that were inherited during transition, updated, or generated during the duration of Service with Service Provider that are required for continued provision of Services by Client	X		
12.	Provide reasonable Knowledge transfer and training remotely to Client for continued provision of Services by Client	X		
No.	**Operations**	**Service Provider**	**Client**	**Clarifications**
13.	Assume full responsibility for all open items at the end of transition and take on full responsibility of the Services		X	

14.	Confirm in writing and sign off the end of Transition-Out activities		X	
15.	Release Service Provider of any further responsibility for open items at the end of transition		X	

Exhibit 2:

END-USER CLIENT DEVICES OVERVIEW
SERVICE DESCRIPTION

REV 2025-08-30

1. SERVICE OVERVIEW

a) The Managed End-User Client Device Services ("Service(s)" or "EDS") is a service line of the Service Provider's End-User Client Services ("ECS") service family and provides various combinations of OS updates, application updates and deployment, and policy compliance for in-scope: (i) desktops and laptops ("Desktop Device Management" or "DDM"); (ii) mobile and tablet devices ("Mobile Device Management" or "MDM"); and (iii) virtual desktops ("Virtual Desktop Management or "VDM"). Additionally, EDS offers Unified Device Management (UDM) which combines DDM and MDM but limits the Supported EDS Tool to Microsoft Intune. UDM is available when Client has purchased Service Providers Managed Microsoft Modern Workplace service.

b) In-scope end-user client devices are collectively referred to as "Client Devices".

c) The Service(s) to be delivered to Client, the EDS Tool(s) to be used, and the quantity and the type of Client's in-scope Client Devices shall be detailed in the *Pricing Summary* section of the applicable SOW.

d) For invoicing purposes, at the end of each billing cycle the Minimum Contracted Quantity for the Service in the *Pricing Summary* shall be compared to the actual quantities being managed, and which ever quantity is greater shall be multiplied by the corresponding unit price in the *Pricing Summary*.

e) The Service includes a 24x7 Helpdesk single point of IT support related to the management of the Client Devices as described in the *ITSM Foundation Services Description*.

f) Service Transition Management is detailed in the *ITSM Foundation Services Description*. In addition, Service Provider shall: (i) gather Client requirements and leverage best practices to develop Client's EDS policies; and (ii) align existing Client processes (if applicable) with respect to procurement, retirement, and policy compliance of Client's Client Devices.

g) Any support out of scope of EDS shall be subject to billable professional services hourly rates as documented in the Quotation of Services section of the applicable SOW. Service Provider shall seek Client approval for billable professional services prior to execution.

h) Client shall use the Service in accordance with this Service Description and in accordance with any additional operational documentation, which shall be provided by Service Provider to Client or as mutually agreed upon, from time-to-time.

i) The MDM service can only be sold as an add-on to the DDM service.

j) The Service delivery requires Nerdio Manager access to Client's Microsoft 365 environment. If Client does not grant the access, some features of the Service may not be available and/or price adjustments on the Pricing Summary may be required.

k) The Service comes bundled with the managed services in the *ITSM Foundation Services Description*, which details standardized support communication channels, ticket management ("ITSM Tool"), service levels, as well as the governance, incident, change, problem, and escalation ITSM processes in support of the Service. Tickets will be securely visible to Client online, including status and updates, via Service Provider's ITSM Tool. See the *ITSM Foundation Services Description* for further details.

1.1. SUPPORTED OS TYPES BY SERVICE

a) Support Table

	Windows	MacOS	ChromeOS	Linux	iOS	Android
DDM (1)	X	X	X	X		
MDM					X	X
VDM	X					
UDM	X	X		X	X	X

b) Each Service in the table may support one or more of the OS types listed with an 'X'.

c) Note (1): when Third-party application patch management is in-scope, support is only provided for Windows.

1.2. SUPPORTED EDS TOOL(S) BY SERVICE

a) Support Table

	Microsoft Intune	Google Workspace Endpoint Manager	RMM	JAMF	Nerdio	Azure Virtual Desktop
DDM	X Subscription provided by Client	X Subscription provided by Client	X Subscription provided by Service Provider	X Subscription can be provided by Client or via Service Provider's tenant	X Subscription provided by Service Provider	
MDM	X Subscription provided by Client	X Subscription provided by Client		X Subscription can be provided by Client or via Service Provider's tenant	X Subscription provided by Service Provider	
VDM					X Subscription provided by Service Provider	X Subscription provided by Client.
UDM	X Subscription provided by Client				X Subscription provided by Service Provider	

b) Each Service in the table may by delivered by one or more of the EDS Tools listed with an 'X'. The party responsible for the EDS tool subscription licensing and any limitations of on OS types are listed as well. RMM is an abbreviation for "Remote Management and Monitoring" and is Service Provider's EDS tool.

1.3. SUPPORTED OS TYPES BY EDS TOOL

a) Support Table

	Windows	MacOS	ChromeOS	Linux	iOS	Android
Microsoft Intune	X	X		X	X	X

	Windows	MacOS	ChromeOS	Linux	iOS	Android
Google Workspace Endpoint Manager	X		X		X	X
RMM	X					
JAMF		X			X	
Nerdio	X					
Azure Virtual Desktop	X					

b) Each EDS Tool in the table may support one or more of the OS Types listed with an "X". RMM is an abbreviation for "Remote Management and Monitoring" and is Service Provider's EDS tool.

2. RESPONSIBILITIES MATRIX

a) The Responsibilities Matrix for each in-scope Service above is defined the respective Addenda *EDS-1: DDM, MDM, VDM, and UDM.*

b) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in the Service. Any limitations shall be detailed in the *Clarifications* column.

c) An 'X' in the *Client* column means Client is responsible for the task.

d) When an 'X' is in both the *Service Provider* and *Client* columns, '(*)' means that there is a specific clarification of responsibilities in the *Clarifications* column.

Exhibit 3:

EDS-1: DDM
SERVICE DESCRIPTION
REV 2025-08-30

1. SERVICE OVERVIEW

a) Desktop Device Management ("DDM") provides administration, monitoring, and support of the *Supported EDS Tool*.

2. DDM RESPONSIBILITIES MATRIX

No.	DDM Task Description	Service Provider	Client	Clarifications
1.	Procure & manage in-scope Client Devices (i.e., device hardware and golden or factory-based OS images).		X	
2.	Procure & manage in-scope Client Devices OS and App licensing, subscriptions, and associated vendor service agreements to maintain the support requirements of the OS and App vendors and the in-scope EDS Tool(s).		X	
3.	Procure in-scope EDS Tool(s) subscription and implement EDS Tool(s).	X (*)	X	According to *Supported EDS Tool(s) By Service* table. The EDS Tool(s) subscription level will define the management capabilities available to Service Provider. Some stated responsibilities may be unavailable if the required tool capabilities are not licensed. (*) Service Provider only procures subscriptions for its RMM EDS Tool or JAMF instance, as detailed in the *Pricing Summary*, and then implements it as part of the Service; all other EDS Tool subscriptions and implementations are done by Client prior to delivery of the Service.
4.	Perform on-site support for in-scope Client Devices.		X	Client provides on-site smart hands support on behalf of Service Provider.
5.	Grant administration access to Client-provisioned in-scope EDS Tool(s).		X	Service Provider shall function as a subcontractor of Client under Client's vendor service agreements.
6.	Procure and manage Azure Active Directory ("AD") or Hybrid Active Directory ("Hybrid AD") Services for user and application-specific conditional access compliance on in-scope Client Devices		X	

No.	DDM Task Description	Service Provider	Client	Clarifications
	when the in-scope EDS Tool is MS Endpoint Manager.			
7.	Define & approve desktop app policies.		X	Service Provider can help Client to define new or adjust existing policies.
8.	Define & approve desktop device policies for corporate-owned Client Devices.		X	Service Provider can help Client to define new or adjust existing policies.
9.	Create, Modify, Delete desktop app and desktop device policies according to client request.	X		
10.	Perform desktop app policy activities such as: wipe, remove, and compliance policies for corporate-sanctioned desktop apps on in-scope Client Devices using an in-scope EDS Tool.	X		Included in all DDM services except for Services identified as “Patch and Application Deployment Only” in the *Pricing Summary*. For corporate-owned and BYOD in-scope Client Devices. Available policies depend on the capabilities of the target OS and EDS Tool.
11.	Perform desktop device policy activities such as: enroll/re-enroll, wipe, lock, configuration profiles, encryption, and compliance policies for corporate-owned in-scope Client Devices using an in-scope EDS Tool.	X		Included in all DDM services except for Services identified as “Patch and Application Deployment Only” in the *Pricing Summary*. N/A for BYOD Client Devices. When enrolling new Client Devices so that the total number of actual enrolled Client Devices exceeds the contractual minimum, additional per Client Device monthly fees apply. See applicable SOW. Available policies depend on the capabilities of the target OS and EDS Tool.
12.	Administer granular access control policies for apps and storage based on attributes such as user identity, location, device status, and IP address.	X		Included in all DDM services except for Services identified as “Patch and Application Deployment Only” in the *Pricing Summary*. EDS Tool(s) subscription level will define the management capabilities available to Service Provider. Some stated responsibilities may be unavailable if the required tool capabilities are not licensed.
13.	Create automation packages or scripts to accomplish in-scope tasks.	X		Scripting and automation are tools Service Provider will use at its discretion to accomplish an in-scope task.

No.	DDM Task Description	Service Provider	Client	Clarifications
				Automation and scripting requests that are not in-scope of this Service are separately billable.
14.	Provide Commercial-off-the-Shelf ("COTS") vendor installation files for approved desktop app deployment packages.		X	In addition to providing installation files, Client is responsible for appropriate license levels and usage.
15.	Deploy approved Commercial-off-the-Shelf ("COTS") corporate-sanctioned desktop apps to in-scope Client Devices using an in-scope EDS Tool and limited to COTS apps supported by an in-scope EDS Tool.	X		Testing the deployment of new apps is performed by Service Provider. Testing of a newly deployed app is performed by Client. The number of new apps that can be deployed per month is limited to two (2). Additional new app deployments above two in a month shall be subject to additional billing. If an update to an existing app requires its redeployment, it will be counted as a new app deployment.
16.	Test & provide approved corporate-sanctioned custom desktop app packages for deployment, and uninstall to in-scope Client Devices using an in-scope EDS Tool.		X	
17.	Deploy & update approved corporate-sanctioned custom desktop app packages to in-scope Client Devices using an in-scope EDS Tool.	X		Frequency: monthly, and according to custom update release availability and Client update policy. Testing the deployment of new apps is performed by Service Provider. Testing of a newly deployed app is performed by Client. The number of new apps that can be deployed per month is limited to two (2). Additional new app deployments above two in a month shall be subject to additional billing. If an update to an existing app requires its redeployment, it will be counted as a new app deployment.
18.	Uninstall approved corporate-sanctioned COTS & custom app packages from in-scope Client Devices using an in-scope EDS Tool.	X	X (*)	COTS and custom apps deployed under the Service can be uninstalled. (*) All other apps that Service Provider did not deploy with the EDS Tool.
19.	Approve desktop OS updates on in-scope Client Devices.		X	
20.	Update desktop OS on corporate-owned in-scope Client Devices using an in-scope EDS Tool.	X		N/A for BYOD Client Devices.

No.	DDM Task Description	Service Provider	Client	Clarifications
				Frequency: monthly, and according to desktop OS vendor update release availability and Client update policy. Includes security, critical, and driver/firmware patches released by the OS vendor.
21.	Deploy out-of-band critical "Zero-Day" patches	X		Windows: Within 8 business hours of release from vendor, where patching can be forced. Mac OS: update timeframe determined by vendor, where patching cannot be forced. ChromeOS: update timeframe determined by vendor, where patching cannot be forced. Linux: N/A.
22.	Resolve failed OS Patches	X	X(*)	If there is a pattern of failures, or an unusually high number of failures, Service Provider will conduct Root Cause Analysis and perform corrective actions to resolve. (*) In all other cases (e.g., due to specific Client Device issues such as the Device being turned off or end-user delays in allowing patching) it is assumed the patches will be applied during the next patch window or when the end-user or client conduct follow-up actions on the affected in-scope Client Devices.
23.	Provide post-deployment & update compliance report to Client for in-scope Client Devices.	X		
24.	Upgrade desktop OS version on corporate-owned in-scope Client Devices.		X	
25.	Enforce compliance for non-compliant in-scope Client Devices.		X	
26.	Provide direct End User support.		X	Client's IT supporters will work directly with the End User. Service Provider IT supporters will work with Client's IT supporters.

No.	DDM Task Description	Service Provider	Client	Clarifications
27.	Provide support to Client's IT supporters for incident troubleshooting for in-scope devices.	X		
28.	Create & maintain operational runbook for in-scope Client Devices.	X		
29.	Send deployment & update notifications to designated Client points of contact.	X		
30.	Send deployment & update notifications to in-scope Client Device end-users.		X	
31.	Perform backup/restore of mobile device end-user data residing on in-scope Client Devices.		X	Assumption: Client has an existing operational self-service backup method (e.g., MS OneDrive) or Client purchased from Service Provider a self-service backup service.
32.	Billable Service Request Management Service request tasks that are not explicitly included in one of the tasks above. Perform any task that is designated as a Client responsibility in this matrix. The delivery of a new service not in scope of this Service. Designing, engineering, and consulting effort for an existing or new in-scope Client Device or Client's IT overall environment. Any mitigation or restoration work of a new in-scope Client Device where the root cause is attributable to a Client action performed on the Device. Deploy or build new in-scope Client Device image. Replace an existing in-scope Client Device (s) with a new Device. Develop, monitor, and maintain customized or third-party tools, scripts, and software installed on an existing in-scope Client Device.	X (*)		(*) When performed by Service Provider, all labor effort and costs associated with the request are billed separately according to the *Change Order Request Procedure* in the applicable SOW.

No.	DDM Task Description	Service Provider	Client	Clarifications
	Create additional documentation beyond Service Provider operational handbook for this Service. Replace existing Client-provisioned EDS Tool. Deploy Autopilot when an in-scope EDS Tool is MS Endpoint Manager. Add new EDS Tool. Upgrade in-scope Client Device App & OS. Develop custom functionality not supported by EDS Tool (Example: counting app licensing).			

3. THIRD-PARTY PATCH APPLICATION MANAGEMENT RESPONSIBILITIES MATRIX

a) DDM has an optional add-on service called Third-party Application Patch Management, which is in scope when detailed in the *Pricing Summary* of the applicable SOW and is charged per-device. This optional add-on service requires the use of Microsoft Intune as the *Supported EDS Tool* for the DDM service. Service Provider will implement this optional add-on service and integrate it with Client's existing Microsoft Intune environment to deliver it.

b) The Third-party Application Patch Management add-on includes patching for up to ten (10) applications as part of the base subscription. For any additional applications beyond the included ten (10), a per-application charge will be added to the *Pricing Summary*.

c) The following table details the Third-party Application Patch Management service.

No.	DDM Task Description	Service Provider	Client	Clarifications
1.	Implement third-party application patch management solution.	X	X(*)	Service Provider will implement and configure the third-party application patch management solution. See addendum DDM-1 (*)Client agrees to provide the required access and resources as agreed upon to meet the service requirements.
2.	Configure standard third-party application patch management package repository.	X		See addendum DDM-1
3.	Configure custom third-party application patch management package repository.	X	X(*)	See addendum DDM-1 (*) Client is responsible for managing and maintaining custom third-party repository.
	Configure third-party application patch management policies.			

No.	DDM Task Description	Service Provider	Client	Clarifications
	Resolve third-party application patch deployment issues.	X	X(*)	(*) Service Provider provides level 2 support for the Device and OS. Client provides level 1 end-user support.
	Track and report on third-party application patch status.	X		
4.	Test third-party application patch versions.		X	
5.	Approve third-party application patch versions for release		X	

DDM-1: CLIENT-SPECIFIC DETAILS FOR THIRD-PARTY APPLICATION PATCHING

1. THIRD PARTY APPLICATION PATCHING SOLUTION

Service Provider will implement the Nerdio solution to provide the service.

2. PACKAGE RESPOSITORIES

The following list of Winget Repositories will be implemented.

No.	Repository Name	Link	Clarifications
1.	Standard Community Winget Repository	https://github.com/microsoft/winget-pkgs	
2.	Custom Winget Repository	*<link>*	

3. APPLICATIONS TO PATCH

The following table lists the application to patch and the repository to utilize.

No.	Application Name	Repository to Use
1.	Adobe Reader	Standard Community Winget Repository
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

Exhibit 4:

EDS-1: MDM
SERVICE DESCRIPTION
REV 2025-08-30

1. MDM RESPONSIBILITIES MATRIX

No.	MDM Task Description	Service Provider	Client	Clarifications
1.	Procure & manage in-scope Client Devices (i.e., device hardware and golden or factory-based OS images). Procure, at Client discretion, Apple Business Manager when Apple Client Devices are in scope, and ensure they are purchased and registered. Procure, at Client discretion, Android Zero Touch when Android Client Devices are in scope, and ensure they are purchased and registered.		X	
2.	Procure & manage in-scope Client Devices OS and App licensing, subscriptions, and associated vendor service agreements to maintain the support requirements of the OS and App vendors and the in-scope EDS Tool(s).		X	
3.	Procure in-scope EDS Tool(s) Subscription Licensing.	*	*	According to *Supported EDS Tool(s) By Service* table above.
4.	Perform on-site support for in-scope Client Devices.		X	Client provides on-site smart hands support on behalf of Service Provider.
5.	Grant administration access to Client-provisioned in-scope EDS Tool(s).		X	Service Provider shall function as a subcontractor of Client under Client's vendor service agreements.
6.	Procure and manage Azure Active Directory ("AD") or Hybrid Active Directory ("Hybrid AD") Services for user and application-specific conditional access compliance on in-scope Client Devices when the in-scope EDS Tool is MS Endpoint Manager.		X	

No.	MDM Task Description	Service Provider	Client	Clarifications
7.	Define & approve mobile app policies.		X	Service Provider can help Client to define new or adjust existing policies these during the transition-in/onboarding project.
8.	Define & approve mobile device policies for corporate-owned Client Devices.		X	Service Provider can help Client to define new or adjust existing policies these during the transition-in/onboarding project.
9.	Approve mobile app deployment packages and updates on in-scope Client Devices.		X	
10.	Deploy & update approved Commercial-off-the-Shelf ("COTS") corporate-sanctioned mobile apps to in-scope Client Devices using an in-scope EDS Tool and limited to COTS mobile apps supported by an in-scope EDS Tool. Integration between an EDS Tool and Apple App Store and/or Google Store, if supported.	X		Frequency: monthly, and according to custom update release availability and Client update policy. Testing the deployment of new apps is performed by Service Provider. Testing of a newly deployed app is performed by Client. The number of new apps that can be deployed per month is limited to two (2). Additional new app deployments above two in a month shall be subject to additional billing. If an update to an existing app requires its redeployment, it will be counted as a new app deployment.
11.	Test, provide, and approve corporate-sanctioned COTS mobile app packages not supported by an in-scope EDS Tool and custom mobile app packages for deployment and update to in-scope Client Devices using an in-scope EDS Tool.		X	
12.	Deploy & update approved custom mobile app packages to in-scope Client Devices using an in-scope EDS Tool.	X		Frequency: monthly, and according to custom update release availability and Client update policy. Testing the deployment of new apps is performed by Service Provider. Testing of a newly deployed app is performed by Client. The number of new apps that can be deployed per month is limited to two (2). Additional new app deployments above two in a month shall be subject to additional billing. If an update to an existing app requires its redeployment, it will be counted as a new app deployment.
13.	Perform the following mobile app policy activities: remove, manage access,	X		For corporate-owned and BYOD in-scope Client Devices.

No.	MDM Task Description	Service Provider	Client	Clarifications
	security, and compliance settings for corporate-sanctioned mobile apps on in-scope Client Devices using an in-scope EDS Tool.			
14.	Perform the following mobile device policy activities: enroll/re-enroll, wipe, lock, access, security, and compliance settings for corporate-owned Client Devices using an in-scope EDS Tool.	X		N/A for BYOD Client Devices. When enrolling new Client Devices so that the total number of actual enrolled Client Devices exceeds the contractual minimum, additional per Client Device monthly fees apply. See applicable SOW.
15.	Approve mobile OS updates on in-scope Client Devices.		X	
16.	Update mobile OS on corporate-owned in-scope Client Devices using an in-scope EDS Tool.	X		N/A for BYOD Client Devices. Frequency: monthly, and according to mobile OS vendor update release availability and Client update policy.
17.	Provide post-deployment compliance report to Client for in-scope Client Devices.	X		
18.	Enforce compliance for non-compliant in-scope Client Devices.		X	
19.	Create & maintain operational runbook for in-scope Client Devices.	X		
20.	Send deployment & update notifications to designated Client points of contact.	X		
21.	Send deployment & update notifications to Client Device end-users.		X	
22.	Perform backup/restore of mobile device end-user data residing on in-scope Client Devices.		X	Assumption: Client has an existing operational self-service backup method (e.g.MS OneDrive) or Client purchased from Service Provider a self-service backup service.
23.	Special Service Request Management Replace existing Client-provisioned EDS Tool.		X	This item covers tasks that are not in scope of service request management such as one-time projects, which may also involve additional managed service fees. All costs associated with the request are billed in a separate SOW.

No.	MDM Task Description	Service Provider	Client	Clarifications
	Deploy Autopilot when an in-scope EDS Tool is MS Endpoint Manager. Add new EDS Tool. Upgrade Client Device App & OS. Develop custom functionality not supported by EDS Tool (Example: counting app licensing).			

Exhibit 5:

MICROSOFT MODERN WORKPLACE (MMW)
SERVICE DESCRIPTION

REV 2025-12-04

1. SERVICE OVERVIEW

a) Managed Microsoft Modern Workplace ("Service" or "MMW") is a service line within the Service Provider's End-User Client Services ("ECS"), and consists of two (2) options:

Managed Services Options	Description
i. Microsoft Identity and Access Management Service ("Microsoft IAM")	This service provides comprehensive administration, proactive management, and ongoing support of Microsoft identity and access controls of Client's Microsoft Environment (Entra ID, Active Directory, Certificate Server, or Hybrid Identity). See section *Microsoft IAM* for further details.
ii. Microsoft 365 Productivity Service ("Microsoft 365 + Microsoft IAM")	This service combines *Microsoft IAM* with the comprehensive administration, proactive management, and ongoing support Client's licensed Microsoft 365 Environment (Microsoft 365 Tenant, Purview, Integrated Apps Service, Exchange Online, OneDrive and SharePoint, Teams with Health Reviews). See sections *Microsoft IAM* and *Microsoft 365* for further details.

b) The Service is designed to achieve the following goals:

i. Maintain or improve the Microsoft Secure Score, Identity Secure Score, and Purview Compliance Score.

ii. Ensure the in-scope Client's licensed environment ("Environment"), as defined in addendum *MMW-1: Client-specific Details,* maintains alignment with Client's policies and strategic goals.

iii. Assist with adopting best practices.

iv. Maintain Client's Environment functionality and performance.

v. Assist Client's IT staff with advice, guidance, and hands-on-keyboard remote support.

vi. Perform proactive and reactive administration of Client's Environment.

c) The Client-purchased Service options and their associated pricing and quantities are identified in the *Pricing Summary*.

d) The Service quantities are based on:

i. **Identity Accounts,** which are defined as any active account present in Entra ID or Active Directory. Identity Accounts may represent employees, service accounts, external users, or any other object requiring an Entra ID or Active Directory account.

ii. **M365 Users**, which are defined as an account with access to interact with M365 services and applications, and consist of two (2) options:

1. **Full Users** are defined as active M365 Users which are assigned at least one (1) license labeled as Enterprise, Government, or Business from any active Microsoft 365 or Office 365 subscription. Examples include but are not limited to E1, E3, E5, G1, G3, G5, Business Basic, Business Standard, and Business Premium.

2. **Essentials Users** are defined as active M365 Users assigned at least one (1) license labeled as Frontline, or Exchange Online. Examples include but are not limited to F1, F3, Exchange Online Plan 1/2, and Exchange Online Kiosk.

e) The monthly fee for the Service includes a standard allocation of Service Request tickets equal to 10% of the total M365 Users or Identity Accounts, whichever is greater if both are present in the *Pricing Summary*, with a minimum of 10 tickets included. For example, 10% of 1,000 M365 Users would mean that 100 Service Request tickets per calendar month are included for all the Service(s). The fee per additional ticket shall be documented in the *Pricing Summary*. Service Requests estimated to require greater than four (4) hours of effort can be considered out of scope and separately billable.

f) All Service functions are subject to the limitations of, and capabilities granted by Client's Microsoft licensing.

g) The Service comes bundled with the managed services in the *ITSM Foundation Services Description*, which details standardized support communication channels, ticket management ("ITSM Tool"), service levels, as well as the governance, incident, change, problem, and escalation ITSM processes in support of the Service. Tickets will be securely visible to Client online, including status and updates, via Service Provider's ITSM Tool. See the *ITSM Foundation Services Description* for further details.

2. MICROSOFT IAM SERVICE

a) The Service provides comprehensive administration, proactive management, and ongoing support of identity and access controls across Client's Microsoft Environment. This includes management of on-premises Microsoft Active Directory Services (Domain Controllers, FSMO Roles, Group Policy Management, Authentication Protocols, and AD DNS), and/or Microsoft Entra ID Services (User/Group Management, MFA, SSO, Conditional Access Policies, PIM, Identity Protection, and Enterprise Applications), and/or Hybrid Identity synchronization components like Microsoft Entra Connect. Additionally, it encompasses the lifecycle management and operational support for Digital Certificates and Public Key Infrastructure (PKI) through Active Directory Certificate Services (AD CS), facilitating secure authentication and operations throughout the identity infrastructure.

b) Microsoft IAM offers options to manage Entra ID, Active Directory, Hybrid Identity (Entra ID + Active Directory), and Active Directory Certificate Servers of Client's Environment.

i. **Entra ID Service.** Provides management delivers secure and streamlined identity management for cloud-based services, covering user lifecycle management, group and permissions administration, multi-factor authentication (MFA), conditional access policies, single sign-on (SSO), and integration of enterprise applications. It ensures robust identity governance and secure access management across Client's Entra ID Environment.

ii. **Active Directory ("AD") Service.** Provides management offers proactive administration and support of on-premises Active Directory Environment. It covers domain controller health, authentication protocols (Kerberos, NTLM), replication, group policy management, domain trusts, and security best practices. The Service ensures critical identity infrastructure remains secure, reliable, and aligned with organizational policies.

iii. **Active Directory Certificate Server Service.** Provides management manages the lifecycle of digital certificates through Active Directory Certificate Services (AD CS) of the Client Environment. It covers provisioning, renewal, revocation, and troubleshooting to enable secure authentication, encryption, and reliable operations across digital identity and security ecosystem. The *Active Directory Certificate Server* service requires the purchase of the *Active Directory* Service or the *Hybrid Identity Service*.

iv. **Hybrid Identity Service.** Provides management manages identity synchronization between Client's on-premises Active Directory and Microsoft Entra ID Environment. The Service includes support and administration of Entra ID Connect, hybrid authentication management, and unified identity governance. This ensures consistent identity policies, streamlined user experiences, and enhanced security across both on-premises and cloud-based resources.

c) The monthly service fee will be calculated by multiplying the minimum contracted quantity of Identity Accounts at the end of the billing cycle by the applicable per unit rates documented in the *Pricing Summary*. For Hybrid Identity, the Identity Account quantity will equal the number of active accounts in Active Directory or the number of active accounts in Entra ID, whichever is greater. For Active Directory Certificate Server Service, the number of AD Certificate Server instances will be multiplied by the unit rate documented in the *Pricing Summary*. The minimum contracted quantities may be adjusted monthly based on the actual measured quantities if they exceed the minimum contracted quantity.

d) Additional service details can be found in sections, *GENERAL & ADDITIONAL RESPONSIBILITIES MATRICES*.

3. MICROSOFT 365 SERVICE

a) The Service provides comprehensive administration, proactive management, and ongoing support Client's Microsoft 365 Environment. This includes management of the Microsoft 365 tenant (subscriptions, domains, organizational settings), core communication and collaboration services (Exchange Online mailboxes, mail flow, security groups, Teams settings, SharePoint/OneDrive site settings), and security and compliance features within Microsoft Purview (data loss prevention, retention policies, sensitivity labels, eDiscovery). Additionally, it encompasses the management of integrated applications (enterprise apps, app registrations, conditional access controls) and regular environment health monitoring (Secure Score, Compliance Score, service health, license usage) to maintain optimal performance and security posture.

b) Microsoft 365 management comes bundled with Microsoft IAM (Entra ID or Hybrid Identity only) services to ensure secure, consistent identity governance of Client's Environment.

c) The monthly service fee will be calculated by multiplying the minimum contracted quantity of Full Users and Essentials Users at the end of the billing cycle by the applicable per unit rates documented in the *Pricing Summary*. The minimum contracted quantities may be adjusted monthly based on the actual measured quantities of Full Users and Essentials Users if they exceed the minimum contracted quantity.

d) Additional service details can be found in section *GENERAL & ADDITIONAL RESPONSIBILITIES MATRICES*.

4. OUT-OF-SCOPE SERVICES

a) The Service explicitly excludes:

i. Management of endpoint solutions (Intune, Autopilot, SCCM, and Operating Systems).

ii. Management of Microsoft Defender products, threat hunting, threat prevention, SIEM/SOAR solutions, security incident response, or other security related tasks.

iii. Management of Microsoft Teams telephony.

iv. Any functionality outside the scope of the Client's Microsoft licenses.

b) These out-of-scope services, if managed by Service Provider, will be separately billable.

5. RESPONSIBILITIES MATRIX EXPLANATION

a) When there is only an 'X' in the *Service Provider* column, the task is performed by Service Provider and the task effort is included in the monthly managed service fee.

b) When there is only an 'X' in the *Client* column, the task is performed by Client; it is not included in Service Provider's managed service fee. However, permanent or temporary delegation of such a task to Service Provider may be possible subject to: (i) Service Provider's acceptance to perform the task; and (ii) Client acceptance that the task effort is subject to additional billing.

c) When there is an 'X' in both the *Service Provider* and *Client* columns, there are shared responsibilities as outlined in the *Clarifications* column.

d) Tasks and services that are not included in the managed service fee, where the service or task effort is subject to additional billing, shall be noted in the *Clarifications* column.

e) Additional explanations concerning each task shall be noted in the *Clarifications* column.

f) *Optional Services* table lists tasks and services that are not included in the managed service fee, where the service or task effort is subject to additional billing.

5.1. GENERAL RESPONSIBILITIES MATRIX – MICROSOFT IAM & MICROSOFT 365

No.	Task Description	Service Provider	Client	Clarifications
1.	IT Asset Procurement, Ownership, and Vendor Support Management.	X (*)	X (*)	(*) For Client's IT Assets, Client shall procure and maintain a vendor support contract for the IT Assets during the term of the Service and replace IT Assets prior to end-of-life so that Service Provider can continue to perform the tasks required to deliver the Service as well as to continue to guarantee the service levels.
2.	Remote Admin Access & User Account Management.		X	Client shall grant Service Provider necessary and sufficient remote admin access to Client's Environment and IT Assets to perform the tasks required to deliver the Service.
3.	Audit Evidence Request Management.	X		Upon Client request, Service Provider delivers audit evidence for an IT Asset to fulfill a Client audit request.
4.	Operational Runbook Management.	X		Create and maintain operational runbook with specific work instructions on how to deliver the Service to Client.
5.	On-site (Remote Hands) Service Management.		X	When requested by Service Provider, provide hands-on physical support for an IT Asset in a Client location.
6.	Information Security Management.	X	X (*)	Service Provider's *Information Security Management Policy & Procedures* are maintained by Service Provider and apply to all Service Provider IT Assets used to deliver the Service. (*) Client's *Information Security Management Policy & Procedures* are maintained by Client and apply to all Client's IT Assets to which the Service is delivered.
7.	Event (Monitoring & Alert) Management.	X	X (*)	Monitoring & alerting on the IT Assets according to *Service Provider's Operational Monitoring Policies & Procedures*. (*) Client shall coordinate with Service Provider whenever they perform an IT Asset maintenance activity so that monitoring alerts can be turned off during the maintenance period.
8.	Incident, Escalation & Problem Management.	X	X (*)	Troubleshoot and resolve incidents with an IT Asset. Escalate to vendor support ("Level 3 Support") for an IT Asset, if needed. (*) For a Client's IT Asset, Client shall provide and maintain vendor support work instructions and vendor support portal access so that Service Provider can perform vendor support escalations on behalf of Client.

				Problem Management includes the creation of Root Cause Analysis Reports (RCAs) for an IT Asset incident with recommended corrective actions as part of Continual Service Improvement. Corrective actions are assigned to either Service Provider, Client, or vendor according to ownership of the corrective action. Failure by Client to promptly implement a corrective action that would either solve a critical security issue or the repetition of an incident may incur additional cost or reduce service levels.
9.	Operational Reporting Management.	X		Client may request operational reports from Service Provider on an ad-hoc basis to support the collaborative troubleshooting of an IT Asset incident.
10.	Standard Service Request Management.	X		Standard Service Requests can be submitted by Client or Service Provider. Standard service request tasks for an IT Asset are included in the Service at no additional fee. See *Additional Responsibilities Matrices* section below for enumerated standard service requests and any limitations thereof. Service Provider and Client perform standard service request tasks according to the task *Change Management* below.
11.	Change Management.	X	X (*)	Service Provider and Client shall follow change management process according to the section *Change Management* in the *ITSM Foundation Services Description.* Service Provider is responsible for technical change execution of Client-approved changes to an IT Asset. (*) Client is responsible for an IT Asset change approval, sending notifications to end users impacted by the change, and preparing before and testing after a change of any applications that may reside on or use the IT Asset that is being changed.
12.	Availability, Performance and Capacity Management.	X		Periodic reviews are performed with change recommendations to be implemented after approval from Client.
13.	Billable Service Request Management.	X		When performed by Service Provider, all labor effort and any material costs associated with the request are billed separately according to the *Change Order Request Procedure* in the applicable SOW. See *Additional Responsibilities Matrices* section below for enumerated billable service requests.

5.2. ADDITIONAL RESPONSIBILITIES MATRICES – MICROSOFT IAM

5.2.1. MICROSOFT ACTIVE DIRECTORY SERVICE

No.	Task Description	Service Provider	Client	Clarifications
1.	Procure licensing for Microsoft AD		X	
2.	Grant sufficient administration access to Service Provider so it can perform its responsibilities		X	Service Provider shall function as a subcontractor of Client under Client's Microsoft Service Agreements.
3.	User and Group Management	X	X (*)	(*) Client is responsible for first level support with the end-user. Service Provider will provide user account and group management as a level 2 option. For first level support Service Provider offers a Managed Service Desk offering.
4.	Maintain operational runbook based on Client-approved IAM & GPO Policies	X	X	Client provides and approves policies; Service Provider executes according to runbook.
5.	Create/Delete/Modify/Troubleshoot/Escalate Domain Controllers • Promote, demote, and restore	X		Management of IT assets below the AD application level (such as Server OS, networking, compute, and storage) are not in scope.

No.	Task Description	Service Provider	Client	Clarifications

6.	Create/Delete/Modify/Troubleshoot/Escalate Microsoft AD Domain Services based on incidents and Client-approved service requests:
	• FSMO Roles:
	  ○ Schema Master
	  ○ Domain Naming Master
	  ○ Relative ID (RID) Master
	  ○ Primary Domain Controller (PDC) Emulator
	  ○ Infrastructure Master
	• Authentication Protocols (i.e., Kerberos, NTLM)
	• AD Trust Domain
	• AD Sites and Services
	• Replication Topology
	• Privileged Access Management (PAM)
	• Group Policy Management (GPM)
	• User & Group Management (UM)
		X		

7.	Create/Delete/Modify/Troubleshoot/Escalate based on incidents and Client-approved service requests: • DNS connectivity • DNS zones • DNS resolution • DNS request latency • DNS record updates	X		
8.	Monthly reviews and recommendations: • Active Directory Health			

5.2.2. MICROSOFT ACTIVE DIRECTORY CERTIFICATE SERVER SERVICE

No.	Task Description	Service Provider	Client	Clarifications
1.	Procure licensing for Microsoft AD Certificate Services		X	
2.	Grant sufficient administration access to Service Provider so it can perform its responsibilities		X	Service Provider shall function as a subcontractor of Client under Client's Microsoft Service Agreements
3.	Maintain operational runbook based on Client-approved Digital Certificate Policies	X		Client provides and approves policies; Service Provider executes according to runbook.
4.	Create/Delete/Modify/Troubleshoot/Escalate Public Key Infrastructure ("PKI") & Digital Certificates based on incidents and Client-approved service requests: • Certification Authorities (CA's) • Web enrollment • Online Responder • Network Device Enrollment Service	X		Management of IT assets below the Certificate Services application level (such as Server OS, networking, compute, and storage) are not in scope.

5.2.3. MICROSOFT ENTRA ID SERVICE (INCLUDING HYBRID IDENTITY VIA ENTRA ID CONNECT, WHEN APPLICABLE)

No.	Task Description	Service Provider	Client	Clarifications
1.	Procure licensing for Microsoft AD		X	
2.	User and Group Management	X	X (*)	(*) Client is responsible for first level support with the end-user. Service Provider will provide user account and group management as a level 2 option. For first level support Service Provider offers a Managed Service Desk offering.
3.	Create/Delete/Modify/Troubleshoot/Escalate Entra ID Services such as: • User & Group Management	X		

No.	Task Description	Service Provider	Client	Clarifications
	• Authentication Protocols (OAuth) • MFA • SSO • Entra ID Self-Service Password Reset (SSPR) • Privileged Identity Management (PIM) • Enterprise Applications/App Registrations (API's) • Identity Governance • Licensing & Subscriptions assignments • Conditional Access Policies • Identity Protection • Risky sign-ins • Identity Secure Score			
4.	Modify/Troubleshoot/Escalate Microsoft Entra Connect (formerly Azure AD Connect). • Entra Cloud Sync • ADFS integrated Entra Connect • Alert and response for Entra ID Connect	X	X (*)	(*) Integrations, new deployments, mergers & acquisitions, and other work requiring design or project effort are outside the scope of this service.
5.	Create/Delete/Modify/Troubleshoot/Escalate Role-Based Access Controls (RBAC).	X		
6.	Monthly reviews and recommendations: • Microsoft Identity Score • Entra ID review (MFA, risky sign-ins, etc.) • AD Synchronization health (hybrid service option only)	X		

5.3. ADDITIONAL RESPONSIBILITIES MATRICES (MICROSOFT 365)

5.3.1. MICROSOFT 365 TENANT AND SUBSCRIPTION SERVICE

No.	Task Description	Service Provider	Client	Clarifications
1.	Procure & Maintain M365 subscriptions according to the Microsoft Agreement.		X	
2.	Manage M365 subscriptions such as: • Assign/Remove licenses • Create/Modify/Remove user templates	X		
3.	Manage domain settings within the Microsoft tenant: • Add/Verify/Remove domain • Provide DNS records	X		
4.	Manage domain procurement and DNS records: • Create/Delete/Modify/Troubleshoot/ Escalate DNS entries with domain registrar • Procure domain • Track and process domain renewals		X (*)	Service Provider may offer additional services to extend the management and support of Client's domain and DNS needs. (*) Service Provider will advise on topics specific to M365 and methods to achieve the desired outcomes but will not directly manage external DNS setting or work directly with the domain registrar.
5.	Manage organizational and tenant wide settings.	X		

5.3.2. MICROSOFT 365 PURVIEW SERVICE

No.	Task Description	Service Provider	Client	Clarifications
1.	Create/Delete/Modify/Troubleshoot/Escalate *data sensitivity labeling* admin settings.	X		

No.	Task Description	Service Provider	Client	Clarifications
2.	Execute *eDiscovery cases and holds* using M365 built-in features, such as Content search, core eDiscovery and Advanced eDiscovery.	X		
3.	Create/Modify/Remove Client requested policies such as: • Data Loss Prevention (DLP) • Data Retention • Sensitivity Labels and Encryption • eDiscovery and Legal Hold • Audit Logs	X	X	Policies will generally require information from Client to successfully implement and achieve the desired outcome. Some complex policies may require additional billable services when advanced engineering or architect expertise is required to design a policy-based solution.

5.3.3. MICROSOFT 365 INTEGRATED APPS SERVICE

No.	Task Description	Service Provider	Client	Clarifications
1.	Create/Delete/Modify/Troubleshoot/Escalate • Org settings • Integrated Apps settings • Enterprise Apps (*) • App Registrations (*) • Conditional Access controls • Access reviews	X		(*) Requires the application to be available via the Microsoft Entra Gallery catalog or is a supported SAML application with available documentation.
2.	Create/Delete/Modify/Troubleshoot/Escalate search and intelligence settings.	X		

5.3.4. MICROSOFT 365 EXCHANGE ONLINE SERVICE

No.	Task Description	Service Provider	Client	Clarifications
1.	Manage Mailbox requests such as: • Create/Modify/Delete a shared mailbox • Create/Modify/Delete a mail contact • Create/Modify/Delete a mail user • Setup Free/Busy calendar information • Configure mailbox permissions • Configure mailbox archive settings • Configure mailbox delegation • Configure data retention	X		
2.	Manage Mail Flow and Routing requests such as: • Create/Modify/Delete mail flow rule • Create/Modify/Delete message trace • Create/Modify/Delete mail connector • Configure email forwarding • Configure aliases	X		
3.	Manage Group and Resource requests such as: • Create/Modify/Delete M365 Group • Create/Modify/Delete distribution list • Create/Modify/Delete dynamic distribution list • Create/Modify/Delete mail-enables security group • Create/Modify/Delete room resource • Create/Modify/Delete equipment resource • Configure shared resource permissions • Configure booking policies	X		
4.	Create/Delete/Modify/Troubleshoot/Escalate Exchange Online protection requests such as: • Connection filter • Malware filter • Spam exception filter • Quarantine filter	X		

No.	Task Description	Service Provider	Client	Clarifications
	• Message size restrictions • Message delivery restrictions • Tenant Allow/Block lists • Quarantine • Anti-Spam/Malware/Phishing (Threat Policies)			
5.	Create/Delete/Modify/Troubleshoot/Escalate hold, retention, and recovery settings for mailboxes using built-in Exchange features such as: • Litigation hold • eDiscovery hold • In-Place hold	X		

5.3.5. MICROSOFT 365 ONEDRIVE AND SHAREPOINT SERVICE

No.	Task Description	Service Provider	Client	Clarifications
1.	Tenant-Level Configuration • Configure tenant-level sharing, notifications, storage limits, and standard policies • Apply changes to tenant-level SharePoint and OneDrive settings impacting existing sites/users.	X(*)	X(**)	(*) Operational adjustments only. Excludes governance program design. (**) Client defines governance, retention, and compliance policies. Client approves policy changes before implementation.
2.	User-Level Tasks • Add/remove users or groups; update membership; sync permissions. • Troubleshoot access and sharing issues (internal/external). • Manage OneDrive issues: sync failures, client errors, sign-in issues, Known Folder Move troubleshooting.	X	X(*)	(*) Client provides correct access decisions and requirements.
3.	Content-Level Tasks • Create SharePoint Site, Team, or Teams Channel using existing approved template or approved provisioning processes. • Update existing SharePoint pages, navigation links, and web parts. • Modify existing SharePoint lists/libraries: columns, views, metadata, versioning. • Correct broken links, references, or file paths in existing structures. • Restore deleted OneDrive or SharePoint files/folders; restore document versions. • Manage OneDrive folder sharing, link settings, and access corrections.	X(*)	X(**)	(*) Intention is to provide incremental adjustments only. (**) Client provides approved content and validates accuracy after publication.
4.	Manage Teams - SharePoint integration (Files tab, folder structure, membership sync)	X		
5.	Project, development, or program management work such as: • Creation of new templates or customized site designs. • Custom creation of any asset. • Content Creation. • Branding and design. • Migrations of any kind. • Custom forms/apps (Power Apps). • Automation (Power Automate). • Restructuring architecture, data, or security. • Custom development such as SPFx, webparts, scripts, APIs, or third-party integrations.	(*)	X	(*) Service Provider may offer separately billable services or project engagements to offer these capabilities.

5.3.6. MICROSOT 365 TEAMS SERVICE

No.	Task Description	Service Provider	Client	Clarifications
1.	Manage Teams settings requests such as: • Create/Delete Team • Add/Remove team owner • Add/Remove team member • Create/Modify/Delete Teams policy • Create/Modify/Delete Team templates • Configure message Settings • Configure meeting Settings	X		Service Provider performs Teams Admin in general but not per Team. The actual Teams and their Channels are managed by the Client Team Owners.
2.	Manage Teams access settings such as: • Configure user settings • Configure guest access • Configure external access • Configure rooms	X		
3.	Manage Microsoft Teams Telephony such as voice routing infrastructure, E911, call quality, and quality of service configurations.		X	Service Provider may offer additional services for the management of Microsoft Teams Telephony and Calling.

5.3.7. MICROSOFT 365 HEALTH REVIEWS SERVICE

No.	Task Description	Service Provider	Client	Clarifications
1.	Complete monthly reviews, generate recommendations, and present during a monthly service check-in meeting: • Microsoft Purview Compliance score • Microsoft Secure score • Microsoft 365 Environment Service Health • OneDrive/SharePoint health and storage • License usage	X		
2.	Complete a weekly review of the Service Health portal and communicate any relevant findings.	X		

5.4. BILLABLE SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Perform any service request that is not explicitly designated as Service Provider's responsibility in the *General Responsibilities Matrix*, a task not included in the service offering level assigned to the Resource or not enumerated in the *Standard Service Requests* table above.	X		
2.	Perform any task that is explicitly designated as Client's responsibility in the *General Responsibilities Matrix*.	X		
3.	Design, architect, engineer, develop, integrate or implement new functionality into the Environment.	X		
4.	Train end-users in Microsoft applications and services.	X		
5.	Provide end user service desk functions.	X		
6.	Perform Microsoft project-based activities such as mergers/acquisitions, deployment of new services, tenant migration, directory synchronization.	X		e.g.: Power Automate, Power Apps development and ongoing support

No.	Task Description	Service Provider	Client	Clarifications
7.	Provide access to billable support or project activities from Microsoft.	X		
8.	Migrate new workloads into the Environment (e.g., Email or File).	X		
9.	Migrate data or functionality from one M365 service to another (e.g., OneDrive to Teams).	X		

MMW-1: CLIENT-SPECIFIC DETAILS

a) The below client M365 tenant IDs will correlate to one or more-line items in the *Pricing Summary*.

No.	Tenant ID	Domains
1.	• <ID1>	• <Domain 1> • <Domain 2>
2.	• <ID2>	• <Domain 1> • <Domain 2>

b) Active Directory services within the below domains will correlate to one or more-line items in the *Pricing Summary*.

No.	Domain Name
1.	• <Domain 1>
2.	• <Domain 2>

c) Service Provider will utilize Nerdio Manager which requires access to the Microsoft 365 tenant and on-premises Active Directory domains. If Client does not permit access to Nerdio Manager some features of the service may not be available or price adjustments on the *Pricing Summary* may be required.

Exhibit 6:

MIS - APPS & TOOLS
SERVICE DESCRIPTION
REV 2025-08-30

1. SERVICE OVERVIEW

a) The MIS "Apps & Tools" service shall remotely manage IT Assets that are technical applications and tools such as IIS, DC, DNS, DHCP, File and Print Server, as documented in the *Pricing Summary* of the SOW.

2. RESPONSIBILITIES MATRIX

2.1. EXPLANATION

a) The *General Responsibilities Matrix* section covers the overall steady state ITSM lifecycle tasks to deliver the Service.

b) The *Additional Responsibilities Matrices* section enumerates standard and billable service request management tasks related to the Service.

c) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in the Service. Any limitations shall be detailed in the *Clarifications* column.

d) An 'X' in the *Client* column means Client is responsible for the task.

e) When an 'X' is in both the *Service Provider* and *Client* columns, '(*)' means that there is a specific clarification for Client and '(**)' means that there is a specific clarification for Service Provider in the *Clarifications* column.

2.2. GENERAL RESPONSIBILITIES MATRIX

No.	Task Description	Service Provider	Client	Clarifications
1.	IT Asset Procurement, Ownership, and Vendor Support Management.		X	For Client's IT Assets, Client shall procure and maintain vendor support contracts during the term of the Service, replacing IT Assets prior to end-of-life so that Service Provider can continue to perform the tasks required to deliver the Service as well as to continue to guarantee the service levels. All IT Assets in the SOW are assumed to be Client's IT Assets, unless documented in the SOW. Excluded: Service Provider procured, owned, and maintained IT Assets, unless documented in the SOW. Excluded: Underlying IT infrastructure for running the IT Assets are not in scope of the Service, unless documented in the SOW.
2.	Remote Admin Access & User Account Management.		X	Client shall grant Service Provider necessary and sufficient remote admin access to Client's network and IT Assets to perform the tasks required to deliver the Service.
3.	Audit Evidence Request Management.	X		Upon Client request, Service Provider delivers audit evidence for an IT Asset to fulfill a Client audit request. Excluded: more than one (1) request per calendar year, unless documented in the SOW.
4.	Operational Runbook Management.	X		Create and maintain operational runbook with specific work instructions on how to deliver the Service to Client.

				Excluded: Customize operational runbook documentation or create additional documentation, unless documented in the SOW.
5.	On-site (Remote Hands) Service Management.		X	When requested by Service Provider, provide hands-on physical support for an IT Asset in a Client location.
6.	Information Security Management.	X (**)	X (*)	(*) Client's *Information Security Management Policy & Procedures* are maintained by Client and apply to all Client's IT Assets to which the Service is delivered. (**) Service Provider's *Information Security Management Policy & Procedures* are maintained by Service Provider and apply to all Service Provider IT Assets used to deliver the Service. Excluded: Customize *Service Provider's Information Security Management Policy & Procedures*, unless documented in the SOW.
7.	Event (Monitoring & Alert) Management.	X		Monitoring & alerting on the IT Assets according to *Service Provider's Operational Monitoring Policies & Procedures*. Excluded: Customize *Service Provider's Operational Monitoring Policies & Procedures,* unless documented in the SOW.
8.	Incident, Escalation & Problem Management.	X	X (*)	Service Provider is responsible for troubleshooting and resolving incidents on an IT Asset. Escalate to vendor support ("Level 3 Support") for an IT Asset, if needed. (*) For a Client's IT Asset, Client shall provide and maintain vendor support work instructions and vendor support portal access so that Service Provider can perform vendor support escalations on behalf of Client. Problem Management includes the creation of Root Cause Analysis Reports (RCAs) for an IT Asset incident with recommended corrective actions as part of Continual Service Improvement. Corrective actions are assigned to either Service Provider, Client, or vendor according to ownership of the corrective action.
9.	Operational Reporting Management.	X		Client may request operational reports from Service Provider on an ad-hoc basis to support the collaborative troubleshooting of an IT Asset incident. Excluded: Client-specific operational reports on a regular basis, unless documented in the SOW.
10.	Standard Service Request Management.	X		Standard service requests can be submitted by Client or Service Provider. Standard service request tasks for an IT Asset are included in the Service at no additional fee. See *Additional Responsibilities Matrices* section below for enumerated standard service requests and any exclusion thereof, as

				a well as enumerated billable service requests. Service Provider and Client perform standard service request tasks according to the task *Change Management* below.
11.	Change Management.	X (**)	X (*)	Service Provider and Client shall follow change management process according to the section *Change Management* in the *Managed Services ITSM Foundation Service Description.* (**) Service Provider is responsible for technical change execution of Client-approved changes to an IT Asset. (*) Client is responsible for an IT Asset change approval, sending notifications to end users impacted by the change, and preparing before and testing after a change of any applications that may reside on or use the IT Asset that is being changed.
12.	Availability, Performance and Capacity Management.	X		Periodic reviews are performed with change recommendations to be implemented after approval from Client. Excluded: Expand or replace IT Asset to improve availability, performance, or capacity.
13.	Patch Management.	X	X (*)	Service Provider performs patching according to the patch frequency of *Service Provider's Operational Patch Management Policy & Procedures*, unless documented in the SOW. Client and Service Provider shall perform patch approval and execution according to the task above*, Change Management.* (*) Client shall grant access to Service Provider to use Client's centralized patch management solution if the IT Asset is or can be patched using such a solution. If no such solution exists, the IT Asset may then be patched manually by Service Provider. Use of Client's centralized patch management solution is limited to in-scope IT Assets. Ad-hoc patching outside the defined patch frequency is included in the Service if an IT Asset is evaluated to be an "Urgent Critical" target for a cyberattack (e.g., an Internet-facing IT Asset), whereby the patch would eliminate the vulnerability; or the patch will fix a bug that is severely impacting the availability or normal operation of a critical IT Asset. The patch must have been released from the vendor before it can be deployed. Excluded: Customize Service Provider's *Operational Patch Management Policy & Procedures*, unless documented in the SOW. Excluded: Apply an ad-hoc patch to an IT Asset outside the defined standard patch frequency and not designated as an "Urgent Critical" patch, unless documented in the SOW.

				Excluded: Apply upgrades to an IT Asset, unless documented in the SOW.
14.	Continuity (Backup & Restore) Management.		X	Client shall ensure that IT Assets have backups in case an IT Asset must be restored to resolve an incident, unless this task is provided by Service Provider, as documented in an SOW.
15.	Continuity (HA/DR Test) Management.	X (**)	X (*)	(**) Only when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are also in scope of the Service, then Service Provider is responsible as follows. Up to one (1) Client-requested HA/DR test per calendar year is included in the Service. Service Provider performs its technical tasks according to *Client's HA/DR Test Plan Procedure.* (*) Client is responsible for creating and maintaining the *HA/DR Test Plan Procedure*, with Service Provider providing feedback on its tasks as requested by Client. (*) Client is responsible for preparing before and testing after a HA/DR test of any applications that may reside on or use the HA/DR IT Assets. Excluded: when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are not in scope of the Service. Excluded: Perform more than 1 HA/DR Test per calendar year or effort related to an actual HA/DR event, unless documented in the SOW.
16.	Billable Service Request Management.	X		When performed by Service Provider, all labor effort and any material costs associated with the request are billed separately according to the *Change Order Request Procedure* in the SOW. All exclusions listed for tasks in this *General Responsibilities Matrix* are considered billable service requests. See *Additional Responsibilities Matrices* section below for enumerated billable service requests.

2.3. ADDITIONAL RESPONSIBILITIES MATRICES

2.3.1. STANDARD SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Start/Shutdown/Restart an IT Asset.	X		
2.	Configure an IT Asset.	X		

2.3.2. BILLABLE SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Perform any task that is explicitly stated as a responsibility of Client or not explicitly stated as a task of Service Provider.	X		
2.	Perform an "Excluded" activity listed for a task.	X		
3.	Deliver a new service not in scope of this Service.	X		
4.	Deploy or build a new IT Asset (i.e., an increase in contractual quantity of the Service).	X		
5.	Deprovision an IT Asset (i.e., a decrease in the contractual quantity of the Service).	X		
6.	Replace an IT Asset with a new IT Asset.	X		
7.	Perform corrective actions or restoration efforts (e.g. from data restore) of an IT Asset where the root cause is not attributable Service Provider's action.	X		
8.	Perform design, engineering, and consulting work in relation to an existing or new Client IT Asset or Client's overall IT environment.	X		
9.	Develop, install, monitor, and maintain customized or third-party tools, scripts, and software installed on an IT Asset.	X		

Exhibit 7:

MIS - STORAGE
SERVICE DESCRIPTION
REV 2025-08-30

1. SERVICE OVERVIEW

a) The MIS "Storage" services shall remotely manage IT Assets such as DAS, NAS, SAN, magnetic tape, and/or optical data storage, as documented in the *Pricing Summary* of the SOW.

2. RESPONSIBILITIES MATRIX

2.1. EXPLANATION

a) The *General Responsibilities Matrix* section covers the overall steady state ITSM lifecycle tasks to deliver the Service.

b) The *Additional Responsibilities Matrices* section enumerates standard and billable service request management tasks related to the Service.

c) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in the Service. Any limitations shall be detailed in the *Clarifications* column.

d) An 'X' in the *Client* column means Client is responsible for the task.

e) When an 'X' is in both the *Service Provider* and *Client* columns, '(*)' means that there is a specific clarification for Client and '(**)' means that there is a specific clarification for Service Provider in the *Clarifications* column.

2.2. GENERAL RESPONSIBILITIES MATRIX

No.	Task Description	Service Provider	Client	Clarifications
1.	IT Asset Procurement, Ownership, and Vendor Support Management.		X	For Client's IT Assets, Client shall procure and maintain vendor support contracts during the term of the Service, replacing IT Assets prior to end-of-life so that Service Provider can continue to perform the tasks required to deliver the Service as well as to continue to guarantee the service levels. All IT Assets in the SOW are assumed to be Client's IT Assets, unless documented in the SOW. Excluded: Service Provider procured, owned, and maintained IT Assets, unless documented in the SOW. Excluded: Underlying IT infrastructure for running the IT Assets are not in scope of the Service, unless documented in the SOW.
2.	Remote Admin Access & User Account Management.		X	Client shall grant Service Provider necessary and sufficient remote admin access to Client's network and IT Assets to perform the tasks required to deliver the Service.
3.	Audit Evidence Request Management.	X		Upon Client request, Service Provider delivers audit evidence for an IT Asset to fulfill a Client audit request. Excluded: more than one (1) request per calendar year, unless documented in the SOW.
4.	Operational Runbook Management.	X		Create and maintain operational runbook with specific work instructions on how to deliver the Service to Client. Excluded: Customize operational runbook documentation or create additional documentation, unless documented in the SOW.

5.	On-site (Remote Hands) Service Management.		X	When requested by Service Provider, provide hands-on physical support for an IT Asset in a Client location.
6.	Information Security Management.	X (**)	X (*)	(*) Client's Information Security Management Policy & Procedures are maintained by Client and apply to all Client's IT Assets to which the Service is delivered. (**) Service Provider's Information Security Management Policy & Procedures are maintained by Service Provider and apply to all Service Provider IT Assets used to deliver the Service. Excluded: Customize Service Provider's Information Security Management Policy & Procedures, unless documented in the SOW.
7.	Event (Monitoring & Alert) Management.	X		Monitoring & alerting on the IT Assets according to Service Provider's Operational Monitoring Policies & Procedures. Excluded: Customize Service Provider's Operational Monitoring Policies & Procedures, unless documented in the SOW.
8.	Incident, Escalation & Problem Management.	X	X (*)	Service Provider is responsible for troubleshooting and resolving incidents on an IT Asset. Escalate to vendor support ("Level 3 Support") for an IT Asset, if needed. (*) For a Client's IT Asset, Client shall provide and maintain vendor support work instructions and vendor support portal access so that Service Provider can perform vendor support escalations on behalf of Client. Problem Management includes the creation of Root Cause Analysis Reports (RCAs) for an IT Asset incident with recommended corrective actions as part of Continual Service Improvement. Corrective actions are assigned to either Service Provider, Client, or vendor according to ownership of the corrective action.
9.	Operational Reporting Management.	X		Client may request operational reports from Service Provider on an ad-hoc basis to support the collaborative troubleshooting of an IT Asset incident. Excluded: Client-specific operational reports on a regular basis, unless documented in the SOW.
10.	Standard Service Request Management.	X		Standard service requests can be submitted by Client or Service Provider. Standard service request tasks for an IT Asset are included in the Service at no additional fee. See *Additional Responsibilities Matrices* section below for enumerated standard service requests and any exclusion thereof, as a well as enumerated billable service requests. Service Provider and Client perform standard service request tasks according to the task *Change Management* below.
11.	Change Management.	X (**)	X (*)	Service Provider and Client shall follow change management process according to the section *Change Management* in the *Managed Services ITSM Foundation* Service *Description.* (**) Service Provider is responsible for technical change execution of Client-approved changes to an IT Asset. (*) Client is responsible for an IT Asset change approval, sending notifications to end users impacted by the change, and preparing before and testing after a change of any applications that may reside on or use the IT Asset that is being changed.
12.	Availability, Performance and Capacity Management.	X		Periodic reviews are performed with change recommendations to be implemented after approval from Client.

				Excluded: Expand or replace IT Asset to improve availability, performance, or capacity.
13.	Patch Management.	X	X (*)	Service Provider performs patching according to the patch frequency of *Service Provider's Operational Patch Management Policy & Procedures*, unless documented in the SOW. Client and Service Provider shall perform patch approval and execution according to the task above*, Change Management.* (*) Client shall grant access to Service Provider to use Client's centralized patch management solution if the IT Asset is or can be patched using such a solution. If no such solution exists, the IT Asset may then be patched manually by Service Provider. Use of Client's centralized patch management solution is limited to in-scope IT Assets. Ad-hoc patching outside the defined patch frequency is included in the Service if an IT Asset is evaluated to be an "Urgent Critical" target for a cyberattack (e.g., an Internet-facing IT Asset), whereby the patch would eliminate the vulnerability; or the patch will fix a bug that is severely impacting the availability or normal operation of a critical IT Asset. The patch must have been released from the vendor before it can be deployed. Excluded: Customize Service Provider's *Operational Patch Management Policy & Procedures*, unless documented in the SOW. Excluded: Apply an ad-hoc patch to an IT Asset outside the defined standard patch frequency and not designated as an "Urgent Critical" patch*,* unless documented in the SOW. Excluded: Apply upgrades to an IT Asset*,* unless documented in the SOW.
14.	Continuity (Backup & Restore) Management.		X	Client shall ensure that IT Assets have backups in case an IT Asset must be restored to resolve an incident, unless this task is provided by Service Provider, as documented in an SOW.
15.	Continuity (HA/DR Test) Management.	X (**)	X (*)	(**) Only when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are also in scope of the Service, then Service Provider is responsible as follows. Up to one (1) Client-requested HA/DR test per calendar year is included in the Service. Service Provider performs its technical tasks according to Client's HA/DR Test Plan Procedure. (*) Client is responsible for creating and maintaining the HA/DR Test Plan Procedure, with Service Provider providing feedback on its tasks as requested by Client. (*) Client is responsible for preparing before and testing after a HA/DR test of any applications that may reside on or use the HA/DR IT Assets. Excluded: when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are not in scope of the Service. Excluded: Perform more than 1 HA/DR Test per calendar year or effort related to an actual HA/DR event, unless documented in the SOW.

16.	Billable Service Request Management.	X		When performed by Service Provider, all labor effort and any material costs associated with the request are billed separately according to the Change Order Request Procedure in the SOW. All exclusions listed for tasks in this General Responsibilities Matrix are considered billable service requests. See Additional Responsibilities Matrices section below for enumerated billable service requests.

2.3. ADDITIONAL RESPONSIBILITIES MATRICES

2.3.1. STANDARD SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Start/Shutdown/Restart an IT Asset.	X		
2.	Configure an IT Asset.	X		

2.3.2. BILLABLE SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Perform any task that is explicitly stated as a responsibility of Client or not explicitly stated as a task of Service Provider.	X		
2.	Perform an “Excluded” activity listed for a task.	X		
3.	Deliver a new service not in scope of this Service.	X		
4.	Deploy or build a new IT Asset (i.e., an increase in contractual quantity of the Service).	X		
5.	Deprovision an IT Asset (i.e., a decrease in the contractual quantity of the Service).	X		
6.	Replace an IT Asset with a new IT Asset.	X		
7.	Perform corrective actions or restoration efforts (e.g. from data restore) of an IT Asset where the root cause is not attributable Service Provider’s action.	X		
8.	Perform design, engineering, and consulting work in relation to an existing or new Client IT Asset or Client’s overall IT environment.	X		
9.	Develop, install, monitor, and maintain customized or third-party tools, scripts, and software installed on an IT Asset.	X		

Exhibit 8:

MIS - PHYSICAL COMPUTE
SERVICE DESCRIPTION
REV 2025-08-30

1. SERVICE OVERVIEW

a) The MIS "Physical Compute" services shall remotely manage physical compute server hardware running bare metal operating systems or hypervisors IT Assets, as documented in the *Pricing Summary* of the SOW.

2. RESPONSIBILITIES MATRIX

2.1. EXPLANATION

a) The *General Responsibilities Matrix* section covers the overall steady state ITSM lifecycle tasks to deliver the Service.

b) The *Additional Responsibilities Matrices* section enumerates standard and billable service request management tasks related to the Service.

c) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in the Service. Any limitations shall be detailed in the *Clarifications* column.

d) An 'X' in the *Client* column means Client is responsible for the task.

e) When an 'X' is in both the *Service Provider* and *Client* columns, '(*)' means that there is a specific clarification for Client and '(**)' means that there is a specific clarification for Service Provider in the *Clarifications* column.

2.2. GENERAL RESPONSIBILITIES MATRIX

No.	Task Description	Service Provider	Client	Clarifications
1.	IT Asset Procurement, Ownership, and Vendor Support Management.		X	For Client's IT Assets, Client shall procure and maintain vendor support contracts during the term of the Service, replacing IT Assets prior to end-of-life so that Service Provider can continue to perform the tasks required to deliver the Service as well as to continue to guarantee the service levels. All IT Assets in the SOW are assumed to be Client's IT Assets, unless documented in the SOW. Excluded: Service Provider procured, owned, and maintained IT Assets, unless documented in the SOW. Excluded: Underlying IT infrastructure for running the IT Assets are not in scope of the Service, unless documented in the SOW.
2.	Remote Admin Access & User Account Management.		X	Client shall grant Service Provider necessary and sufficient remote admin access to Client's network and IT Assets to perform the tasks required to deliver the Service.
3.	Audit Evidence Request Management.	X		Upon Client request, Service Provider delivers audit evidence for an IT Asset to fulfill a Client audit request. Excluded: more than one (1) request per calendar year, unless documented in the SOW.
4.	Operational Runbook Management.	X		Create and maintain operational runbook with specific work instructions on how to deliver the Service to Client.

				Excluded: Customize operational runbook documentation or create additional documentation, unless documented in the SOW.
5.	On-site (Remote Hands) Service Management.		X	When requested by Service Provider, provide hands-on physical support for an IT Asset in a Client location.
6.	Information Security Management.	X (**)	X (*)	(*) Client's Information Security Management Policy & Procedures are maintained by Client and apply to all Client's IT Assets to which the Service is delivered. (**) Service Provider's Information Security Management Policy & Procedures are maintained by Service Provider and apply to all Service Provider IT Assets used to deliver the Service. Excluded: Customize Service Provider's Information Security Management Policy & Procedures, unless documented in the SOW.
7.	Event (Monitoring & Alert) Management.	X		Monitoring & alerting on the IT Assets according to Service Provider's Operational Monitoring Policies & Procedures. Excluded: Customize Service Provider's Operational Monitoring Policies & Procedures, unless documented in the SOW.
8.	Incident, Escalation & Problem Management.	X	X (*)	Service Provider is responsible for troubleshooting and resolving incidents on an IT Asset. Escalate to vendor support ("Level 3 Support") for an IT Asset, if needed. (*) For a Client's IT Asset, Client shall provide and maintain vendor support work instructions and vendor support portal access so that Service Provider can perform vendor support escalations on behalf of Client. Problem Management includes the creation of Root Cause Analysis Reports (RCAs) for an IT Asset incident with recommended corrective actions as part of Continual Service Improvement. Corrective actions are assigned to either Service Provider, Client, or vendor according to ownership of the corrective action.
9.	Operational Reporting Management.	X		Client may request operational reports from Service Provider on an ad-hoc basis to support the collaborative troubleshooting of an IT Asset incident. Excluded: Client-specific operational reports on a regular basis, unless documented in the SOW.
10.	Standard Service Request Management.	X		Standard service requests can be submitted by Client or Service Provider. Standard service request tasks for an IT Asset are included in the Service at no additional fee. See Additional Responsibilities Matrices section below for enumerated standard service requests and any exclusion thereof, as a well as enumerated billable service requests. Service Provider and Client perform standard service request tasks according to the task Change Management below.
11.	Change Management.	X (**)	X (*)	Service Provider and Client shall follow change management process according to the section Change Management in the Managed Services ITSM Foundation Service Description. (**) Service Provider is responsible for technical change execution of Client-approved changes to an IT Asset. (*) Client is responsible for an IT Asset change approval, sending notifications to end users impacted by the change, and preparing before and testing after a change of any applications that may reside on or use the IT Asset that is being changed.
12.	Availability, Performance and Capacity Management.	X		Periodic reviews are performed with change recommendations to be implemented after approval from Client.

				Excluded: Expand or replace IT Asset to improve availability, performance, or capacity.
13.	Patch Management.	X	X (*)	Service Provider performs patching according to the patch frequency of Service Provider's Operational Patch Management Policy & Procedures, unless documented in the SOW. Client and Service Provider shall perform patch approval and execution according to the task above, Change Management. (*) Client shall grant access to Service Provider to use Client's centralized patch management solution if the IT Asset is or can be patched using such a solution. If no such solution exists, the IT Asset may then be patched manually by Service Provider. Use of Client's centralized patch management solution is limited to in-scope IT Assets. Ad-hoc patching outside the defined patch frequency is included in the Service if an IT Asset is evaluated to be an "Urgent Critical" target for a cyberattack (e.g., an Internet-facing IT Asset), whereby the patch would eliminate the vulnerability; or the patch will fix a bug that is severely impacting the availability or normal operation of a critical IT Asset. The patch must have been released from the vendor before it can be deployed. Excluded: Customize Service Provider's Operational Patch Management Policy & Procedures, unless documented in the SOW. Excluded: Apply an ad-hoc patch to an IT Asset outside the defined standard patch frequency and not designated as an "Urgent Critical" patch, unless documented in the SOW. Excluded: Apply upgrades to an IT Asset, unless documented in the SOW.
14.	Continuity (Backup & Restore) Management.		X	Client shall ensure that IT Assets have backups in case an IT Asset must be restored to resolve an incident, unless this task is provided by Service Provider, as documented in an SOW.
15.	Continuity (HA/DR Test) Management.	X (**)	X (*)	(**) Only when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are also in scope of the Service, then Service Provider is responsible as follows. Up to one (1) Client-requested HA/DR test per calendar year is included in the Service. Service Provider performs its technical tasks according to Client's HA/DR Test Plan Procedure. (*) Client is responsible for creating and maintaining the HA/DR Test Plan Procedure, with Service Provider providing feedback on its tasks as requested by Client. (*) Client is responsible for preparing before and testing after a HA/DR test of any applications that may reside on or use the HA/DR IT Assets. Excluded: when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are not in scope of the Service. Excluded: Perform more than 1 HA/DR Test per calendar year or effort related to an actual HA/DR event, unless documented in the SOW.
16.	Billable Service Request Management.	X		When performed by Service Provider, all labor effort and any material costs associated with the request are billed separately according to the Change Order Request Procedure in the SOW. All exclusions listed for tasks in this General Responsibilities Matrix are considered billable service requests. See Additional Responsibilities Matrices section below for enumerated billable service requests.

2.3. ADDITIONAL RESPONSIBILITIES MATRICES

2.3.1. STANDARD SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Start/Shutdown/Restart an IT Asset.	X		
2.	Configure an IT Asset.	X		

2.3.2. BILLABLE SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Perform any task that is explicitly stated as a responsibility of Client or not explicitly stated as a task of Service Provider.	X		
2.	Perform an "Excluded" activity listed for a task.	X		
3.	Deliver a new service not in scope of this Service.	X		
4.	Deploy or build a new IT Asset (i.e., an increase in contractual quantity of the Service).	X		
5.	Deprovision an IT Asset (i.e., a decrease in the contractual quantity of the Service).	X		
6.	Replace an IT Asset with a new IT Asset.	X		
7.	Perform corrective actions or restoration efforts (e.g. from data restore) of an IT Asset where the root cause is not attributable Service Provider's action.	X		
8.	Perform design, engineering, and consulting work in relation to an existing or new Client IT Asset or Client's overall IT environment.	X		
9.	Develop, install, monitor, and maintain customized or third-party tools, scripts, and software installed on an IT Asset.	X		

Exhibit 9:

MIS - VIRTUAL COMPUTE
SERVICE DESCRIPTION
REV 2025-08-30

1. SERVICE OVERVIEW

a) The MIS "Virtual Compute" services remotely manage virtualization IT Assets such as virtualization technologies and virtual machines running on Type 1 hypervisors like VMware ESXi or Microsoft Hyper-V, as documented in the *Pricing Summary* of the SOW.

2. RESPONSIBILITIES MATRIX

2.1. EXPLANATION

a) The *General Responsibilities Matrix* section covers the overall steady state ITSM lifecycle tasks to deliver the Service.

b) The *Additional Responsibilities Matrices* section enumerates standard and billable service request management tasks related to the Service.

c) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in the Service. Any limitations shall be detailed in the *Clarifications* column.

d) An 'X' in the *Client* column means Client is responsible for the task.

e) When an 'X' is in both the *Service Provider* and *Client* columns, '(*)' means that there is a specific clarification for Client and '(**)' means that there is a specific clarification for Service Provider in the *Clarifications* column.

2.2. GENERAL RESPONSIBILITIES MATRIX

No.	Task Description	Service Provider	Client	Clarifications
1.	IT Asset Procurement, Ownership, and Vendor Support Management.		X	For Client's IT Assets, Client shall procure and maintain vendor support contracts during the term of the Service, replacing IT Assets prior to end-of-life so that Service Provider can continue to perform the tasks required to deliver the Service as well as to continue to guarantee the service levels. All IT Assets in the SOW are assumed to be Client's IT Assets, unless documented in the SOW. Excluded: Service Provider procured, owned, and maintained IT Assets, unless documented in the SOW. Excluded: Underlying IT infrastructure for running the IT Assets are not in scope of the Service, unless documented in the SOW.
2.	Remote Admin Access & User Account Management.		X	Client shall grant Service Provider necessary and sufficient remote admin access to Client's network and IT Assets to perform the tasks required to deliver the Service.
3.	Audit Evidence Request Management.	X		Upon Client request, Service Provider delivers audit evidence for an IT Asset to fulfill a Client audit request. Excluded: more than one (1) request per calendar year, unless documented in the SOW.
4.	Operational Runbook Management.	X		Create and maintain operational runbook with specific work instructions on how to deliver the Service to Client. Excluded: Customize operational runbook documentation or create additional documentation, unless documented in the SOW.
5.	On-site (Remote Hands) Service Management.		X	When requested by Service Provider, provide hands-on physical support for an IT Asset in a Client location.
6.	Information Security Management.	X (**)	X (*)	(*) Client's *Information Security Management Policy & Procedures* are maintained by Client and apply to all Client's IT Assets to which the Service is delivered. (**) Service Provider's *Information Security Management Policy & Procedures* are maintained by Service Provider and apply to all Service Provider IT Assets used to deliver the Service.

				Excluded: Customize *Service Provider's Information Security Management Policy & Procedures*, unless documented in the SOW.
7.	Event (Monitoring & Alert) Management.	X		Monitoring & alerting on the IT Assets according to *Service Provider's* Operational *Monitoring Policies & Procedures*. Excluded: Customize *Service Provider's Operational Monitoring Policies & Procedures,* unless documented in the SOW.
8.	Incident, Escalation & Problem Management.	X	X (*)	Service Provider is responsible for troubleshooting and resolving incidents on an IT Asset. Escalate to vendor support ("Level 3 Support") for an IT Asset, if needed. (*) For a Client's IT Asset, Client shall provide and maintain vendor support work instructions and vendor support portal access so that Service Provider can perform vendor support escalations on behalf of Client. Problem Management includes the creation of Root Cause Analysis Reports (RCAs) for an IT Asset incident with recommended corrective actions as part of Continual Service Improvement. Corrective actions are assigned to either Service Provider, Client, or vendor according to ownership of the corrective action.
9.	Operational Reporting Management.	X		Client may request operational reports from Service Provider on an ad-hoc basis to support the collaborative troubleshooting of an IT Asset incident. Excluded: Client-specific operational reports on a regular basis, unless documented in the SOW.
10.	Standard Service Request Management.	X		Standard service requests can be submitted by Client or Service Provider. Standard service request tasks for an IT Asset are included in the Service at no additional fee. See Additional Responsibilities Matrices section below for enumerated standard service requests and any exclusion thereof, as a well as enumerated billable service requests. Service Provider and Client perform standard service request tasks according to the task Change Management below.
11.	Change Management.	X (**)	X (*)	Service Provider and Client shall follow change management process according to the section *Change Management* in the *Managed* Services *ITSM Foundation Service Description.* (**) Service Provider is responsible for technical change execution of Client-approved changes to an IT Asset. (*) Client is responsible for an IT Asset change approval, sending notifications to end users impacted by the change, and preparing before and testing after a change of any applications that may reside on or use the IT Asset that is being changed.
12.	Availability, Performance and Capacity Management.	X		Periodic reviews are performed with change recommendations to be implemented after approval from Client. Excluded: Expand or replace IT Asset to improve availability, performance, or capacity.
13.	Patch Management.	X	X (*)	Service Provider performs patching according to the patch frequency of Service Provider's Operational Patch Management Policy & Procedures, unless documented in the SOW. Client and Service Provider shall perform patch approval and execution according to the task above, Change Management. (*) Client shall grant access to Service Provider to use Client's centralized patch management solution if the IT Asset is or can be

				patched using such a solution. If no such solution exists, the IT Asset may then be patched manually by Service Provider. Use of Client's centralized patch management solution is limited to in-scope IT Assets. Ad-hoc patching outside the defined patch frequency is included in the Service if an IT Asset is evaluated to be an "Urgent Critical" target for a cyberattack (e.g., an Internet-facing IT Asset), whereby the patch would eliminate the vulnerability; or the patch will fix a bug that is severely impacting the availability or normal operation of a critical IT Asset. The patch must have been released from the vendor before it can be deployed. Excluded: Customize Service Provider's Operational Patch Management Policy & Procedures, unless documented in the SOW. Excluded: Apply an ad-hoc patch to an IT Asset outside the defined standard patch frequency and not designated as an "Urgent Critical" patch, unless documented in the SOW. Excluded: Apply upgrades to an IT Asset, unless documented in the SOW.
14.	Continuity (Backup & Restore) Management.		X	Client shall ensure that IT Assets have backups in case an IT Asset must be restored to resolve an incident, unless this task is provided by Service Provider, as documented in an SOW.
15.	Continuity (HA/DR Test) Management.	X (**)	X (*)	(**) Only when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are also in scope of the Service, then Service Provider is responsible as follows. Up to one (1) Client-requested HA/DR test per calendar year is included in the Service. Service Provider performs its technical tasks according to Client's HA/DR Test Plan Procedure. (*) Client is responsible for creating and maintaining the HA/DR Test Plan Procedure, with Service Provider providing feedback on its tasks as requested by Client. (*) Client is responsible for preparing before and testing after a HA/DR test of any applications that may reside on or use the HA/DR IT Assets. Excluded: when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are not in scope of the Service. Excluded: Perform more than 1 HA/DR Test per calendar year or effort related to an actual HA/DR event, unless documented in the SOW.
16.	Billable Service Request Management.	X		When performed by Service Provider, all labor effort and any material costs associated with the request are billed separately according to the *Change Order Request Procedure* in the SOW. All exclusions listed for tasks in this *General Responsibilities Matrix* are considered billable service requests. See *Additional Responsibilities Matrices* section below for enumerated billable service requests.

2.3. ADDITIONAL RESPONSIBILITIES MATRICES

2.3.1. STANDARD SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Start/Shutdown/Restart an IT Asset.	X		
2.	Configure an IT Asset.	X		

2.3.2. BILLABLE SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Perform any task that is explicitly stated as a responsibility of Client or not explicitly stated as a task of Service Provider.	X		
2.	Perform an “Excluded” activity listed for a task.	X		
3.	Deliver a new service not in scope of this Service.	X		
4.	Deploy or build a new IT Asset (i.e., an increase in contractual quantity of the Service).	X		
5.	Deprovision an IT Asset (i.e., a decrease in the contractual quantity of the Service).	X		
6.	Replace an IT Asset with a new IT Asset.	X		
7.	Perform corrective actions or restoration efforts (e.g. from data restore) of an IT Asset where the root cause is not attributable Service Provider’s action.	X		
8.	Perform design, engineering, and consulting work in relation to an existing or new Client IT Asset or Client’s overall IT environment.	X		
9.	Develop, install, monitor, and maintain customized or third-party tools, scripts, and software installed on an IT Asset.	X		

Exhibit 10:

MIS - PUBLIC CLOUD FOUNDATION (MICROSOFT AZURE)
SERVICE DESCRIPTION

REV 2025-09-26

1. SERVICE OVERVIEW

a) Public Cloud Foundation Services for Azure (the "Service") is part of Service Provider's Managed Infrastructure Services ("MIS") service line. The Service provides ongoing administration, support, monitoring, and governance of all Azure provisioned resources ("Resource(s)") in-scope of the "Client Azure Subscriptions" per "Client Azure Environment" and within scope of the "Supported Azure Resource Types", as detailed in Addendum PCF-1: *Client-specific Details*.

b) Resources that are not in scope of the Client Azure Subscriptions or the Supported Azure Resource Types are out-of-scope of the Service.

c) Each Client Azure Environment shall have a line item in the *Pricing Summary*, where the "Client Azure Environment Size" shall be designated as "Small", "Medium", "Large", or "Custom". Client Azure Environment Size is based on the calculated monthly effort to support the quantities and types of Azure Resources in the Client Azure Environment.

d) On a quarterly basis, the Client Azure Environment Size is recalculated based on then-current quantities and types of Resources. If the recalculated Client Azure Environment Size is fifteen (15) % below or above the currently assigned Client Azure Environment Size, Service Provider shall discuss with Client the option to either reduce the quantities to remain within the current Client Azure Environment Size designation and pricing or move the Client Azure Environment to the appropriate Client Azure Environment Size designation and pricing. Small is the lowest Client Azure Environment Size designation allowed.

e) The Service comes bundled with the managed services in the *ITSM Foundation Services Description*, which details standardized support communication channels, ticket management ("ITSM Tool"), service levels, as well as the governance, incident, change, problem, and escalation ITSM processes in support of the Service. Security Tickets will be securely visible to Client online, including status and updates, via Service Provider's ITSM Tool. See the *ITSM Foundation Services Description* for further details.

2. RESPONSIBILITIES MATRIX

2.1. EXPLANATION

a) The *General Responsibilities Matrix* section covers the overall steady state ITSM lifecycle tasks to deliver the Service.

b) The *Additional Responsibilities Matrices* section enumerates standard and billable service request management tasks related to the Service.

c) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in the Service. Any limitations shall be detailed in the *Clarifications* column.

d) An 'X' in the *Client* column means Client is responsible for the task.

e) When an 'X' is in both the *Service Provider* and *Client* columns, '(*)' means that there is a specific clarification for Client and '(**)' means that there is a specific clarification for Service Provider in the *Clarifications* column.

2.2. GENERAL RESPONSIBILITIES MATRIX

No.	Task Description	Service Provider	Client	Clarifications
1.	Resource Procurement, Ownership, and Vendor Support Management.	X	X (*)	(*) For Client's Resources, Client shall procure and maintain a vendor support contract for the Resources during the term of the Service and replace Resources prior to end-of-life so that Service Provider can continue to perform the tasks required to deliver the Service as well as to continue to guarantee the service levels. Service Provider may offer other services which provide procurement activities.
2.	Remote Admin Access & User Account Management.		X	Client shall grant Service Provider necessary and sufficient remote admin access to Client's network, Microsoft Azure tenant, and Resources to perform the tasks required to deliver the Service.

				Service Provider may be unable to execute some or all Service functions if appropriate access is not granted.
3.	Audit Evidence Request Management.	X		Upon Client request, Service Provider delivers audit evidence for a Resource to fulfill a Client audit request.
4.	Operational Runbook Management.	X		Create and maintain operational runbook with specific work instructions on how to deliver the Service to Client.
5.	On-site (Remote Hands) Service Management.		X	When requested by Service Provider, provide hands-on physical support for a Resource in a Client location.
6.	Information Security Management.	X	X (*)	Service Provider's *Information Security Management Policy & Procedures* are maintained by Service Provider and apply to all Service Provider Resources used to deliver the Service. (*) Client's *Information Security Management Policy & Procedures* are maintained by Client and apply to all Client's Resources to which the Service is delivered.
7.	Event (Monitoring & Alert) Management.	X	X (*)	Monitoring & alerting on the Resources according to *Service Provider's Operational Monitoring Policies & Procedures*. Service Provider will provide and administer the monitoring solution/s. (*) Client shall coordinate with Service Provider whenever they perform a Resource maintenance activity so that monitoring alerts can be turned off during the maintenance period.
8.	Incident, Escalation & Problem Management.	X	X (*)	Troubleshoot and resolve incidents on a Resource. Escalate to vendor support ("Level 3 Support") for a Resource, if needed. (*) For a Client's Resource, Client shall provide and maintain vendor support contracts and vendor support portal access so that Service Provider can perform vendor support escalations on behalf of Client. Problem Management includes the creation of Root Cause Analysis Reports (RCAs) for a Resource incident with recommended corrective actions as part of Continual Service Improvement. Corrective actions are assigned to either Service Provider, Client, or vendor according to ownership of the corrective action. Failure by Client to promptly implement a corrective action that would either solve a critical security issue or the repetition of an incident may incur additional cost or reduce service levels.
9.	Operational Reporting Management.	X		Client may request operational reports from Service Provider on an ad-hoc basis to support the collaborative troubleshooting of a Resource incident.
10.	Standard Service Request Management.	X		Standard service requests can be submitted by Client or Service Provider. Standard service request tasks for a Resource are included in the Service at no additional fee. See *Additional Responsibilities Matrices* section below for enumerated standard service requests and any limitations thereof. Service Provider and Client perform standard service request tasks according to the task *Change Management* below.
11.	Change Management.	X	X (*)	Service Provider and Client shall follow change management process according to the section *Change Management* in the *ITSM Foundation Services Description.* Service Provider is responsible for technical change execution of Client-approved changes to a Resource. (*) Client is responsible for a Resource change approval, sending notifications to end users impacted by the change, and preparing

				before and testing after a change of any applications that may reside on or use the *Resource* that is being changed.
12.	Availability, Performance and Capacity Management.	X		Periodic reviews are performed with change recommendations to be implemented after approval from Client.
13.	Billable Service Request Management.	X		When performed by Service Provider, all labor effort and any material costs associated with the request are billed separately according to the *Change Order Request Procedure* in the applicable SOW. Service Provider may offer additional managed service offerings for purchase that fulfill the Billable Service Request. See *Additional Responsibilities Matrices* section below for enumerated billable service requests.

2.3. AZURE RESPONSIBILITIES MATRICES

2.3.1. ADMINISTRATION

No.	Task Description	Service Provider	Client	Clarifications
3.	Maintain, and improve existing Azure Policies for Resources based on Service Provider identified recommendations or Client initiated Service Requests.	X		For example: Regulatory Compliance, Audit Trail, Logs, and Legal Compliance.
4.	Conduct a monthly review of configurations for existing Resources and conduct remediation activities to resolve identified drift from defined Azure Policies.	X		
5.	Maintain and improve existing Azure Resource Tagging strategy for *Resources*.	X		
6.	Maintain and improve existing Azure Organizational Hierarchy (management groups, subscriptions, and resource groups).	X		
7.	Assign Role-Based Access Control to Resources.	X		
8.	Update configurations for *Resources* in response to changes Microsoft introduces.	X		

2.3.2. AZURE VIRTUAL COMPUTE

No.	Task Description	Service Provider	Client	Clarifications
1.	Deployment, redeployment, or deletion of a virtual machine.	X		Deployment of a Virtual Machine is considered a Resource provisioning request. Further clarifications is provided in section, *AZURE RESOURCE PROVISIONING.*
2.	Start/Stop virtual machine.	X		
3.	Administer virtual compute disk including: • Create / Delete • Attach / Detach • Resize • Create snapshot	X		
4.	Administer virtual compute NIC including: • Create / Delete • Attach / Detach	X		
5.	Change virtual machine compute size (series).	X		

No.	Task Description	Service Provider	Client	Clarifications
6.	Troubleshoot virtual machine connectivity.	X		
7.	OS Management. For example: • Allocate disk space in OS • Configure NIC in OS • Provide backup services and management • OS Patch management • OS application, access, file, or configuration management		X	Service Provider may offer additional managed services which provide these functions.

2.3.3. AZURE NETWORK MANAGEMENT

No.	Task Description	Service Provider	Client	Clarifications
1.	Administer Azure Virtual Networks including: • Add additional address space • Create subnet • Add/delete/modify peering • Add/delete/modify DNS • Add/delete/modify virtual network gateway • Add/delete/modify local network gateway	X		
2.	Administer Azure Network Security Group including: • Deploy and delete group • Manage associations • Add/delete/modify rules	X		
3.	Deploy/delete DDoS protection plan.	X		
4.	Administer Azure Firewall including: • Add/delete public IP • Add/delete/modify policy • Add/delete/modify Rule Collection and Collection Groups • Add/delete/modify DNAT rule • Add/delete/modify application rule • Enable DNS	X		
5.	Add/delete/modify Bastion.	X		
6.	Add/delete/modify Azure ExpressRoute circuit and administer connections.	X		
7.	Administer Azure Route Table including: • Add/delete/modify route • Manage associations • Enable/disable route propagation	X		
8.	Administer Front Door profile including: • Add/delete Endpoint • Add/delete SSL certificate	X		
9.	Add/delete/modify Azure Traffic Manager.	X		
10.	Administer Azure CDN profile including: • Add/delete endpoint • Setup of custom domain • Add/delete SSL certificate	X		
11.	Administer Azure Application Gateway including: • Add/delete/modify Application Gateway • Configure web application firewall • Add/delete/modify application firewall rule • Manage application firewall associations	X		

No.	Task Description	Service Provider	Client	Clarifications
	• Add/delete/modify IP address • Add/delete/modify backend pool • Add/delete/modify backend setting • Add/delete/modify listener • Add/delete/modify rule • Add/delete SSL certificate • Add/delete/modify health probe			
12.	Administer Azure Load Balancer including: • Add/delete/modify load balancer • Add/delete/modify IP address • Add/delete/modify backend pools • Add/delete/modify health probe • Add/delete/modify NAT rule • Add/delete/modify outbound rule	X		
13.	Add/delete/modify Public IP Address.	X		
14.	Add/delete/modify IP groups.	X		
15.	Add/delete/modify NAT gateway.	X		
16.	Add/delete/modify private DNS zone.	X		
17.	Add/delete/modify application security group.	X		
18.	Third Party Network Management. For example: • Administration and support Palo Alto • Administration and support for Cisco		X	Service Provider may offer additional managed services which provide these functions.

2.3.4. AZURE STORAGE MANAGEMENT

No.	Task Description	Service Provider	Client	Clarifications
1.	Add/delete/modify Azure Storage Account.	X		
2.	Add/delete/modify storage container.	X		
3.	Add/delete/modify file share.	X		
4.	Administer identity-based access.	X		
5.	Configure firewall rules.	X		
6.	Add/delete/modify IP address and range.	X		
7.	Administer custom domain.	X		
8.	Administer shared access signature.	X		
9.	Add/delete/modify lifecycle management rule.	X		

2.3.5. AZURE RESOURCE PROVISIONING

No.	Task Description	Service Provider	Client	Clarifications
1.	Define Resource provisioning templates by collaboratively documenting the identified deployment scenario such as resource configuration tasks and deployment process.	X		Service Provider may limit the scope for a resource provisioning template or limit the Azure resources and services eligible for consideration, based on the complexity requiring additional architecting or design considerations.
2.	Provision Resource into the *Client Azure Environment* using a resource provisioning template.	X		Includes 10 requests monthly, additional provisioning requests available for an additional charge.

No.	Task Description	Service Provider	Client	Clarifications
				All changes to a *Client Azure Environment* should be submitted to Service Provider to maintain proper governance and visibility through Change Management. A request to provision a Resource will be considered a Standard Service Request if a resource provisioning template exists. If no template exists, the request will be considered a Billable Service Request.
3.	Provide a cost and security estimation prior to executing a Resource provisioning template.	X		
4.	Configure and maintain a Resource.	X		Client will be responsible for the configuration and maintenance of any Resource not in-scope of the Service, unless the Resource is under management through another Service Provider offering.
5.	Deprovision and complete pre- and post-configuration for a Resource.	X		Client will be responsible for the deprovisioning and post-configuration of any Resource not in-scope of the Service, unless the Resource is under management through another Service Provider offering.
6.	Inform Service Provider of Client provisioned Azure resources .		X	

2.3.6. AZURE CLIENT ENVIRONMENT REVIEWS

No.	Task Description	Service Provider	Client	Clarifications

1.	Review of health, consumption, and performance data.	X		Results and recommendations will be provided through the regular cadence of meetings with the Client Success Manager. Schedule of proactive reviews:
				• **Monthly**
				  • Defender for Cloud Security Recommendations
				  • Azure Policy Compliance
				• **Quarterly**
				  • Azure Advisor
				  • Cost Savings
				  • Reliability
				  • Operational Excellence
				  • Performance
				  • Azure Cost Management
				  • Accumulated Cost Report
				  • Cost Trend Report

2.	Provide recommendations to improve performance, reliability, compliance, and cost savings.	X		

2.4. BILLABLE SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Perform any service request that is not explicitly designated as Service Provider's responsibility in the *General Responsibilities Matrix*, a task not included in the service offering level assigned to the Resource or not enumerated in the *Standard Service Requests* table above.	X		

No.	Task Description	Service Provider	Client	Clarifications
2.	Perform any task that is explicitly designated as Client's responsibility in the *General Responsibilities Matrix*.	X		
3.	Design and/or deploy new Azure Policies.	X		
4.	Provide user or group, or general Entra ID management.	X		
5.	Manage user accounts, groups, roles, access, and identity.	X		
6.	Deliver a new service not in scope of this Service.	X		
7.	Design, implement, test, support, administer, or operate disaster recovery solutions, including Azure Site Recovery.	X		
8.	Design, implement, test, support, administer, or operate backup solutions, including Azure Backup.	X		
9.	Design or build a new Resource.	X		
10.	Replace a Resource with a new Resource.	X		
11.	Perform mitigation or restoration work of a Resource where the root cause is attributable to a Client's actions performed on the affected Resource.	X		
12.	Perform design, engineering, and consulting work in relation to an existing or new Client Resource or Client's overall IT environment.	X		
13.	Develop, install, monitor, and maintain customized or third-party tools, scripts, and software installed on a Resource.	X		
14.	Create additional documentation beyond Service Provider operational runbook for a Resource.	X		
15.	Modify *Service Provider's Information Security Management Policy & Procedures* to align with Client's Policy & Procedures.	X		
16.	Modify *Service Provider's Operational Monitoring Policies & Procedures* to align with Client's Policy & Procedures.	X		
17.	Manage Client's patch management solution for the Resources.	X		
18.	Modify Service Provider's *Operational Patch Management Policy* to align with Client's Policy & Procedures.	X		
19.	Apply a patch to a Resource outside the defined standard patch frequency, unless designated as "Urgent Critical".	X		
20.	Upgrade a Resource.	X		A patch is typically a smaller change to software functionality (e.g., release 2.3 to 2.4) and occur more frequently than upgrades. An upgrade is typically a larger change to software functionality (e.g. 2.4 to 3.1) and occurs less frequently than patches.
21.	Manage Client's backup management solution for the Resources.	X		
22.	Perform ad-hoc backups of a Resource's data outside defined standard backup frequency.	X		

No.	Task Description	Service Provider	Client	Clarifications
23.	Perform ad-hoc restores of a Resource's data not related to an incident.	X		
24.	Perform more than one (1) HA/DR test within the same calendar year.	X		

PCF-1: CLIENT-SPECIFIC DETAILS

1. CLIENT AZURE SUBSCRIPTIONS

a) The below client Azure environment IDs will correlate to one or more line items in the *Pricing Summary*.

b) Service Provider will utilize Nerdio Manager which requires access to the Microsoft Azure tenant. If Client does not permit access to Nerdio Manager some features of the service may not be available or price adjustments on the *Pricing Summary* may be required.

Client Azure Environment ID	Client Subscription Name	Client Subscription ID

2. SUPPORTED AZURE RESOURCE TYPES

1.	Azure Application Gateway
2.	Azure Application Security Group
3.	Azure Blob Storage
4.	Azure Content Delivery Network
5.	Azure Disk Storage
6.	Azure DNS
7.	Azure ExpressRoute
8.	Azure Firewall
9.	Azure Key Vault
10.	Azure Load Balancer
11.	Azure Local Network Gateway
12.	Azure Log Analytics
13.	Azure Managed Identity
14.	Azure Monitor
15.	Azure Network Security Group
16.	Azure Network Watcher
17.	Azure Private Endpoint
18.	Azure Route Table
19.	Azure Security Center
20.	Azure Virtual Machine (OS excluded)
21.	Azure Virtual Machine Scale Sets
22.	Azure Traffic Manager
23.	Azure Virtual Network
24.	Azure Virtual Network Gateway
25.	Azure VPN Gateway
26.	Azure Web Application Firewall
27.	Microsoft Defender for Cloud
28.	Azure Bastion
29.	Azure Update Manager
30.	Azure Policy
31.	Azure Monitor
32.	Activity Log
33.	Azure Resource Manager
34.	Azure Management Groups
35.	Azure RBAC
36.	Azure Resource Health
37.	Azure Advisor
38.	Azure Well-Architected Review
39.	Azure Automation
40.	Azure Lighthouse

Exhibit 11:

MIS - OPERATING SYSTEM (PER OS TYPE)
SERVICE DESCRIPTION
REV 2025-08-30

1. SERVICE OVERVIEW

a) The MIS "Operating System" service shall remotely manage IT Assets such as Windows and Linux operating systems instances running on physical or virtual servers, as documented in the *Pricing Summary* of the SOW.

2. RESPONSIBILITIES MATRIX

2.1. EXPLANATION

a) The *General Responsibilities Matrix* section covers the overall steady state ITSM lifecycle tasks to deliver the Service.

b) The *Additional Responsibilities Matrices* section enumerates standard and billable service request management tasks related to the Service.

c) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in the Service. Any limitations shall be detailed in the *Clarifications* column.

d) An 'X' in the *Client* column means Client is responsible for the task.

e) When an 'X' is in both the *Service Provider* and *Client* columns, '(*)' means that there is a specific clarification for Client and '(**)' means that there is a specific clarification for Service Provider in the *Clarifications* column.

2.2. GENERAL RESPONSIBILITIES MATRIX

No.	Task Description	Service Provider	Client	Clarifications
1.	IT Asset Procurement, Ownership, and Vendor Support Management.		X	For Client's IT Assets, Client shall procure and maintain vendor support contracts during the term of the Service, replacing IT Assets prior to end-of-life so that Service Provider can continue to perform the tasks required to deliver the Service as well as to continue to guarantee the service levels. All IT Assets in the SOW are assumed to be Client's IT Assets, unless documented in the SOW. Excluded: Service Provider procured, owned, and maintained IT Assets, unless documented in the SOW. Excluded: Underlying IT infrastructure for running the IT Assets are not in scope of the Service, unless documented in the SOW.
2.	Remote Admin Access & User Account Management.		X	Client shall grant Service Provider necessary and sufficient remote admin access to Client's network and IT Assets to perform the tasks required to deliver the Service.
3.	Audit Evidence Request Management.	X		Upon Client request, Service Provider delivers audit evidence for an IT Asset to fulfill a Client audit request. Excluded: more than one (1) request per calendar year, unless documented in the SOW.
4.	Operational Runbook Management.	X		Create and maintain operational runbook with specific work instructions on how to deliver the Service to Client. Excluded: Customize operational runbook documentation or create additional documentation, unless documented in the SOW.

5.	On-site (Remote Hands) Service Management.		X	When requested by Service Provider, provide hands-on physical support for an IT Asset in a Client location.
6.	Information Security Management.	X (**)	X (*)	(*) Client's Information Security Management Policy & Procedures are maintained by Client and apply to all Client's IT Assets to which the Service is delivered. (**) Service Provider's Information Security Management Policy & Procedures are maintained by Service Provider and apply to all Service Provider IT Assets used to deliver the Service. Excluded: Customize Service Provider's Information Security Management Policy & Procedures, unless documented in the SOW.
7.	Event (Monitoring & Alert) Management.	X		Monitoring & alerting on the IT Assets according to Service Provider's Operational Monitoring Policies & Procedures. Excluded: Customize Service Provider's Operational Monitoring Policies & Procedures, unless documented in the SOW.
8.	Incident, Escalation & Problem Management.	X	X (*)	Service Provider is responsible for troubleshooting and resolving incidents on an IT Asset. Escalate to vendor support ("Level 3 Support") for an IT Asset, if needed. (*) For a Client's IT Asset, Client shall provide and maintain vendor support work instructions and vendor support portal access so that Service Provider can perform vendor support escalations on behalf of Client. Problem Management includes the creation of Root Cause Analysis Reports (RCAs) for an IT Asset incident with recommended corrective actions as part of Continual Service Improvement. Corrective actions are assigned to either Service Provider, Client, or vendor according to ownership of the corrective action.
9.	Operational Reporting Management.	X		Client may request operational reports from Service Provider on an ad-hoc basis to support the collaborative troubleshooting of an IT Asset incident. Excluded: Client-specific operational reports on a regular basis, unless documented in the SOW.
10.	Standard Service Request Management.	X		Standard service requests can be submitted by Client or Service Provider. Standard service request tasks for an IT Asset are included in the Service at no additional fee. See Additional Responsibilities Matrices section below for enumerated standard service requests and any exclusion thereof, as a well as enumerated billable service requests. Service Provider and Client perform standard service request tasks according to the task Change Management below.
11.	Change Management.	X (**)	X (*)	Service Provider and Client shall follow change management process according to the section Change Management in the Managed Services ITSM Foundation Service Description. (**) Service Provider is responsible for technical change execution of Client-approved changes to an IT Asset. (*) Client is responsible for an IT Asset change approval, sending notifications to end users impacted by the change, and preparing before and testing after a change of any applications that may reside on or use the IT Asset that is being changed.
12.	Availability, Performance and Capacity Management.	X		Periodic reviews are performed with change recommendations to be implemented after approval from Client. Excluded: Expand or replace IT Asset to improve availability, performance, or capacity.

13.	Patch Management.	X	X (*)	Service Provider performs patching according to the patch frequency of Service Provider's Operational Patch Management Policy & Procedures, unless documented in the SOW. Client and Service Provider shall perform patch approval and execution according to the task above, Change Management. (*) Client shall grant access to Service Provider to use Client's centralized patch management solution if the IT Asset is or can be patched using such a solution. If no such solution exists, the IT Asset may then be patched manually by Service Provider. Use of Client's centralized patch management solution is limited to in-scope IT Assets. Ad-hoc patching outside the defined patch frequency is included in the Service if an IT Asset is evaluated to be an "Urgent Critical" target for a cyberattack (e.g., an Internet-facing IT Asset), whereby the patch would eliminate the vulnerability; or the patch will fix a bug that is severely impacting the availability or normal operation of a critical IT Asset. The patch must have been released from the vendor before it can be deployed. Excluded: Customize Service Provider's Operational Patch Management Policy & Procedures, unless documented in the SOW. Excluded: Apply an ad-hoc patch to an IT Asset outside the defined standard patch frequency and not designated as an "Urgent Critical" patch, unless documented in the SOW. Excluded: Apply upgrades to an IT Asset, unless documented in the SOW.
14.	Continuity (Backup & Restore) Management.		X	Client shall ensure that IT Assets have backups in case an IT Asset must be restored to resolve an incident, unless this task is provided by Service Provider, as documented in an SOW.
15.	Continuity (HA/DR Test) Management.	X (**)	X (*)	(**) Only when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are also in scope of the Service, then Service Provider is responsible as follows. Up to one (1) Client-requested HA/DR test per calendar year is included in the Service. Service Provider performs its technical tasks according to Client's HA/DR Test Plan Procedure. (*) Client is responsible for creating and maintaining the HA/DR Test Plan Procedure, with Service Provider providing feedback on its tasks as requested by Client. (*) Client is responsible for preparing before and testing after a HA/DR test of any applications that may reside on or use the HA/DR IT Assets. Excluded: when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are not in scope of the Service. Excluded: Perform more than 1 HA/DR Test per calendar year or effort related to an actual HA/DR event, unless documented in the SOW.
16.	Billable Service Request Management.	X		When performed by Service Provider, all labor effort and any material costs associated with the request are billed separately according to the Change Order Request Procedure in the SOW. All exclusions listed for tasks in this General Responsibilities Matrix are considered billable service requests. See Additional Responsibilities Matrices section below for enumerated billable service requests.

2.3. ADDITIONAL RESPONSIBILITIES MATRICES

2.3.1. STANDARD SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Start/Shutdown/Restart an IT Asset.	X		
2.	Configure an IT Asset: File system and OS-level network changes.	X		Excluded: Microsoft AD, MS IIS, FTP, SharePoint, Exchange, network shares, job scheduling, file transfers, printer management, and SSL/TLS/SSH certificates.

2.3.2. BILLABLE SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Perform any task that is explicitly stated as a responsibility of Client or not explicitly stated as a task of Service Provider.	X		
2.	Perform an “Excluded” activity listed for a task.	X		
3.	Deliver a new service not in scope of this Service.	X		
4.	Deploy or build a new IT Asset (i.e., an increase in contractual quantity of the Service).	X		
5.	Deprovision an IT Asset (i.e., a decrease in the contractual quantity of the Service).	X		
6.	Replace an IT Asset with a new IT Asset.	X		
7.	Perform corrective actions or restoration efforts (e.g. from data restore) of an IT Asset where the root cause is not attributable Service Provider’s action.	X		
8.	Perform design, engineering, and consulting work in relation to an existing or new Client IT Asset or Client’s overall IT environment.	X		
9.	Develop, install, monitor, and maintain customized or third-party tools, scripts, and software installed on an IT Asset.	X		

Exhibit 12:

MIS - DATABASE
SERVICE DESCRIPTION
REV 2025-08-30

1. SERVICE OVERVIEW

a) The MIS “Database” service shall remotely manage IT Assets such as MS SQL or Oracle database instances running on physical or virtual servers, as documented in the *Pricing Summary* of the SOW.

2. RESPONSIBILITIES MATRIX

2.1. EXPLANATION

a) The *General Responsibilities Matrix* section covers the overall steady state ITSM lifecycle tasks to deliver the Service.

b) The *Additional Responsibilities Matrices* section enumerates standard and billable service request management tasks related to the Service.

c) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in the Service. Any limitations shall be detailed in the *Clarifications* column.

d) An 'X' in the *Client* column means Client is responsible for the task.

e) When an 'X' is in both the *Service Provider* and *Client* columns, '(*)' means that there is a specific clarification for Client and '(**)' means that there is a specific clarification for Service Provider in the *Clarifications* column.

2.2. GENERAL RESPONSIBILITIES MATRIX

No.	Task Description	Service Provider	Client	Clarifications
1.	IT Asset Procurement, Ownership, and Vendor Support Management.		X	For Client's IT Assets, Client shall procure and maintain vendor support contracts during the term of the Service, replacing IT Assets prior to end-of-life so that Service Provider can continue to perform the tasks required to deliver the Service as well as to continue to guarantee the service levels. All IT Assets in the SOW are assumed to be Client's IT Assets, unless documented in the SOW. Excluded: Service Provider procured, owned, and maintained IT Assets, unless documented in the SOW. Excluded: Underlying IT infrastructure for running the IT Assets are not in scope of the Service, unless documented in the SOW.
2.	Remote Admin Access & User Account Management.		X	Client shall grant Service Provider necessary and sufficient remote admin access to Client's network and IT Assets to perform the tasks required to deliver the Service.
3.	Audit Evidence Request Management.	X		Upon Client request, Service Provider delivers audit evidence for an IT Asset to fulfill a Client audit request. Excluded: more than one (1) request per calendar year, unless documented in the SOW.
4.	Operational Runbook Management.	X		Create and maintain operational runbook with specific work instructions on how to deliver the Service to Client. Excluded: Customize operational runbook documentation or create additional documentation, unless documented in the SOW.
5.	On-site (Remote Hands) Service Management.		X	When requested by Service Provider, provide hands-on physical support for an IT Asset in a Client location.
6.	Information Security Management.	X (**)	X (*)	(*) Client's *Information Security Management Policy & Procedures* are maintained by Client and apply to all Client's IT Assets to which the Service is delivered. (**) Service Provider's *Information Security Management Policy & Procedures* are maintained by Service Provider and apply to all Service Provider IT Assets used to deliver the Service. Excluded: Customize *Service Provider's Information Security Management Policy & Procedures*, unless documented in the SOW.
7.	Event (Monitoring & Alert) Management.	X		Monitoring & alerting on the IT Assets according to *Service Provider's Operational Monitoring Policies & Procedures*. Excluded: Customize *Service Provider's Operational Monitoring Policies & Procedures,* unless documented in the SOW.

8.	Incident, Escalation & Problem Management.	X	X (*)	Service Provider is responsible for troubleshooting and resolving incidents on an IT Asset. Escalate to vendor support ("Level 3 Support") for an IT Asset, if needed. (*) For a Client's IT Asset, Client shall provide and maintain vendor support work instructions and vendor support portal access so that Service Provider can perform vendor support escalations on behalf of Client. Problem Management includes the creation of Root Cause Analysis Reports (RCAs) for an IT Asset incident with recommended corrective actions as part of Continual Service Improvement. Corrective actions are assigned to either Service Provider, Client, or vendor according to ownership of the corrective action.
9.	Operational Reporting Management.	X		Client may request operational reports from Service Provider on an ad-hoc basis to support the collaborative troubleshooting of an IT Asset incident. Excluded: Client-specific operational reports on a regular basis, unless documented in the SOW.
10.	Standard Service Request Management.	X		Standard service requests can be submitted by Client or Service Provider. Standard service request tasks for an IT Asset are included in the Service at no additional fee. See *Additional Responsibilities Matrices* section below for enumerated standard service requests and any exclusion thereof, as a well as enumerated billable service requests. Service Provider and Client perform standard service request tasks according to the task *Change Management* below.
11.	Change Management.	X (**)	X (*)	Service Provider and Client shall follow change management process according to the section *Change Management* in the *Managed Services ITSM Foundation Service Description.* (**) Service Provider is responsible for technical change execution of Client-approved changes to an IT Asset. (*) Client is responsible for an IT Asset change approval, sending notifications to end users impacted by the change, and preparing before and testing after a change of any applications that may reside on or use the IT Asset that is being changed.
12.	Availability, Performance and Capacity Management.	X		Periodic reviews are performed with change recommendations to be implemented after approval from Client. Excluded: Expand or replace IT Asset to improve availability, performance, or capacity.
13.	Patch Management.	X	X (*)	Service Provider performs patching according to the patch frequency of *Service Provider's Operational Patch Management Policy & Procedures*, unless documented in the SOW. Client and Service Provider shall perform patch approval and execution according to the task above*, Change Management.* (*) Client shall grant access to Service Provider to use Client's centralized patch management solution if the IT Asset is or can be patched using such a solution. If no such solution exists, the IT Asset may then be patched manually by Service Provider. Use of Client's centralized patch management solution is limited to in-scope IT Assets. Ad-hoc patching outside the defined patch frequency is included in the Service if an IT Asset is evaluated to be an "Urgent Critical" target for a cyberattack (e.g., an Internet-facing IT Asset), whereby the patch would eliminate the vulnerability; or the patch will fix a bug that is severely impacting the availability or normal operation of

				a critical IT Asset. The patch must have been released from the vendor before it can be deployed. Excluded: Customize Service Provider's *Operational Patch Management Policy & Procedures*, unless documented in the SOW. Excluded: Apply an ad-hoc patch to an IT Asset outside the defined standard patch frequency and not designated as an "Urgent Critical" patch, unless documented in the SOW. Excluded: Apply upgrades to an IT Asset, unless documented in the SOW.
14.	Continuity (Backup & Restore) Management.		X	Client shall ensure that IT Assets have backups in case an IT Asset must be restored to resolve an incident, unless this task is provided by Service Provider, as documented in an SOW.
15.	Continuity (HA/DR Test) Management.	X (**)	X (*)	(**) Only when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are also in scope of the Service, then Service Provider is responsible as follows. Up to one (1) Client-requested HA/DR test per calendar year is included in the Service. Service Provider performs its technical tasks according to *Client's HA/DR Test Plan Procedure.* (*) Client is responsible for creating and maintaining the *HA/DR Test Plan Procedure*, with Service Provider providing feedback on its tasks as requested by Client. (*) Client is responsible for preparing before and testing after a HA/DR test of any applications that may reside on or use the HA/DR IT Assets. Excluded: when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are not in scope of the Service. Excluded: Perform more than 1 HA/DR Test per calendar year or effort related to an actual HA/DR event, unless documented in the SOW.
16.	Billable Service Request Management.	X		When performed by Service Provider, all labor effort and any material costs associated with the request are billed separately according to the *Change Order Request Procedure* in the SOW. All exclusions listed for tasks in this *General Responsibilities Matrix* are considered billable service requests. See *Additional Responsibilities Matrices* section below for enumerated billable service requests.

2.3. ADDITIONAL RESPONSIBILITIES MATRICES

2.3.1. STANDARD SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Start/Shutdown/Restart an IT Asset.	X		
2.	Configure an IT Asset: DB profile parameters DB consistency checks DB processes DB free space DB data files DB tablespaces DB archive logs	X		Excluded: Optimize poorly performing DB queries Excluded: Perform DB and tablespace imports, exports, and reorganizations

No.	Task Description	Service Provider	Client	Clarifications
	DB statistics DB export/import DB logfile roll forwards DB reorganizations DB tablespace reorganizations DB wait requests DB user requests and sessions DB cache hit ratio DB traces on expensive query DB blocked process DB table indexes DB consistency checks			

2.3.2. BILLABLE SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Perform any task that is explicitly stated as a responsibility of Client or not explicitly stated as a task of Service Provider.	X		
2.	Perform an “Excluded” activity listed for a task.	X		
3.	Deliver a new service not in scope of this Service.	X		
4.	Deploy or build a new IT Asset (i.e., an increase in contractual quantity of the Service).	X		
5.	Deprovision an IT Asset (i.e., a decrease in the contractual quantity of the Service).	X		
6.	Replace an IT Asset with a new IT Asset.	X		
7.	Perform corrective actions or restoration efforts (e.g. from data restore) of an IT Asset where the root cause is not attributable Service Provider’s action.	X		
8.	Perform design, engineering, and consulting work in relation to an existing or new Client IT Asset or Client’s overall IT environment.	X		
9.	Develop, install, monitor, and maintain customized or third-party tools, scripts, and software installed on an IT Asset.	X		

Exhibit 13:

MIS - NETWORKING (PER DEVICE TYPE)
SERVICE DESCRIPTION
REV 2025-08-30

1. SERVICE OVERVIEW

a) The MIS "Networking" services remotely manage networking IT Assets such as switches, routers, and firewalls that provide networking connectivity and security between computer systems, software applications, and end user devices, as documented in the *Pricing Summary* of the SOW.

2. RESPONSIBILITIES MATRIX

2.1. EXPLANATION

a) The *General Responsibilities Matrix* section covers the overall steady state ITSM lifecycle tasks to deliver the Service.

b) The *Additional Responsibilities Matrices* section enumerates standard and billable service request management tasks related to the Service.

c) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in the Service. Any limitations shall be detailed in the *Clarifications* column.

d) An 'X' in the *Client* column means Client is responsible for the task.

e) When an 'X' is in both the *Service Provider* and *Client* columns, '(*)' means that there is a specific clarification for Client and '(**)' means that there is a specific clarification for Service Provider in the *Clarifications* column.

2.2. GENERAL RESPONSIBILITIES MATRIX

No.	Task Description	Service Provider	Client	Clarifications
1.	IT Asset Procurement, Ownership, and Vendor Support Management.		X	For Client's IT Assets, Client shall procure and maintain vendor support contracts during the term of the Service, replacing IT Assets prior to end-of-life so that Service Provider can continue to perform the tasks required to deliver the Service as well as to continue to guarantee the service levels. All IT Assets in the SOW are assumed to be Client's IT Assets, unless documented in the SOW. Excluded: Service Provider procured, owned, and maintained IT Assets, unless documented in the SOW. Excluded: Underlying IT infrastructure for running the IT Assets are not in scope of the Service, unless documented in the SOW. Example: physical networking cabling and WAN connections.
2.	Remote Admin Access & User Account Management.		X	Client shall grant Service Provider necessary and sufficient remote admin access to Client's network and IT Assets to perform the tasks required to deliver the Service.
3.	Audit Evidence Request Management.	X		Upon Client request, Service Provider delivers audit evidence for an IT Asset to fulfill a Client audit request. Excluded: more than one (1) request per calendar year, unless documented in the SOW.
4.	Operational Runbook Management.	X		Create and maintain operational runbook with specific work instructions on how to deliver the Service to Client. Excluded: Customize operational runbook documentation or create additional documentation, unless documented in the SOW.
5.	On-site (Remote Hands) Service Management.		X	When requested by Service Provider, provide hands-on physical support for an IT Asset in a Client location.

6.	Information Security Management.	X (**)	X (*)	(*) Client's *Information Security Management Policy & Procedures* are maintained by Client and apply to all Client's IT Assets to which the Service is delivered. (**) Service Provider's *Information Security Management Policy & Procedures* are maintained by Service Provider and apply to all Service Provider IT Assets used to deliver the Service. Excluded: Customize *Service Provider's Information Security Management Policy & Procedures*, unless documented in the SOW.
7.	Event (Monitoring & Alert) Management.	X		Monitoring & alerting on the IT Assets according to *Service Provider's Operational Monitoring Policies & Procedures*. Excluded: Customize *Service Provider's Operational Monitoring Policies & Procedures,* unless documented in the SOW.
8.	Incident, Escalation & Problem Management.	X	X (*)	Service Provider is responsible for troubleshooting and resolving incidents on an IT Asset. Escalate to vendor support ("Level 3 Support") for an IT Asset, if needed. (*) For a Client's IT Asset, Client shall provide and maintain vendor support work instructions and vendor support portal access so that Service Provider can perform vendor support escalations on behalf of Client. Problem Management includes the creation of Root Cause Analysis Reports (RCAs) for an IT Asset incident with recommended corrective actions as part of Continual Service Improvement. Corrective actions are assigned to either Service Provider, Client, or vendor according to ownership of the corrective action.
9.	Operational Reporting Management.	X		Client may request operational reports from Service Provider on an ad-hoc basis to support the collaborative troubleshooting of an IT Asset incident. Excluded: Client-specific operational reports on a regular basis, unless documented in the SOW.
10.	Standard Service Request Management.	X		Standard service requests can be submitted by Client or Service Provider. Standard service request tasks for an IT Asset are included in the Service at no additional fee. See *Additional Responsibilities Matrices* section below for enumerated standard service requests and any exclusion thereof, as a well as enumerated billable service requests. Service Provider and Client perform standard service request tasks according to the task *Change Management* below.
11.	Change Management.	X (**)	X (*)	Service Provider and Client shall follow change management process according to the section *Change Management* in the *Managed Services ITSM Foundation Service Description.* (**) Service Provider is responsible for technical change execution of Client-approved changes to an IT Asset. (*) Client is responsible for an IT Asset change approval, sending notifications to end users impacted by the change, and preparing before and testing after a change of any applications that may reside on or use the IT Asset that is being changed.
12.	Availability, Performance and Capacity Management.	X		Periodic reviews are performed with change recommendations to be implemented after approval from Client. Excluded: Expand or replace IT Asset to improve availability, performance, or capacity.
13.	Patch Management.	X	X (*)	Service Provider performs patching according to the patch frequency of *Service Provider's Operational Patch Management Policy & Procedures*, unless documented in the SOW.

				Client and Service Provider shall perform patch approval and execution according to the task above, *Change Management.* (*) Client shall grant access to Service Provider to use Client's centralized patch management solution if the IT Asset is or can be patched using such a solution. If no such solution exists, the IT Asset may then be patched manually by Service Provider. Use of Client's centralized patch management solution is limited to in-scope IT Assets. Ad-hoc patching outside the defined patch frequency is included in the Service if an IT Asset is evaluated to be an "Urgent Critical" target for a cyberattack (e.g., an Internet-facing IT Asset), whereby the patch would eliminate the vulnerability; or the patch will fix a bug that is severely impacting the availability or normal operation of a critical IT Asset. The patch must have been released from the vendor before it can be deployed. Excluded: Customize Service Provider's *Operational Patch Management Policy & Procedures*, unless documented in the SOW. Excluded: Apply an ad-hoc patch to an IT Asset outside the defined standard patch frequency and not designated as an "Urgent Critical" patch, unless documented in the SOW. Excluded: Apply upgrades to an IT Asset, unless documented in the SOW.
14.	Continuity (Backup & Restore) Management.	X (**)	X	Client shall ensure that IT Assets have backups in case an IT Asset must be restored to resolve an incident, unless this task is provided by Service Provider, as documented in an SOW. (**) Service Provider shall make a backup of network device configuration data prior to executing approved changes for the purposes of rollback planning only. This does not include network device log data.
15.	Continuity (HA/DR Test) Management.	X (**)	X (*)	(**) Only when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are also in scope of the Service, then Service Provider is responsible as follows. Up to one (1) Client-requested HA/DR test per calendar year is included in the Service. Service Provider performs its technical tasks according to *Client's HA/DR Test Plan Procedure.* (*) Client is responsible for creating and maintaining the *HA/DR Test Plan Procedure*, with Service Provider providing feedback on its tasks as requested by Client. (*) Client is responsible for preparing before and testing after a HA/DR test of any applications that may reside on or use the HA/DR IT Assets. Excluded: when an IT Asset is already configured for HA/DR and the additional IT Assets supporting HA/DR are not in scope of the Service. Excluded: Perform more than 1 HA/DR Test per calendar year or effort related to an actual HA/DR event, unless documented in the SOW.
16.	Billable Service Request Management.	X		When performed by Service Provider, all labor effort and any material costs associated with the request are billed separately according to the *Change Order Request Procedure* in the SOW. All exclusions listed for tasks in this *General Responsibilities Matrix* are considered billable service requests. See *Additional Responsibilities Matrices* section below for enumerated billable service requests.

2.3. ADDITIONAL RESPONSIBILITIES MATRICES

2.3.1. BILLABLE SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Perform any task that is explicitly stated as a responsibility of Client or not explicitly stated as a task of Service Provider.	X		
2.	Perform an "Excluded" activity listed for a task.	X		
3.	Deliver a new service not in scope of this Service.	X		
4.	Deploy or build a new IT Asset (i.e., an increase in contractual quantity of the Service).	X		
5.	Deprovision an IT Asset (i.e., a decrease in the contractual quantity of the Service).	X		
6.	Replace an IT Asset with a new IT Asset.	X		
7.	Perform corrective actions or restoration efforts (e.g. from data restore) of an IT Asset where the root cause is not attributable Service Provider's action.	X		
8.	Perform design, engineering, and consulting work in relation to an existing or new Client IT Asset or Client's overall IT environment.	X		
9.	Develop, install, monitor, and maintain customized or third-party tools, scripts, and software installed on an IT Asset.	X		

2.3.2. STANDARD SERVICE REQUESTS

2.3.2.1. SWITCH

No.	Task Description	Service Provider	Client	Clarifications
1.	Static Routes.	X		
2.	Dynamic Routing.	X		
3.	DHCP Configuration.	X	X (*)	(*) Client is responsible for enabling communication to its own managed DHCP servers.
4.	VLAN Segmentation.	X		
5.	Spanning-tree Protocol.	X		
6.	MAC Address Identification.	X		
7.	Domain Name System (DNS) Configuration.	X	X (*)	(*) Client is responsible for enabling communication to its own DNS servers.
8.	Network Time Protocol (NTP) Configuration.	X	X (*)	(*) Client is responsible for enabling communication to its own NTP servers.
9.	VLAN Trunk Protocol (VTP) Configuration.	X		
10.	QoS (Quality of Service).	X		
11.	Access Control Lists (ACLs).	X		
12.	Authentication, Authorization, and Accounting (AAA) Configuration.	X	X (*)	(*) Client is responsible for enabling AAA on its owned and managed LDAP/Active Directory server(s).

No.	Task Description	Service Provider	Client	Clarifications
13.	Syslog Management.	X	X (*)	Syslog is managed using Service Provider's monitoring solution. (*) If Client requires to send logs to a different syslog server, Client must provision and manage that server.

2.3.2.2. ROUTER

No.	Task Description	Service Provider	Client	Clarifications
1.	Routing Tables.	X		Includes all routing protocols.
2.	DHCP Server Configuration.	X	X (*)	(*) Client is responsible for enabling communication to its own managed DHCP servers.
3.	Site-to-site VPN Tunnels.	X		
4.	Remote Access VPNs.	X		
5.	IP Tunneling.	X		
6.	Domain Name System (DNS) Configuration.	X	X (*)	(*) Client is responsible for enabling communication to its own DNS servers.
7.	Network Time Protocol (NTP) Configuration.	X	X (*)	(*) Client is responsible for enabling communication to its own NTP servers.
8.	Telephony Configuration.	X		Call Routing (Direct Inward Dial), Media Resources, Codecs.
9.	Quality of Service (QoS).	X		
10.	Access Control Lists (ACLs).	X		
11.	Authentication, Authorization, and Accounting (AAA) Configuration.	X	X (*)	(*) Client is responsible for enabling AAA on its owned and managed LDAP/Active Directory server(s).
12.	Syslog Management.	X	X (*)	Syslog is managed using Service Provider's monitoring solution. (*) If Client requires to send logs to a different syslog server, Client must provision and manage that server.
13.	Digital Certificate Management.	X	X (*)	Service Provider installs Client-provided certificate and sets up an expiration alert to notify Client. (*) Client is responsible for generating the Certificate Signing Request (CSR), producing self-signed certification, or requesting the certificate from a Certificate Authority (CA) based on that CSR, and providing Service Provider with the certificate for installation. Client is responsible for renewing or revoking the certificate with a CA.

2.3.2.3. TRADITIONAL FIREWALL

a) Traditional Firewall capabilities include stateful packet inspection to perform packet header filtering on network ports, protocols, and IP addresses to deny/allow network traffic (OSI Layers 3 & 4).

No.	Task Description	Service Provider	Client	Clarifications
1.	Routing Tables.	X		
2.	DHCP Server Configuration.	X	X (*)	(*) Client is responsible for enabling communication to its own managed DHCP servers.
3.	Site-to-site VPN Tunnels.	X	X (*)	(*) Client is responsible for providing the VPN peer contact information to enable the communication.

No.	Task Description	Service Provider	Client	Clarifications
4.	Remote Access VPNs.	X		
5.	Network Address Translation (NAT).	X		
6.	Firewall Policy Management.	X		
7.	Firewall Inspection.	X		
8.	Network Time Protocol (NTP) Configuration.	X	X (*)	(*) Client is responsible for enabling communication to its own NTP servers.
9.	QoS (Quality of Service).	X		
10.	Authentication, Authorization, and Accounting (AAA)	X	X (*)	(*) Client is responsible for enabling AAA on its owned and managed LDAP/Active Directory server(s).
11.	Syslog Management.	X	X (*)	Syslog is managed using Service Provider's monitoring solution. (*) If Client requires to send logs to a different syslog server, Client must provision and manage that server.
12.	Digital Certificate Management.	X	X (*)	Service Provider installs Client-provided certificate and sets up an expiration alert to notify Client. (*) Client is responsible for generating the Certificate Signing Request (CSR), producing self-signed certification, or requesting the certificate from a Certificate Authority (CA) based on that CSR, and providing Service Provider with the certificate for installation. Client is responsible for renewing or revoking the certificate with a CA.

2.3.2.4. NEXT GENERATION FIREWALL (NGFW) & ADVANCED NETWORKING CAPABILITIES

a) NGFWs expand the capabilities of the Traditional Firewall by using use deep packet inspection to perform OSI layer 5-7 packet content filtering to deny/allow network traffic (up to OSI Layer 7) – especially for websites and applications.
b) The following capabilities must be licensed, activated, and implemented prior to Service Provider delivering the Service.
c) Outbound Website URL Filtering and Inbound Malware Protection capabilities are included by default with the management of each NGFW.
d) The capabilities with "(*)" are only supported by Service Provider if explicitly documented as being supported in the *Pricing Summary* of the SOW.

No.	Task Description	Service Provider	Client	Clarifications
1.	Outbound Website URL Filtering.	X		URL filtering is the capability of comparing all web traffic against URL filters, which are typically contained in a database of sites that users are permitted to access or denied from accessing.
2.	Inbound Malware Protection.	X		Malware Protection is the non-signature-based capability to detect malware, including the use of sandboxing to examine malicious and suspicious files.
3.	Inbound Sandboxing.	X		Sandboxing is a capability providing protection against malicious software by sending suspicious files to an isolated sandbox system. The suspicious files can then run in the sandbox so their behavior can be examined to determine whether they are malicious or not.
4.	SSL Inspection.	X		SSL Inspection is the capability to inspect SSL/TLS traffic entering or leaving a network for malicious content.
5.	DNS Security.	X		DNS Security Extensions or DNSSEC, is the capability of establishing a set of specifications for authenticating DNS requests and responses using digital signatures based on cryptography. DNSSEC ensures that the root name server is permitted to send a response, the information in the response is safe, and that the response was not modified while in transit.

No.	Task Description	Service Provider	Client	Clarifications
6.	Application Control.	X		Application Control is the capability to create granular policies based on users or groups to identify, block or limit usage of applications and widgets. Applications are classified into categories, based on diverse criteria such as application type, security risk level, resource usage, productivity implications.
7.	User Identification.	X		User Identification is the capability to enforce policies within the network to control a user's traffic based on the identity and access management (IAM) policies assigned to users.
8.	Inbound IDS/IPS.	X		Intrusion Detection is the capability of monitoring network traffic and analyzing it for signs of possible intrusions, such as exploit attempts and incidents that may be imminent threats to the network. Intrusion Prevention is the capability of performing intrusion detection and then stopping the detected incidents, typically done by dropping packets or terminating sessions.
9.	Data Loss Prevention (DLP).	X		DLP is the capability to protect Client data by identifying sensitive information and then using deep content analysis to detect and prevent potential data leaks. The content analysis uses methods like keyword matches, regular expressions, and internal functions to recognize content that matches Client's DLP policy.

2.3.2.5. WEB APPLICATION FIREWALL (WAF)

No.	Task Description	Service Provider	Client	Clarifications
1.	Inbound Injection protection	X		Injection flaw occurs when suspicious data is inserted into an application as a command or query. This hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
2.	Inbound Cross-site scripting protection	X		Attackers use webpages or web applications to send malicious code and compromise users' interactions with a vulnerable application. These types of attacks typically occur because of common flaws within a web application and enable a bad actor to take on the user's identity, carry out any actions the user normally performs, and access all their data.
3.	Inbound Web traffic filtering	X		Create rules to filter web traffic based on conditions that include IP addresses, HTTP headers and body, or custom URIs. This gives you an additional layer of protection from web attacks that attempt to exploit vulnerabilities in custom or third-party web applications.
4.	Inbound WAF Bot Control	X		Managed rule group that gives you visibility and control over common and pervasive bot traffic that can consume excess resources, skew metrics, cause downtime, or perform other undesired activities.
5.	Inbound Real-time visibility	X		Provides real-time metrics and captures raw requests that include details about IP addresses, geo locations, URIs, User-Agent and referrers.
6.	Inbound Security misconfigurations	X		Security misconfiguration refers to the failure to properly configure and maintain the security settings of an application, system, or network. It can occur when default configurations are not changed, unnecessary services are not disabled, or security patches are not applied promptly.
7.	Inbound XML External Entities (XXE)	X		Security vulnerability that occurs when an application parses XML input from an untrusted source. It enables an attacker to exploit an

No.	Task Description	Service Provider	Client	Clarifications
				XML parser's processing of external entities and can lead to disclosure of confidential data, denial of service, server-side request forgery, and even remote code execution.
8.	Inbound Content delivery network (CDN)	X		Linked group of servers that are distributed around the world to deliver faster website content to users. This content can be anything from images and videos to JavaScript files, HTML pages, and style sheets.
9.	Authentication, Authorization, and Accounting (AAA) Configuration.	X	X (*)	(*) Client is responsible of enabling AAA on its owned and managed LDAP/Active Directory server(s).
10.	Syslog Management.	X	X (*)	Syslog is managed using Service Provider's monitoring solution. (*) If Client requires to send logs to a different syslog server, Client must provision and managed that server.
11.	Digital Certificate Management.	X	X (*)	Service Provider installs Client-provided certificate and sets up an expiration alert to notify Client. (*) Client is responsible for generating the Certificate Signing Request (CSR), producing self-signed certification, or requesting the certificate from a Certificate Authority (CA) based on that CSR, and providing Service Provider with the certificate for installation. Client is responsible for renewing or revoking the certificate with a CA.

2.3.2.6. LOAD BALANCER

No.	Task Description	Service Provider	Client	Clarifications
1.	Application availability	X		Load balancers perform health checks on servers before routing requests to them. If one server is about to fail, or is offline for maintenance or upgrades, load balancing automatically reroutes the workload to a working server to avoid service interruptions and maintain high availability.
2.	Application scalability	X		Load balancing enables an on-demand, high performance infrastructure that can handle the heaviest or lightest network traffic loads. Physical or virtual servers can be added or removed as needed, making scalability simple and automated.
3.	Application security	X		Load balancers can include security features such as SSL encryption, web application firewalls (WAF) and multi-factor authentication (MFA). They can also be incorporated into application delivery controllers (ADC) to improve application security. By safely routing or offloading network traffic, load balancing can help defend against security risks such as distributed denial-of-service (DDoS) attacks.
4.	Optimize traffic routing	X		Match your load balancing policy to your application requirements and optimize efficiency and reliability. Client chooses from round-robin, least connections, IP hash load balancing, or customized policies.
5.	Multiple protocol flexibility	X		Client uses rules to define routing policies to balance incoming traffic with supported protocols such as TCP, HTTP, HTTP/2, and WebSockets.
6.	TLS termination/SSL offloading			Transport Layer Security (TLS) termination decrypts SSL-encrypted data traffic. SSL termination also works to increase site and web application performance by reducing the workload scope of back-end servers.
7.	Pass-through layer 4 (TCP/UDP) load balancing			Flexible Network Load Balancer preserves the original Client packet (IP/Port) characteristics and load-balances them as is, without terminating the Client session. The load-balancing decision is based

No.	Task Description	Service Provider	Client	Clarifications
				on a hash of source/destination IP/Port and protocol information. It can provide network flow connection persistence based on Client source IP and ensure that the subsequent requests from a Client session are sent to the same back-end server.
8.	Concurrency control with entity tags			Provide optimistic concurrency control for load balancers via the API and protect against conflicting changes made by multiple users. Any conflicting changes to a load balancer, such as to its shape, listeners, back-end sets, or routing policies, are tagged for review prior to implementation.
9.	Authentication, Authorization, and Accounting (AAA) Configuration.	X	X (*)	(*) Client is responsible of enabling AAA on its owned and managed LDAP/Active Directory server(s).
10.	Syslog Management.	X	X (*)	Syslog is managed using Service Provider's monitoring solution. (*) If Client requires to send logs to a different syslog server, Client must provision and managed that server.
11.	Digital Certificate Management.	X	X (*)	Service Provider installs Client-provided certificate and sets up an expiration alert to notify Client. (*) Client is responsible for generating the Certificate Signing Request (CSR), producing self-signed certification, or requesting the certificate from a Certificate Authority (CA) based on that CSR, and providing Service Provider with the certificate for installation. Client is responsible for renewing or revoking the certificate with a CA.

2.3.2.7. NETWORK ACCESS CONTROL (NAC)

No.	Task Description	Service Provider	Client	Clarifications
1.	Configure and troubleshoot of management features (syslog, SNMP, SSH, netflow, NTP).	X		
2.	Assess and remediate device compliance.	X		
3.	Manage and troubleshoot end users, devices, and guest access.	X		
4.	Authentication, Authorization, and Accounting (AAA) – Troubleshoot.	X		
5.	Certificate Management - Get current, configure and troubleshoot certificates.	X		
6.	Management and troubleshooting access policies and exclusions.	X		
7.	License synchronization health.	X		
8.	Captive Portal.	X	X (*)	This is a web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi or wired network before they are granted broader access to network resources.

2.3.2.8. CENTRALIZED NETWORK MANAGEMENT CONSOLE (APPLIANCE)

No.	Task Description	Service Provider	Client	Clarifications
1.	Configure and troubleshoot management features (syslog, SNMP, SSH, netflow, NTP).	X		
2.	Assess and remediate device compliance.	X		

3.	Manage and troubleshoot devices under management via console.	X		

2.3.2.9. TELCO LINE

No.	Task Description	Service Provider	Client	Clarifications
1.	Monitor line status (up/down).	X		
2.	Receive and respond to outage alerts.	X		
3.	Coordinate with telco provider for repairs and troubleshooting.	X		

2.3.2.10. LIGHTWEIGHT ACCESS POINTS (LWAP) WITH WLAN CONTROLLER (WLC)

No.	Task Description	Service Provider	Client	Clarifications
1.	WLAN Security Configuration.	X		Security protocols and authentication.
2.	WLAN Segmentation.	X		
3.	DHCP Server Configuration.	X	X (*)	(*) Client is responsible of enabling communication to its own managed DHCP servers.
4.	Domain Name System (DNS) Configuration.	X	X (*)	(*) Client is responsible of enabling communication to its own DNS servers.
5.	Network Time Protocol (NTP) Configuration.	X	X (*)	(*) Client is responsible of enabling communication to its own NTP servers.
6.	Roaming Troubleshooting.	X	X (*)	(*) Client is responsible of ensuring that wireless overlapping within wireless access points is optimal to enable roaming.
7.	Coverage Troubleshooting.	X	X (*)	(*) Client is responsible of performing onsite wireless site surveys and place wireless access points properly to cover all facilities required areas.
8.	Access Point Registration.	X		
9.	SSID Configuration.	X		
10.	Guest SSID.	X		
11.	Captive Portal.	X	X (*)	This is a web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi or wired network before they are granted broader access to network resources. (*) Client is responsible for the Captive Portal Content (e.g. Terms and Conditions of Use) of Captive Portal.
12.	Bring-Your-Own-Device (BYOD).	X	X (*)	(*) Client is responsible of issuing, renewing, and revoking certificates for BYOD.
13.	Quality of Service (QoS).	X		
14.	Access Control Lists (ACLs).	X		
15.	Authentication, Authorization, and Accounting (AAA) Configuration.	X	X (*)	(*) Client is responsible of enabling AAA on its owned and managed LDAP/Active Directory server(s).
16.	Syslog Management.	X	X (*)	Syslog is managed using Service Provider's monitoring solution. (*) If Client requires to send logs to a different syslog server, Client must provision and managed that server.

No.	Task Description	Service Provider	Client	Clarifications
17.	Digital Certificate Management.	X	X (*)	Service Provider installs Client-provided certificate and sets up an expiration alert to notify Client. (*) Client is responsible for generating the Certificate Signing Request (CSR), producing self-signed certification, or requesting the certificate from a Certificate Authority (CA) based on that CSR, and providing Service Provider with the certificate for installation. Client is responsible for renewing or revoking the certificate with a CA.

2.3.2.11. STANDALONE WIRELESS ACCESS POINTS (WAP) WITHOUT WLAN CONTROLLER (WLC)

No.	Task Description	Service Provider	Client	Clarifications
1.	WLAN Security Configuration.	X		
2.	WLAN Segmentation.	X		
3.	DHCP Server Configuration.	X	X (*)	(*) Client is responsible of enabling communication to its own managed DHCP servers.
4.	Domain Name System (DNS) Configuration.	X	X (*)	(*) Client is responsible of enabling communication to its own DNS servers.
5.	Network Time Protocol (NTP) Configuration.	X	X (*)	(*) Client is responsible of enabling communication to its own NTP servers.
6.	Roaming Troubleshooting.	X	X (*)	(*) Client is responsible of ensuring that wireless overlapping within wireless access points is optimal to enable roaming.
7.	Coverage Troubleshooting.	X	X (*)	(*) Client is responsible of performing onsite wireless site surveys and place wireless access points properly to cover all facilities required areas.
8.	SSID Configuration.	X		
9.	Guest SSID.	X		
10.	Quality of Service (QoS).	X		
11.	Access Control Lists (ACLs).	X		
12.	Authentication, Authorization, and Accounting (AAA) Configuration.	X	X (*)	(*) Client is responsible of enabling AAA on its owned and managed LDAP/Active Directory server(s).
13.	Syslog Management.	X	X (*)	Syslog is managed using Service Provider's monitoring solution. (*) If Client requires to send logs to a different syslog server, Client must provision and managed that server.
14.	Digital Certificate Management.	X	X (*)	Service Provider installs Client-provided certificate and sets up an expiration alert to notify Client. (*) Client is responsible for generating the Certificate Signing Request (CSR), producing self-signed certification, or requesting the certificate from a Certificate Authority (CA) based on that CSR, and providing Service Provider with the certificate for installation. Client is responsible for renewing or revoking the certificate with a CA.

2.3.2.12. UNIFIED COMMUNICATIONS AND COLLABORATION (UCC)

2.3.2.12.1. END USER MANAGEMENT

No.	Task Description	Service Provider	Client	Clarifications
1.	Voice/Video Quality	X		
2.	Call Dialing.	X		
3.	PSTN Calling.	X		
4.	Phone Registration.	X		
5.	Codecs/Protocols.	X		
6.	IM & Presence.	X		
7.	Softphone VPNless.	X		
8.	Voicemail.	X		
9.	Deskphone Configuration.	X		
10.	Softphone Configuration.	X		
11.	Call Routing.	X		
12.	End-user Profiles.	X		
13.	Authentication, Authorization, and Accounting (AAA) Configuration.?	X	X (*)	(*) Client is responsible of enabling AAA on its owned and managed LDAP/Active Directory server(s).
14.	Syslog Management.	X	X (*)	Syslog is managed using Service Provider's monitoring solution. (*) If Client requires to send logs to a different syslog server, Client must provision and managed that server.
15.	Digital Certificate Management.	X	X (*)	Service Provider installs Client-provided certificate and sets up an expiration alert to notify Client. (*) Client is responsible for generating the Certificate Signing Request (CSR), producing self-signed certification, or requesting the certificate from a Certificate Authority (CA) based on that CSR, and providing Service Provider with the certificate for installation. Client is responsible for renewing or revoking the certificate with a CA.

2.3.2.12.2. AGENT MANAGEMENT (CONTACT CENTER)

No.	Task Description	Service Provider	Client	Clarifications
1.	Routing and Queue Management.	X		
2.	Call Distribution.	X		
3.	Disposition Codes.	X		
4.	Call Back Options.	X		
5.	Agent Desktop.	X		
6.	Localization.	X		
7.	Remote Agent.	X		
8.	Single Sign-On (SSO).	X		
9.	Supervisor Management.	X		
10.	Call Recording.	X		
11.	Music On Hold.	X		
12.	Virtual Agent.	X		
13.	Self-service Interactive Voice Response (IVR).	X		

No.	Task Description	Service Provider	Client	Clarifications
14.	Reporting and Dashboard.	X		
15.	Authentication, Authorization, and Accounting (AAA) Configuration.	X	X (*)	(*) Client is responsible of enabling AAA on its owned and managed LDAP/Active Directory server(s).
16.	Syslog Management.	X	X (*)	Syslog is managed using Service Provider's monitoring solution. (*) If Client requires to send logs to a different syslog server, Client must provision and managed that server.
17.	Digital Certificate Management.	X	X (*)	Service Provider installs Client-provided certificate and sets up an expiration alert to notify Client. (*) Client is responsible for generating the Certificate Signing Request (CSR), producing self-signed certification, or requesting the certificate from a Certificate Authority (CA) based on that CSR, and providing Service Provider with the certificate for installation. Client is responsible for renewing or revoking the certificate with a CA.

Exhibit 14:

MIS – DATA PROTECTION (BACKUP & RECOVERY – BUR)
SERVICE DESCRIPTION
REV 2025-10-28

1. SERVICE OVERVIEW

a) "MIS – Data Protection (Backup & Recovery – BUR)" or "Service" shall remotely manage 24x7 a backup and recovery solution deployed at the Client's IT environment.

b) The specific backup tool ("Backup Tool") used to deliver the Service shall be documented in the *Pricing Summary* of the SOW.

c) If the Backup Tool is provided by Client, it shall be labeled "BYOL" (Bring-Your-Own-License), and if the Backup Tool is provided by Service Provider, it shall be labeled "MSP" (Managed Service Provider), as documented in the *Pricing Summary* of the SOW.

d) All Backup Tool job alerts shall be sent to Service Provider's ITSM Tool for processing by Service Provider.

2. RESPONSIBILITIES MATRIX

2.1. EXPLANATION

a) The *General Responsibilities Matrix* section covers the overall steady state ITSM lifecycle tasks to deliver the Service.

b) The *Additional Responsibilities Matrices* section enumerates standard and billable service request management tasks related to the Service.

c) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in the Service. Any limitations shall be detailed in the *Clarifications* column.

d) An 'X' in the *Client* column means Client is responsible for the task.

e) When an 'X' is in both the *Service Provider* and *Client* columns, '(*)' means that there is a specific clarification for Client and '(**)' means that there is a specific clarification for Service Provider in the *Clarifications* column.

2.2. GENERAL RESPONSIBILITIES MATRIX

No.	Task Description	Service Provider	Client	Clarifications
1.	IT Asset Procurement, Ownership, and Vendor Support Management.	X (**)	X (*)	(**) For an **MSP** Backup Tool, Service Provider shall procure and maintain vendor support contracts during the term of the Service, replacing IT Assets prior to end-of-life so that Service Provider can continue to perform the tasks required to deliver the Service as well as to continue to guarantee the service levels. (*) For a **BYOL** Backup Tool, Client shall procure and maintain vendor support contracts during the term of the Service, replacing IT Assets prior to end-of-life so that Service Provider can continue to perform the tasks required to deliver the Service as well as to continue to guarantee the service levels. Excluded: Underlying IT infrastructure for running the Backup Tool or backed-up IT Assets are not in scope of the Service, unless documented in the SOW.
2.	Remote Admin Access & User Account Management.		X	Client shall grant Service Provider necessary and sufficient remote admin access to Client's network and backed-up IT Assets to perform the tasks required to deliver the Service.

3.	Audit Evidence Request Management.	X		Upon Client request, Service Provider delivers audit evidence for the Service to fulfill a Client audit request. Excluded: more than one (1) request per calendar year, unless documented in the SOW.
4.	Operational Runbook Management.	X		Create and maintain operational runbook with specific work instructions on how to deliver the Service to Client. Excluded: Customize operational runbook documentation or create additional documentation, unless documented in the SOW.
5.	On-site (Remote Hands) Service Management.		X	When requested by Service Provider, provide hands-on physical support for Backup Tool infrastructure or backed-up IT Asset in a Client location.
6.	Information Security Management.	X (**)	X (*)	(*) Client's *Information Security Management Policy & Procedures* are maintained by Client and apply to all Client's backed-up IT Assets to which the Service is delivered. (**) Service Provider's *Information Security Management Policy & Procedures* are maintained by Service Provider and apply to this Service. Excluded: Customize *Service Provider's Information Security Management Policy & Procedures*, unless documented in the SOW.
7.	Event (Monitoring & Alert) Management.	X		Monitoring & alerting on the backed-up IT Assets according to *Service Provider's Operational Monitoring Policies & Procedures*. Excluded: Customize *Service Provider's Operational Monitoring Policies & Procedures,* unless documented in the SOW.
8.	Incident, Escalation & Problem Management.	X	X (*)	Service Provider is responsible for troubleshooting and resolving incidents related to the Service. Escalate to vendor support ("Level 3 Support") for the Observability Tool, if needed. (*) For the BYOL Backup Tool, Client shall provide and maintain vendor support work instructions and vendor support portal access so that Service Provider can perform vendor support escalations on behalf of Client. Problem Management includes the creation of Root Cause Analysis Reports (RCAs) for an IT Asset incident with recommended corrective actions as part of Continual Service Improvement. Corrective actions are assigned to either Service Provider, Client, or vendor according to ownership of the corrective action.
9.	Operational Reporting Management.	X		Client may request operational reports from Service Provider on an ad-hoc basis to support the collaborative troubleshooting of a backed-up IT Asset incident. Excluded: Client-specific operational reports on a regular basis, unless documented in the SOW.

10.	Standard Service Request Management.	X		Standard service requests can be submitted by Client or Service Provider. Standard service request tasks for a backed-up IT Asset are included in the Service at no additional fee. See *Additional Responsibilities Matrices* section below for enumerated standard service requests and any exclusion thereof, as a well as enumerated billable service requests. Service Provider and Client perform standard service request tasks according to the task *Change Management* below.
11.	Change Management.	X (**)	X (*)	Service Provider and Client shall follow change management process according to the section *Change Management* in the *Managed Services ITSM Foundation Service Description.* (**) Service Provider is responsible for technical change execution of Client-approved changes to a backed-upIT Asset. (*) Client is responsible for an IT Asset change approval, sending notifications to end users impacted by the change, and preparing before and testing after a change of any applications that may reside on or use the backed-up IT Asset that is being changed.
12.	Availability, Performance and Capacity Management.	X		Periodic reviews are performed of the Service with change recommendations to be implemented after approval from Client. Excluded: Expand or replace backed-up IT Asset to improve availability, performance, or capacity.
13.	Billable Service Request Management.	X		When performed by Service Provider, all labor effort and any material costs associated with the request are billed separately according to the *Change Order Request Procedure* in the SOW. All exclusions listed for tasks in this *General Responsibilities Matrix* are considered billable service requests. See *Additional Responsibilities Matrices* section below for enumerated billable service requests.

2.3. ADDITIONAL RESPONSIBILITIES MATRICES

2.3.1. STANDARD SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Start/Shutdown/Restart Service.	X		
2.	Maintain and optimize backup configurations inside Backup Tool for backed-up in-scope IT Assets.	X		

No.	Task Description	Service Provider	Client	Clarifications
3.	Monitor & triage backup job alerts 24x7 for in-scope IT Assets. Handle false positive alerts. Handle true positive alerts by restarting failed backups or escalating repeatedly failing or slow-running backups to Client according to mutually agreed upon procedure.	X		
4.	Perform first data restore task of each calendar month when requested by Client.	X		Additional data restores in the same calendar month are billable. See *Billable Service Requests*.
5.	Apply patch updates to Backup Tool (include agent), when available and if applicable.	X		

2.3.2. BILLABLE SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Perform post data restore system-specific restoration efforts.	X		
2.	Perform additional data restores beyond the first data restore of a calendar month.	X		
3.	Perform data restore validations beyond those supported by Backup Tool.	X		
4.	Perform any task that is explicitly stated as a responsibility of Client or not explicitly stated as a task of Service Provider.	X		
5.	Perform an “Excluded” activity listed for a task.	X		
6.	Deliver a new service not in scope of this Service.	X		
7.	Deploy or build a new backed-up IT Asset (i.e., an increase in contractual quantity of the Service).	X		
8.	Deprovision an existing backed-up IT Asset (i.e., a decrease in the contractual quantity of the Service).	X		
9.	Replace an existing backed-up IT Asset with a new backed-up IT Asset.	X		
10.	Perform design, engineering, and consulting work in relation to an existing or new Client backed-up IT Asset or Client’s overall IT environment.	X		
11.	Develop, install, monitor, and maintain customized or third-party tools, scripts, and software installed on an IT Asset.	X		

Exhibit 15:

MSS – EMAIL SECURITY – PLATFORM MANAGEMENT
SERVICE DESCRIPTION

REV 2025-11-02

1. SERVICE OVERVIEW

a) Email Security – Platform Management ("the Service") is a part of the Service Provider's Managed Security Services ("MSS") service family and manages Client's Email Security Platform. An "Email Security Platform" is a cybersecurity solution that protects an organization's email infrastructure from malicious attacks, data breaches, and other digital threats. It inspects and then blocks incoming emails with malicious content, encrypts outbound traffic, and provides layers of defense beyond the basic security features of standard Email Messaging Platforms. Service Provider will abide by Client's state laws in the event of a data breach.

b) If an Email Security Platform is designated as "BYOL" or Bring-Your-Own-License in the *Pricing Summary*, the platform's subscriptions and the platform's instance are provided by Client, and Service Provider remotely manages the platform. Under BYOL, it is assumed that the platform is already implemented before this Service can be applied.

c) If an Email Security Platform is designated as "MSSP" or "Managed Security Service Provider" in the *Pricing Summary*, the platform's subscriptions and the platform's instance are provided by Service Provider, and Service Provider remotely manages the platform. Under MSSP, it is assumed that the platform needs to be implemented and this is performed by Service Provider. All MSSP Email Security Platform subscriptions quantities are contractual minimums and increases in quantities will incur additional fees.

d) If an Email Security Platform is designated as "MSSP", the following term and termination section is applicable to the Service, superseding any similar term and termination section referenced in the SOW:

(i) If the Service is terminated for convenience prior to completion of the initial Service Term, Client shall not be relieved of its obligations regarding payments for the remaining months of the initial Service Term.

(ii) Additional services (e.g., increases in quantities of existing base subscriptions or add-on subscriptions) procured during the initial Service Term or any renewal Service Term shall co-terminate with current Service Term.

(iii) Client agrees to the terms of the MSSP Email Security Platform online agreements located at: https://www.mimecast.com/contracts/.

e) The Service comes bundled with the managed services in the *ITSM Foundation Services Description*, which details standardized support communication channels, ticket management ("ITSM Tool"), service levels, as well as the governance, incident, change, problem, and escalation ITSM processes in support of the Service. Security Tickets will be securely visible to Client online, including status and updates, via Service Provider's ITSM Tool. See the *ITSM Foundation Services Description* for further details.

2. RESPONSIBILITIES MATRIX

2.1. EXPLANATION

a) The *General Responsibilities Matrix* section covers the overall steady state ITSM lifecycle tasks to deliver the Service.

b) The *Additional Responsibilities Matrices* section enumerates standard and billable service request management tasks related to the Service.

c) An 'X' in the *Service Provider* column means Service Provider is responsible for the task and it is included in the Service. Any limitations shall be detailed in the *Clarifications* column.

d) An 'X' in the *Client* column means Client is responsible for the task.

e) When an 'X' is in both the *Service Provider* and *Client* columns, '(*)' means that there is a specific clarification for Client and '(**)' means that there is a specific clarification for Service Provider in the *Clarifications* column.

2.2. GENERAL RESPONSIBILITIES MATRIX

No.	Task Description	Service Provider	Client	Clarifications
1.	Procurement, Ownership, and Vendor Support Contract Management.	X (**)	X (*)	(*) If the Email Security Platform is designated as "BYOL" in the *Pricing Summary*, Client shall procure and own the platform and shall maintain vendor support contracts for the duration of the term of the Service. (**) If the Email Security Platform is designated as an "MSSP" service in the *Pricing Summary*, Service Provider shall procure and own the platform and shall maintain vendor support contracts for the duration of the term of the Service. (**) Service Provider will be reviewing Vendor Security and Platform Bulletins and proactively bringing to Client's attention any items relevant to maintain service delivery.

No.	Task Description	Service Provider	Client	Clarifications
				The Email Security Platform (and any client software agents, if applicable) shall be kept up to date to continue to guarantee Service availability.
2.	Manage IT infrastructure for running the Email Security Platform.	X (**)	X (*)	(*) If the Email Security Platform is designated as "BYOL" in the *Pricing Summary*, Client shall manage IT infrastructure for running the platform. (**) If the Email Security Platform is designated as "MSSP" in the *Pricing Summary*, Service Provider shall manage IT infrastructure for running the platform unless the platform is running at Client location or in platform vendor's cloud.
3.	Remote Access.		X	Client shall grant Service Provider necessary and sufficient remote admin privileges to Client's network and Email Security Platform to perform the tasks required to deliver the Service. Client shall establish Jump box for Service Provider to access Client's network and/or Email Security Platform, if required.
4.	Audit Evidence Request Management.	X		Upon Client request, Service Provider delivers audit evidence for the Service to fulfill a Client audit request. Excluded: more than one (1) request per calendar year, unless documented in the SOW.
5.	Operational Runbook Management.	X		Create and maintain operational runbook with specific work instructions on how to deliver the Service to Client. Excluded: Customize operational runbook documentation or create additional documentation, unless documented in the SOW.
6.	On-site (Remote Hands) Service Management.		X	When requested by Service Provider, provide hands-on physical support for Email Security Platform when in a Client location.
7.	Information Security Management.	X (**)	X (*)	(*) Client's *Information Security Management Policy & Procedures* are maintained by Client and apply to all Client's IT Assets to which the Service is delivered. (**) Service Provider's *Information Security Management Policy & Procedures* are maintained by Service Provider and apply to this Service. Excluded: Customize *Service Provider's Information Security Management Policy & Procedures*, unless documented in the SOW.
8.	Event (Monitoring & Alert) Management.	X		Monitoring & alerting of the Email Security Platform according to *Service Provider's Operational Monitoring Policies & Procedures*. For clarity, this task refers to event management related to the Email Security Platform up/down status – it does not include event management handling related to suspicious emails. Triaging suspicious emails that were not blocked by the Email Security Platform is an add-on service. Excluded: customization of *Service Provider's Operational Monitoring Policies & Procedures,* unless documented in the SOW.
9.	Incident, Escalation & Problem Management.	X	X (*)	Service Provider is responsible for troubleshooting and resolving incidents related to the Service. Escalate to Email Security Platform vendor support ("Level 3 Support"), if needed. For clarity, this task refers to incident management related to the Email Security Platform – it does not include incident handling related to suspicious emails. Triaging suspicious emails that were not blocked by the Email Security Platform is an add-on service.

No.	Task Description	Service Provider	Client	Clarifications
				(*) For the BYOL Email Security Platform, Client shall provide and maintain vendor support work instructions and vendor support portal access so that Service Provider can perform vendor support escalations on behalf of Client. Problem Management includes the creation of Root Cause Analysis Reports (RCAs) for an IT Asset incident with recommended corrective actions as part of Continual Service Improvement. Corrective actions are assigned to either Service Provider, Client, or vendor according to ownership of the corrective action.
10.	Availability, Performance and Capacity Management.	X		Periodic reviews are performed of the Service with change recommendations to be implemented after approval from Client. Excluded: Expand or replace Email Security Platform to improve availability, performance, or capacity.
11.	Standard Service Request Management.	X		Standard service requests can be submitted by Client or Service Provider. Standard service request tasks for the Email Security Platform are included in the Service at no additional fee. See *Additional Responsibilities Matrices* section below for enumerated standard service requests and any exclusion thereof, as a well as enumerated billable service requests. Service Provider and Client perform standard service request tasks according to the task *Change Management* below.
12.	Change Management.	X (**)	X (*)	Service Provider and Client shall follow change management process according to the section *Change Management* in the *Managed Services ITSM Foundation Service Description.* (**) Service Provider is responsible for technical change execution of Client-approved changes to the Service and the Email the Security Platform. (*) Client is responsible for sending notifications to end users impacted by the change and preparing before and testing after a change of any impacted applications.
13.	Patch Management.	X	X (*)	(*) If the Email Security Platform is designated as "BYOL" in the *Pricing Summary*, Service Provider is responsible for patching. If the Email Security Platform is designated as "MSSP" in the *Pricing Summary*, and the platform is in the cloud, the platform vendor is responsible. Otherwise, Service Provider is responsible. For clarity, this task refers to patch management of the Email Security Platform – it does not include patch remediation execution on a Client IT asset according to the Response Recommendations of a Security Alert. (*) Client is responsible for patching underlying IT infrastructure in Client's IT environment that is supporting the Email Security Platform. Excluded: upgrades are separately billable.
14.	Continuity (Backup & Restore) Management.	X (**)	X (*)	(*) If the Email Security Platform is designated as "BYOL" in the *Pricing Summary*, Client is responsible for the backing up and restoring data related to the Email Security Platform software application binaries and data. Service Provider will ensure Email Security Platform is subsequently recovered and available. (**) If the Email Security Platform is designated as "MSSP" in the *Pricing Summary*, and the platform is in the cloud, the platform vendor is responsible for this task.

No.	Task Description	Service Provider	Client	Clarifications
15.	Billable Service Request Management.	X		When performed by Service Provider, all labor effort and any material costs associated with the request are billed separately according to the *Change Order Request Procedure* in the SOW. All exclusions listed for tasks in this *General Responsibilities Matrix* are considered billable service requests. See *Additional Responsibilities Matrices* section below for enumerated billable service requests.

2.3 ADDITIONAL RESPONSIBILITIES MATRICES

2.3.1 STANDARD SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Whitelist or backlist email addresses, domains and/or IPs.	X		
2.	Modify filtering sensitivity.	X		
3.	Add new user and remove existing user without a change in quantity of the Service.	X		
4.	Administration, Configuration, and Patching of the Email Security Platform.	X		

2.3.2 BILLABLE SERVICE REQUESTS

No.	Task Description	Service Provider	Client	Clarifications
1.	Manage Email Security Platform capabilities above and beyond those stated in this service description.	X		Service Provider shall evaluate, on a case-by-case basis, the additional monthly fee to manage those additional capabilities and shall be documented in the *Pricing Summary* when included in the Service.
2.	Perform phishing email triage when submitted manually.	X		Triage suspicious emails that were not blocked by the Email Security Platform and were manually submitted by Client end-users using the 'Report Phishing' button of the Email Messaging Platform. Service Provider performs this when the "Reported Phishing Email Triage" service is detailed in the *Pricing Summary*.
3.	Perform any service request that is not explicitly designated as Service Provider's responsibility in the *Support Responsibilities Matrix* or not enumerated in the *Standard Service Requests* table above.	X		
4.	Perform any task that is explicitly designated as Client's responsibility in the *Responsibilities Matrix*.	X		
5.	Deliver a new service not in scope of this Service.	X		
6.	Changing the quantities of the existing Services delivered.	X		
7.	Perform design, engineering, and consulting work in relation to a Email Security Platform or Client's IT environment.	X		
8.	Create additional documentation or reports beyond Service Provider runbook and standard reports for the Service.	X		

No.	Task Description	Service Provider	Client	Clarifications
9.	Modify *Service Provider's Information Security Management Policy & Procedures* to align with Client's Policy & Procedures.	X		
10.	Create, modify, or maintain *Client's Information Security Management Policy & Procedures.*	X		
11.	Implement, Reimplement, Migrate, or Upgrade Email Security Platform.	X		