avaya.com

Avaya Managed Services

Service Description

For Perpetual with Support Advantage or Subscription Customers

Version 6.0

October 12 2023

Table of Contents

1 About this Document

This Service Description describes the Avaya Managed Services Offer for eligible Supported Products and supersedes all prior descriptions or contract supplements relating to such support. When a translated version of this document conflicts with the English version, the English version will take precedence.

This document is an attachment to the End Customer's Commercial Agreement with Avaya and shall serve as the Service Description with respect to such support offering. In the event of a conflict between this Service Description and the End Customer's Commercial Agreement with Avaya, the terms and conditions of the End Customer's Commercial Agreement will control. In the event that an Avaya authorized reseller, distributor, systems integrator or service provider is purchasing support coverage for the End Customer, Avaya will provide the support specified herein to the End Customer.

1.1 Terms

The following are terms that may be referenced in this document:

- **Commercial Agreement**- as the context implies either the Customer's direct agreement or reseller agreement.
- **End Customer-** is the customer contracting the Service from Avaya.
- **End Users**- means Customer's employees, agents, permitted contractors or any other users of the Private Service.
- **Fixed Term Software Subscription** - a fixed quantity of Units of software provided by Avaya under the Subscription Licensing Terms for Customer's internal use (not for further resale, sublease, or sublicense) on a time-bound subscription basis.
- **Managed Order-** refers to an Avaya ordering document that contains Customer's order specifications. The order contains Service requirements and Customer pricing and is signed and submitted to Avaya by Customer along with the Customer's order.
- **Order Effective Date-**the start date of the Subscription Contract Term
- **Party**- refers to Avaya or Customer individually and "Parties" refers to Avaya and the Customer.
- **Provisioned**- means End Users configured for the Service.
- **Remote-** The delivery of Service remotely, not onsite.
- **Service Agreement Supplement or SAS** - a document that describes the features, terms and conditions of an Avaya support services offer.
- **Service Description or SD** – Scopes of Work/SOW's or SAS's that describe the features, terms and conditions of an Avaya service offer.
- **Subscription Managed Service Offer**- is the Managed Services provided by Avaya.
- **Supported Products**- refers to the specific products supported under the Subscription Managed Services.
- **Supported Site**- refers to Customer sites where Managed Services will be provided.

2 Supported Products

2.1 Release Levels

The Avaya Managed Service Offer defines release levels and the support that is available on such releases. The Avaya Managed Service Offer follows Avaya Subscription in supporting R6.3, R7, R8 and R10 Software release levels. Customers on older releases and CS1000 can convert into Managed Services coverage but must do so as part of an upgrade to a newer Avaya platform.

The scope of the Managed Services Offer support is limited to those available on such releases and are subject to Avaya Product Lifecycle Policy found at https://downloads.avaya.com/css/P8/documents/100081098.

2.2 Eligible Bundles & Products

The Avaya Managed Services Offer is available for the following Perpetual License and Subscription bundles and products:

2.2.1 Unified Communications Users

Separate prices for the following UC Users:

- UC Basic
- UC Core
- UC Power

No separate price for Attendant Console – it is entitled with UC Users.

Vendor Management only for ASR/TTS & VTT Transcription.

2.2.2 Contact Center Agents

Separate prices for the following CC Users:

- CC Basic Voice
- Digital Basic
- Digital Premium
- Oceana Supervisors
- Advanced Reporting
- Oceana Geo HA

No separate price for AES for Managed – it is entitled with CC Agents.

Important Note: AACC is not supported for Managed Services at this time.

2.2.3 IVR/port

Separate IVR/port pricing based on AEP Ports, except those entitled in the CC Basic Voice Agent

2.2.4 POM Outbound

Separate price based on the number of outbound ports

No separate pricing for Predictive, Preview and Email & SMS – these are entitled with POM Base Bundle

2.2.5 Workforce Management

Separate prices for the following

- AIX WE CR/Screen Capture
- AIX WE QM
- AIX WE WFM
- AIX WE WFO
- AIX WE Desktop and Process Analytics
- AIX WE Customer Feedback
- AIX WE Speech Analytics

No separate price for the following as they are entitled under Workforce Management: Speech additional languages, Real Time Speech add-on, Interaction Data Export Manager, N+N, and Encryption Server (Encryption itself is part of the ACR, QM, WFM, and WFO offers)

2.3 Eligibility Requirements

The Customer will ensure all Supported Products satisfy the Eligibility Requirements and will promptly implement all corrections, as may be reasonably required by Avaya, to ensure compliance.

The Supported Products will be deemed compliant with the Eligibility Requirements if they have been:

- Installed by Avaya or other manufacturers, as applicable, or their respective authorized resellers; and
- Covered by a support agreement with Avaya or their authorized resellers that has not expired earlier than 90 days before Order Effective Date with the exception of those Supported Products that have been installed within this 90-day period.
- For Perpetual License deployments, customers are required to carry Support Advantage coverage on the Perpetual licenses during the same term as the Managed Services.

3 Managed Services Service Elements

Under the Managed Services Offer, Avaya provides remote Services based on the Information Technology Infrastructure Library (ITIL®) principles.

3.1 Summary of Managed Services Elements

Table 1 provides an overview of the Service Elements provided by Avaya.

Note: Hardware Support continues to be available through Support Advantage and purchased separately. Hardware Support provides options for Advanced Parts Replacement and Onsite support.

Managed Service Elements
Service Management – Provides a designated service management interface to the Customer in support of the performance of the Managed Services. Details are in Section 3.2
Service Desk – Provides a level 2 service desk support for Customer's IT designated contacts for operational support during hours of coverage. Details are in Section 3.3
Event Monitoring and Notification – Monitors Supported Products for events that indicate an incident may be occurring, responding, and resolving alarms and providing notification update to customer. Details are in Section 3.4
Incident Management - Provides for the lifecycle of actions aimed at restoring Normal Service Operation impacted by an incident. Details are in Section 3.5
Problem Management – Provides for the lifecycle of actions aimed at preventing problems from reoccurring. Details are in 3.7
Configuration Management - Configuration Management is the process for creating and maintaining information pertaining to the Customer's configuration Details are in 3.8
Change Management - Change Management is the lifecycle of actions required to manage and implement changes to the use, configuration and set-up of the Supported Products. Details are in 3.9

Managed Service Elements
Back Up Management - Configure and activate automatic backup capabilities for the Supported Products in accordance with the backup frequency agreed in the Operations Guide. Details are in section 3.10
Release Management - Provides for the identification, scheduling and remote deployment of minor software releases firmware updates, and service packs. Details are in 3.11
Vendor Case Management - With a Letter of Agency (LOA) from the Customer, Avaya acts as Customer's agent and case manages, on Customer's behalf up to three (3) third-party vendors that are connected to the Supported Products. Details are in 3.12

Table 1 – Managed Service Elements

3.2 Service Management

Once the customer has been onboarded to Managed Services, a designated Service Delivery Manager (SDM) is assigned. This resource provides a interface to the Customer in support of the performance of the Managed Services. At the day-to-day level, the Service Delivery Manager arranges periodic touchpoints with Customer representatives to discuss performance (based on reporting and Customer feedback) and suggest improvement opportunities (if applicable). The Service Delivery Manager is an escalation point for facilitating resolution of incidents.

On an as-needed basis, working with the assigned Service Delivery Manager, Project Managers or other technical resources may be assigned as needed for short duration work such as Release Management upgrades or Move, Add, Change, Delete (MACD) projects.

3.3 Service Desk

The Avaya service desk will enable the customer to:

- Report Incidents and open service requests, including MACD requests, on the Avaya web portal or by calling Support 1-866-282-9267, and
- Track, via the Avaya web portal, the status of open iincidents.

The Service Desk is intended to act as the interface for the Customer's internal IT staff. Only Customer designated contacts may access the Avaya service desk. The Customer will be provided with up to 20 web portal logins.

In a Wholesale model, Partner designated contacts may access the Avaya service desk on behalf of the customer.

3.3.1 Exclusions

The following exclusion applies. The Avaya service desk may be accessed by Customer Designated Contacts only and not by individual End Users. The Avaya service desk is not a Help Desk for the Customer's End Users and will not assist with general usability and operational support queries,

3.4 Event Monitoring

Avaya will use the Avaya Managed Services Platform (AMSP) to proactively and reactively monitor Supported Products to detect Events. Remote monitoring will be performed using SNMP and ICMP. An Event will be classified as an Incident Severity as set out in Section 3.5.1 Upon detection of an Event, an incident record will be sent to the Avaya support team for resolution.

Avaya will provide electronic notification of Critical and Major incidents to customer designated contacts per timeframes outlined in section 4.1.

3.4.1 Exclusions

Event Monitoring excludes monitoring of Events at endpoint and/or individual User level, such as inability to retrieve e-mail, phone login or complete an action in a client software application.

3.5 Incident Management

Incident Management starts with the creation of an incident record and ends with the incident record closure. Avaya Incident Management responsibilities include:

- Identify Incidents and classify Incident Severity based on:
  - Events detected; and
  - Incidents reported by Customer.
- Assess, diagnose and confirm Incidents;
- Analyze and troubleshoot Incidents;
- Perform restore and remedial actions with the aim to restore Normal Service Operation impacted by an Incident which may include a temporary fix or work-around until a permanent fix, including deployment of patches or bug-fixes, becomes available; and
- Close Incidents including updating Incident Records with the details and history of Incidents.

3.5.1 Incident Severities

Incidents will be classified by Avaya in accordance with Table 2.

Incident Severity	Definition
Critical Incident	Incidents resulting in a loss of service that impact all End Users at a Supported Site.
Major Incident	Incidents resulting in a severe degradation or loss of service that impact a large number of End Users at a Supported Site, typically more than 25% of Users.
Minor Incident	Incidents that do not significantly affect Customer's normal business operations, including Incidents that affect: • A small number of Users at a Supported Site, including single User affecting Incidents; and • Availability or operation of a particular feature or functionality.

Table 2 Incident Severities

3.5.2 Customer Responsibilities

Customer responsibilities are:

- Performing initial troubleshooting activities for Minor Incidents;
- Resolving interoperability issues originating from any products or solutions which are integrated with, or connected to, Supported Products;
- Resolving all Customer network issues that may cause or contribute to Incidents, including static, call quality, packet loss, jitter and delay;
- Providing all information as reasonably required by Avaya to restore Normal Service Operation, including information gathered by any software or devices that monitor data traveling over Customer's network;
- At the request of Avaya restoring the Supported Product to its unaltered version to enable Incident reproduction and diagnosis, save for any alterations made by Avaya;
- Providing the required cooperation required to deploy temporary fixes or workarounds, including security patches or bug-fixes, as deemed necessary by Avaya to restore Normal Service Operation;
- Ensuring that Customer-provided virtualized environments used by Supported Products are:
    - Deployed and configured in accordance with Avaya specifications;
    - Covered under a support agreement with the provider of the virtualized environment or its authorized reseller throughout the Order Term and;
    - Accessible by Avaya on a read-only basis, if required to restore Normal Service Operation affected by an Incident.

3.5.3 On-site Intervention

Avaya will dispatch an on-site technician if, in the reasonable opinion of Avaya, an on-site technical intervention is required to restore Normal Service Operation subject to the following provisions:

- Customer has contracted for Support Advantage (SA) Parts & Onsite support. Note: the scope and exclusions of the contracted SA Parts & Onsite support is governed by Support Advantage SAS for Parts & Onsite,
- SA On-Site and Parts support does not include telephone set replacement. If set replacement coverage is required SA Terminal Replacement must also be purchased by the Ccustomer.

3.5.4 Customer responsibilities

Customer responsibilities are:

- Contracting SA On-Site & Parts and SA Terminal Replacement
- Fulfilling Customer responsibilities defined by SA Parts & Onsite SAS.

3.6 Vendor Case Management

Under Vendor Case Management, Avaya will act as Customer's agent and manage, on Customer's behalf Customer up to three (3) third-party vendors that are associated with the Avaya supports. Avaya will:

- Provide case management only – Avaya does not manage the actual application;
- Notifying Ccustomer's Vendors to perform the corrective activities required to resolve error conditions that impact normal usage of the Supported Products (such as network carrier issues), monitor progress and record status in the AMSP;
- Coordinate with Customer Vendors to perform On-Site Support, if required to restore Normal Service Operation, monitor progress and record status in the AMSP

3.6.1 Customer Responsiblities

Customer responsibilities include:

- Execute a LOA with each 3rd party vendor in order for Avaya to provide this support.
- Contract support with each 3rd party vendor.

3.6.2 Scope:

- Customer identified carriers will count as one (1) Customer Vendor
- Not counted towards the maximum number of 3 Customer Vendors are:
  - Customer Vendors who deliver On-Site Support on Customer's behalf for the Supported Sites where no SA Parts & Onsite Support is available.
  - Customer Vendors supporting Avaya Professional Services (APS) productized applications (e.g. Call Back Assist, etc.)
  - Avaya Vendors supporting Subscription and Support Advantage products that are supported with supplier backed Support Agreements. . Examples: Mutare, Avaya WFO, Nuance, etc.

3.7 Problem Management

Problem Management starts with the creation of a problem record and ends once the actions aimed to prevent the problem from reoccurring have been completed and the associated problem record is closed by Avaya.

3.7.1 Definitions

A "problem" is a critical or chronic incident:

- A critical incident, in the reasonable opinion of Avaya, is likely to reoccur; and
- A "chronic incident is an identical incident that impacts normal service operation that occurs 4 or more times over a consecutive 3-month period with respect to the same Supported Product.

3.7.2 Avaya Responsibilities

Avaya responsibilities are:

- Identifying problems based on:
  - Analyzing Incident Records to identify chronic incidents;
  - Based on the case completion information available in incident records, performing a critical incident analysis to assess risk of reoccurrence and if the relevant critical incident should be treated as a problem;
  - Reviewing incidents that require a permanent fix and qualifying if such incidents should be treated as a problem; and
  - Reviewing Problems notified by customer;
- Communicating and confirming identified problems;
- Analyzing and diagnosing the root cause for problems;
- Performing corrective actions aimed at preventing problems from reoccurring, including the implementation of security patches; and
- Closing, including updating problem records with details and history.

3.7.3 Customer Responsibilities

Customer responsibilities are:

- Allowing Avaya to implement corrective actions, which may include scheduled changes or deployment of security patches, as Avaya deems necessary to prevent Pproblems from reoccurring;
- Promptly implementing the corrective actions recommended by Avaya with the aim to prevent problems from reoccurring, including purchasing and deploying additional resources.

3.8 Configuration Management

Configuration Management is the process for creating and maintaining information pertaining to the Customer's configuration.

3.8.1 Avaya Responsibilities

Avaya responsibilities are:

- Creating and maintaining Configuration Item (CI) records for the Supported Products in the Configuration Management Data Base (CMDB) including the following information such as type of equipment and software release level.

- Providing Customer, via the Avaya web portal, with read-only access to the information stored in the CI records;
- Posting monthly inventory reports on the Avaya web portal; and
- Posting, upon Customer's request, an interim inventory report on the Avaya web portal, if CI records have been updated during that month.

3.8.2 Customer Responsibilities

Customer responsibilities are:

- Notifying Avaya of any changes made by Customer to the Supported Products; and
- Notifying Avaya of any changes to Customer network or products connected to, or integrated with, Supported Products that may impact performance of the Supported Products, including network configuration or changes to IP addresses.

3.9 Change Management – MACDs & Operational Changes

Change Management is the lifecycle of actions required to manage and implement changes to the use, configuration and set-up of the Supported Products. Changes include MACDs and operational changes. An operational change may occur as a result of Incident Management or Problem Management.

3.9.1 MACDs

A MACD is a move, addition, change or deletion of user profiles, call-flows and dial plans. MACDs

- Affects only one Supported Site;
- Can be completed within 1 change window;
- Requires no project management;
- Does not change the architecture of the solution;
- Requires no additional software or hardware; and
- Requires no implementation or professional services.

3.9.2 Simple or Complex MACDs

MACDs are categorized as Simple or Complex:

- **Simple MACDs** are performed at the user level, including adding, changing or deleting user mailboxes and phone extensions and resetting passwords; and
- **Complex MACDs** are performed at the system or application level.

3.9.3 Customer or Avaya Supported MACDs

The Customer can perform MACDs or has the option for Avaya to perform the changes or a combination of the two.

If the Customer performs their own MACDs, the Customer has the responsibility to notify Avaya in advance when they are making a complex MACD change. If the Customer incorrectly implements a

change that results in Avaya having to fix it, Avaya has the right to charge the customer. MACD Service Levels will not apply if the Customer chooses to perform MACDs.

If the Customer chooses Avaya to support MACDs, except for simple MACDs all changes will be submitted, approved and implemented by Avaya in accordance with the Change Management process agreed in the Operations Guide. The Operations Guide details the operational processes that Avaya will use while performing the Managed Services with the Customer.

Avaya will store the details of MACDs and Operational Changes in a change record in the AMSP.

3.9.4 MACD Time Frames

Avaya will perform remote MACDs within the time periods set out Table 3,

Simple MACD – up to 15 activities per MACD	In accordance with the Service Level Objective: Next Business Day for 95% of eligible MACDs
Simple MACD – greater than 15 activities per MACD	As agreed by the Customer & Avaya on a case by case basis, depending on Customer's priorities and MACD scope.
Complex MACD	As agreed by the Customer & Avaya on a case by case basis depending upon Customer's priorities, available change windows and MACD scope.

Table 3 - MACD Time Periods

3.9.5 Remote MACD Entitlement

During each consecutive 12-month period (defined as a MACD Year) measured from the Operations Start date the Customer will be entitled to a monthly remote block of hours (BOH). The MACD entitlement does not apply to on-site MACDs and projects.

The MACD Entitlement will be calculated at the start of each MACD Year. MACDs will expire, if unused during the applicable month, at the earlier of: (i) 3 months following the end of applicable month; and (ii) end of the relevant MACD Year.

The MACD Entitlement for Unified Communications users will be calculated as set out in Table 4.

Formula:	Total number of UC Basic, Core and Power users × 3% × 0.25 hours = Monthly MACD Entitlement
Example:	5,000 UC Core Users × 3% × 0.25 hours = 37.5 hours per month

Table 4 - Unified Communications MACD Entitlement

The MACD Entitlement for Contact Center Communications will be calculated as set out in Table 5.

	Total Number of Agents (Basic CC Voice, Digital Basic and Digital Premium)	Monthly MACD Entitlement
Agent Licenses	100 – 249	15 hours per month
	250 – 1,500	25 hours per month
	1,501 – 5,000	45 hours per month
	5,001 – 10,000	65 hours per month
	10,001 – 20,000	95 hours per month
	20,001 +	115 hours per month

Table 5 Contact Center MACD Entitlement

3.9.6 MACD Tracking & Invoicing

This section details the invoicing and usage tracking methodology applicable to the performance of remote MACDs by Avaya that are not included in the Monthly MACD Entitlement. The remote MACD Charges comprise:

- Charges for remote MACD block of hours purchased by Customer in addition to the Monthly MACD Entitlement;
- Remote MACD block of hours purchased
- Charges for remote MACDs performed by Avaya on a T&M basis. Avaya will charge and invoice Customer for any remote MACDs performed by Avaya on a T&M basis monthly in arrears.

3.9.7 Tracking of MACD Hours

Avaya will track Customer's usage of remote MACD block of hours, whether included in the Monthly MACD Entitlement or additionally purchased, as described in Table 6,

Period	Minimum Usage	Minimum Increment	Overtime Factor
Business Hours	No minimum	15 minutes (any started 15 minutes will be rounded up to the quarter hour)	Not applicable
Outside Business Hours	1 hour	30 minutes (any started 30 minutes will be rounded up to the half hour)	2 (1 hour of MACD work will use 2 hours from applicable MACD block of hours)

Table 1 - Tracking of MACD Usage

3.9.8 Customer Responsibilities

Customer responsibilities are:

- Submitting Complex MACD requests no later than 3 Business Days prior to the requested change window;

- Providing required change windows; and
- Making only those changes to the Supported Products that have been reviewed and approved by Avaya in accordance with the agreed Change Management process.

3.9.9 Out of Scope

The following are not in scope:

- All **On-site MACDs** will be charged and invoiced to Customer separately in accordance with the then prevailing rates of Avaya.

- **Projects** will be performed in accordance with a statement of work agreed by Avaya and the Customer and will be subject to additional charges.

3.10 Backup Management

Avaya will support the following with backup management:

- Prior to Managed Services activation:
  - Configure and activate automatic backup capabilities for the Supported Products in accordance with the backup frequency agreed in the Operations Guide; or
- Perform a manual backup of the Supported Products that do not have automatic backup capability.
- Before performing any system level changes in accordance Change Management, perform a backup of the relevant Supported Product either by initiating an unscheduled automatic backup or performing a manual backup; and
- Monitor the Supported Products for any Events indicating failed backups.

If Avaya determines that Normal Service Operation must be restored from a Supported Product backup, Avaya will perform the restoration based on:

- Procedures and instructions set out in the relevant manufacturer specifications; and
- Backup restoration process agreed by the Parties in the Operations Guide.

3.10.1 Customer Responsibilities

Customer responsibilities are:

- Providing backup server, media or file location in accordance with the specifications detailed in the Operations Guide;
- Notifying Avaya of, and resolving, any issues relating to backup server, media or file location provided by Customer, that may prevent successful completion of backups;
- Regularly backing up Customer products integrated with, or connected to, the Supported Products in accordance with good computing practices; and
- Ensuring the quality of backups and resulting ability to restore Normal Service Operation from backups including:
  - Prior to Service Activation, and thereafter regularly, verifying that Normal Service Operation can be restored from available backups; and
  - Implementing an appropriate backup rotation scheme.

3.11 Release Management

Release Management provides for the identification, scheduling, remote update deployment and CMDB update of the following "Updates" to the Supported Products:

- Minor software releases or updates;
- Firmware updates; and
- Service packs
- Avaya provided Operating System (OS) patches, and anti-virus updates (when applicable)

3.11.1 Update Identification, Review and Scheduling

Avaya will notify Customer of any applicable Updates within 5 Business Days from: (i) receipt of the update notification; or (ii) becoming aware of an Update if automatic notifications are not available.

During the monthly Stewardship meeting with the Avaya Service Delivery Manager, based on an update recommendation report provided by Avaya in advance of this meeting, the Parties will:

- Review Updates applicable to the Supported Products, considering their impact on Customer's product environment; and
- Determine the Updates that will be deployed.

Avaya will develop an Update deployment schedule based on:

- Priority and impact of each Update;
- Available change windows;
- Change Management process; and
- Dependencies on any activities performed by Avaya or Customer.

Following successful deployment of an Update, Avaya will update the relevant CI record.

3.11.2 Exclusions

Release Management does not include provision and deployment of:

- Any updates that require on-site deployment;
- Updates that require impact assessment on the operation of customer applications as deemed necessary by Avaya or requested by Customer;
- Major software releases or hardware upgrades that require reinstall & restore process of Software and Software Translations; and
- Security Certificate or Certificate Management; and
- Emergency patches that are required to support Incident Management to fix something immediately for the Customer or a patch because of a security vulnerability.

3.11.3 Customer Responsibilities

Customer responsibilities include:

- Reviewing and approving Updates and Update deployment schedules;
- Providing suitable change windows; and
- Implementing on-premise deployed software and hardware upgrades;

3.11.4 Disclaimers

Avaya will not be responsible for failure to comply or delay in complying with any of its obligations including failure to meet any Service Levels, to the extent such failure or delay has been caused by, or contributed to:

- Customer's decision not to implement or delay the implementation of any Update; or
- Customer's failure or delay in the acquisition or implementation of any upgrades.

4 Avaya Client Scorecards

Managed Services customers now have a new Service feature available to them in Avaya Client Scorecards. Avaya Client Scorecards are a window into the health and status of customer's production environment. In coordination with your Service Management team, the Client Scorecards allow a customer to take targeted actions required for optimization, ability to understand their solutions in relation to support, see recommended updates needed and receive advice on potential issues.

The Avaya Client Scorecard is a set of performance scores based on input taken from reading the environment, application & configuration information from your landscape. These scores help identify critical security & best practice areas where your environment is well aligned versus needing improvement or immediate attention.

Avaya Client Scorecards highlights performance in the following key areas:

Lifecycle Status:
In terms of security, newer software and firmware versions are inherently more secure than older counterparts. The weakest link in terms of security is often the oldest. Thus, Avaya strongly advises a thorough review of software versions. Assets unable to receive Service Packs, Bug Fixes, Patches, and Security Updates are of particular concern. Beyond the potential security risks, non-upgraded assets may also lead to compliance issues. Avaya suggests upgrading any assets that have exceeded their end-of-service life.

Connectivity Status:
SAL access for all devices is crucial. In emergencies, SAL-connected servers quickly identify and diagnose issues, minimizing outage time. Servers without SAL may prolong outages significantly. Avaya strongly advises auditing for SAL registration of every element.

SIP Conversion:
Growing demands for agility, remote work, digital integration, and productivity call for widespread SIP device adoption. Avaya suggests migrating non-SIP devices to enhance functionality, flexibility, and security. Consideration of DaaS is also recommended. Transitioning from legacy Gateways (GWs) with DS1 packs can significantly reduce space, power usage, and carbon footprint. Migrating from DS1 to SIP trunks offers cost savings and improved resilience. Since major carriers are discontinuing DS1 services, Avaya advises an immediate shift to SIP Trunks and consideration of retiring outdated Circuit Packs and GWs.

Security:
Security plays a crucial role in ensuring a secure network, encompassing various elements such as encryption protocols, encryption algorithms, password strength and certificates. Avaya advises TLS 1.2/1.3 with advanced encryption algorithms such as SHA512 for enhanced security. Implementing stringent password policies for strength, expiry & login attempts is pivotal for security. Self-signed certificates lack trustworthiness and should be migrated. Certificate planning and migration can be complex, but ensuring the correct certificate structure is essential for security and compliance.

Certificate Expiry:
For trust and functionality, maintain valid certificates. Expired certificates can lead to issues with features, phones, trunks, or clients. Avaya advises updating expired certificates and monitoring upcoming expirations.

Vulnerability:
Vulnerability Management is crucial for security risk management. Most major attacks target known vulnerabilities, not only zero-day attacks. Avaya advises frequent scans and prompt patching of critical vulnerabilities.

Avaya Client Scorecards require Avaya's standard Managed Services [ASCI] connectivity and are available upon request or on a pre-determined schedule through your Service Management team.

5 Service Levels Agreement, Reporting & Service Credits

This section details the Service Levels Agreements that will apply to the Managed Services Offer. Service Levels will begin on the start date of the Support Contract.

5.1 Sevice Level Agreement:

The Managed Services Offer will be performed in accordance with the Service Level Objectives listed in Table 6.

Service Level	Service Level Description	Incident Severity	Target
Time to Notify	Elapsed time from creation of an Incident Record until Avaya has provided an electronic notification to Customer.	Critical	15 minutes for 95% of Incidents
		Major	60 minutes for 95% of Incidents
Time to Restore	Elapsed time from creation of an Incident Record until Avaya has restored Normal Service Operation	Critical	MTTR of 4 hours
		Major	MTTR of 6 hours
		Minor	Next Business Day for 85% of Incidents
Time to Complete MACD	Elapsed time from receipt by Avaya of an Eligible* MACD request until MACD completion.	N/A	Next Business Day for 95% of Eligible MACDs

Table 6: Service Level Description

* An Eligible MACD is simple MACD of no more than 15 activities and is received by Avaya before 3pm local Supported Site time during Business Days.

Where:
MTTR refers to the mean time to restore which is calculated based on the following formula:

> **X** divided by **Y**
> Where:
> ***X*** is equal to the sum of the Time to Restore periods for all Incidents with the same Incident Severity which have occurred during a Measurement Period; and
> ***Y*** is equal to the total number of Incidents with the same Incident Severity that have occurred during a Measurement Period.

5.2 Service Level Exclusions and Limitations

The following exclusions and limitations apply to the Service Levels:

- When measuring and determining the Avaya compliance with the Service Level targets the Avaya and the Customer "Parties" will exclude:
  - Any time during which Avaya has been prevented from performing, or has been unable to perform, an activity for reasons beyond the reasonable control of Avaya, including denial of remote or on-site access to the Supported Products or Supported Sites;
  - Any time during which Avaya has been awaiting a Customer or third-party deliverable, action, dependency or prerequisite, including Customer testing or verification of Incident solutions prior to implementation;

- Scheduled maintenance time or planned downtime;
- Supported Products that do not satisfy the Eligibility Requirements as identified in Section 2.3;
- Incidents for which no temporary fix or work-around is available and that require deployment of an, patch or bug-fix to restore Normal Service Operation;
- Incidents that require an Operational Change;
- Incidents caused, or contributed to, by:
  - Actions or omissions of Customer or third parties, including carrier and service providers;
  - Reasons external to the Supported Products, including power failures and shutdowns, third party products and applications, networks and network service interruptions;
  - Custom Applications or originating from Custom Applications; and
  - Any other reasons beyond the reasonable control of Avaya, including force majeure events.

- Incidents that require On-Site Support are eligible for the Time to Restore SLA only if:
  - Customer has purchased SA Parts & Site support;
  - The affected Support Product is manufactured by Avaya; and
  - The affected Supported Site is in a major metropolitan area.
- Time to Complete MACD SLA will not start for an Eligible MACD until such time as Avaya has received a correctly completed and authorized MACD request from Customer; and
- Time to Complete MACD SLA will only apply if during the applicable Measurement Period Avaya has failed to complete more than two or more MACD requests on the next Business Day after receipt of the request.

5.3 Standard & Service Level Reporting

Avaya will provide the standard reports detailed in Table 7. Standard reports will be updated and provided monthly electronically, which may include posting reports on AMSP.

Report	Description
Incident Management Reports	Report summarizing open and closed Incidents since the last report, including Incident description, priority, impact and status. This report will also include a 6-month rolling trend analysis.
Service Level Report	Report detailing Avaya performance against the Service Levels including a 6-month rolling trend analysis.
MACD Summary Report	Summary of MACDs completed by Avaya under Change Management including information on MACD quantity, type and status, and compliance with the MACD Service Level.
Inventory Report	Report summarizing records stored in the CMDB.

Table 7 Standard Reports

5.3.1 Service Level Reports

Customer will review each Service Level report within 2 weeks from the date it has been made available to Customer. If Customer has not rejected a Service Level report in writing within this time period, the Service Level report will be deemed accepted by Customer. Any comments or disputes relating to Service Levels or Service Level reports will be addressed by the Parties during the monthly stewardship meetings. Any unresolved matters will be escalated pursuant to the escalation process agreed in the Operations Guide.

5.4 Service Credits

This Section details the Service Credits that will apply from the Managed Services Operation Start Date. Service credits that will apply if Avaya has failed to achieve the agreed Service Level targets set out in Section 4.4.1

5.4.1 Time to Restore Credits

The following Service Credits will apply if, during any monthly measurement period, Avaya has failed to achieve the Time to Restore target for a Critical or Major Incident:

Incident Severity	Service Credit
Critical	2% of the Recurring Charges payable for the affected Measurement Period for the Supported Site where the Time to Restore exceeded 4 hours.
Major	2% of the Recurring Charges payable for the affected Measurement Period for the Supported Site where the Time to Restore exceeded 6 hours.

5.4.2 Time to Complete MACD

If Avaya has failed to achieve the Time to Complete MACD target during any Measurement Period, the applicable Service Credit will amount to 1% of the Recurring Charges payable for the affected Measurement Period for the Supported Site were eligible MACD was not completed prior to close the next Business Day.

5.4.3 Service Credit Terms

The Service Credits are subject to the following terms:

- Service Credits will become due and payable only if requested by Customer in writing within 90 days after the end of the relevant Measurement Period;
- Services Credits due will be paid by Avaya within 90 days from receipt of Customer's request;
- Payment of Service Credits will be made in the form of a credit against future amounts due from Customer to Avaya;
- The total amount of all Service Credits due from Avaya for any Measurement Period may not exceed 5% of all Recurring Charges due for that Measurement Period;

- Customer's right to request Service Credits will not suspend its obligation to make timely payments of any Charges due and payable by Customer to Avaya; and
- The Parties agree that Service Credits are fair and reasonable, represent a genuine pre-estimate of any resulting loss or expense to Customer, and are the sole and exclusive remedy to Customer in the event of an Avaya failure to achieve the Service Levels targets.

6 SERVICE TRANSITION

Service Activation & Transition to Managed Services will commence promptly following the Order Effective Date and will be performed in accordance with the Transition Plan. Service Transition will conclude on Operations Start Date which will be 90 days after Order Effective Date. For customers already in Managed Services Support, migrating or renewing to the new Managed Services offer, the 90 day Service Transition and Onboarding period will not apply.

6.1 Key Dates

Key Date	Description
Service Activation & Transition	Beginning on Order Effective Date Avaya will activate and start the Managed Services for Supported Site(s) and the Supported Products located at such Supported Site.
Operation Start Date	Ninety (90) days after Order Effective Date.

6.2 Service Activation & Transition

This Section details the responsibilities of Avaya and the customer ("Parties") during Service Activation & Transition.

6.2.1 Initiation

During this stage:

- The Parties will each assign a project or program manager to kick-off and manage Service Activation & Transition;
- Customer will Designate a SPOC that Avaya may contact in relation to all general aspects of the Managed Service, including operational matters. The Customer SPOC will have, or will obtain within Customer's organization, a thorough understanding of Customer's business requirements and technical environment, and will ensure all Customer binding decisions are duly authorized; and
- Avaya will develop a draft of the Transition Plan,

6.2.2 Transition Plan

The Transition Plan will be developed by Avaya and will include the following items and such other items as may be agreed by the Parties in writing or deemed necessary by Avaya:

- Project plan;
- Communication plan;

- Risk mitigation plan;
- Specification of data and information to be provided by Customer including:
  - Data for Supported Products required to activate the Managed Services; and
  - Information required for developing the Operations Guide.
- Detailed list of Service Transition responsibilities and deliverables of the Parties; and
- Service Transition dependencies, prerequisites and assumptions.

Upon completion of the Transition Plan by Avaya and following a review by Customer and implementation of any mutually agreed Customer requested changes, Avaya will submit the Transition Plan for Customer's acceptance. Within 5 Business Days from its receipt, Customer will accept the Transition Plan. Any changes to the agreed Transition Plan will be mutually agreed in writing by the Parties.
Avaya will not commence with the activities required to activate the Managed Services until Customer has accepted the Transition Plan.

6.3 Customer Data Collection

Customer will promptly make available to Avaya the data for all Supported Products required to activate Managed Services as detailed in the Transition Plan.

6.4 VPN Connection

The Parties will implement the VPN Connection to enable Avaya to remotely monitor and access the Supported Products throughout the term of the contract. The VPN connection will carry the following traffic:

- **Machine-to-machine** sessions comprising automated transactions, including SNMP polling of the Supported Products by the AMSP, transmission of alarms by the Supported Products to the AMSP and analysis of RTCP data to determine and diagnose voice quality issues; and
- **Human-to-machine** sessions involving remote access to the Supported Products by the Avaya technicians.

The VPN Connection will comply with the following specifications:

- **Transport medium**: Internet;
- **Security protocol suite:** IPsec;
- **Connection redundancy:** single VPN connection;
- Address translation: not required, but allowed at one or both sides of the VPN Connection; and
- Traffic flows: bi-directional.

6.4.1 Avaya and Customer Responsibilities

Each Party is responsible for the implementation of its end of the VPN Connection and performance of the following activities:

- Implementation and administration of IPsec configuration details;
- Implementation of the required firewall and access control policies;
- Performing tests to confirm that the VPN Connection is able to support:
  - Bi-directional machine-to-machine sessions; and
  - Human-to-machine sessions using each of the management applications required by Avaya.

The Parties will agree on the technical specifications and settings for the VPN Connection comprising:

- IPsec configuration details based on a VPN worksheet supplied by Avaya; and
- Firewall and access control policies based on the traffic flow information provided to Customer by Avaya consisting of the source and destination IP addresses, destination ports and protocols and direction of the required traffic flows.

Avaya will perform tests to confirm the readiness of VPN Connection for the Managed Services, including testing the ability of Avaya to access the Supported Products via Customer network. Upon successful completion of the tests Avaya will confirm the VPN Connection readiness to Customer.

- If during the tests Avaya identifies any issues that require remediation by Customer, Customer will remedy those issues promptly following notification from Avaya, so as to ensure that the Operation Start Date is not delayed. Following such remediation, Avaya will re-perform the readiness tests.

6.4.2 Additional Customer Responsibilities

To enable the VPN Connection Customer will:

- Assign an IPsec qualified and knowledgeable resource who will work with Avaya to establish the VPN connection.
- Implement the VPN Connection no later than 3 months after the Order Effective Date.
- Provide the following:
  - Publicly accessible interface to terminate the VPN Connection at Customer's end of the VPN Connection;
  - Adequate bandwidth to support the traffic generated by the Managed Services;
  - Unique IP addresses for each Supported Product; and
  - NUIs for the Support Products which have no built-in network connectivity.
- Ensure that Customer's end of the VPN Connection is available, and all Supported Products can be remotely monitored and accessed by Avaya via Customer's network on a 24x7 basis, without restriction or interruption; and
- Administer, operate and maintain Customer's end of the VPN Connection, including providing Avaya with a point of contact for ongoing VPN Connection administration and support.

6.5 Operations Guide

Avaya will develop the Operations Guide. The Operations Guide and any changes to it will be provided for Customer's review and approval. The Operations Guide will include the information as detailed in below table. Information may be excluded or added as agreed to by the Parties in writing or as deemed necessary by Avaya:

Topic	Content
Governance	• Key contacts for performing the Managed Services; • Escalation processes; and • Change advisory board.

Topic	Content
Invoicing	• Invoicing processes (including escalation of invoicing issues); and • Invoicing data and reporting.
Infrastructure Requirements	• Remote access methodology (VPN Connection); and • Specification for backup server, media or file location.
Processes & scope	• Managed Service elements as listed in Section 3 and; • Change Control

6.6 Service Activation & Operations Start Date

Prior to Service Activation for a Supported Site Avaya will:

- Set up Event Monitoring on the Supported Products;
- Perform backups for the Supported Products;
- Confirm readiness of the Supported Products, including confirmation that Customer complies with the relevant responsibilities, and AMSP for Managed Services delivery; and
- Provide each Customer Designated Contact with login credentials to AMSP.

Once all sites have gone through Service Activation then the Operation Start Date begins. Each site gets a Service Activation Date and once all sites are onboarded to the Services, then that is the Operation Start Date that Avaya will activate and start the Managed Services.

6.7 Delays in Service Transition

If Customer has not timely accepted the Transition Plan or if Customer fails to perform any Service Transition responsibility in accordance with the timelines set out in the Transition Plan, until such time as Customer has completed the delayed responsibility, following written notification to Customer Avaya may:

i. Suspend Service Transition;
ii. Exclude affected Supported Products from Service Transition; and/or
iii. Charge Customer for any additional activities performed and costs incurred by Avaya as a result of the delay.

In case Supported Products were excluded from Service Transition:

- Transition at a later stage will be separately chargeable and performed by Avaya subject to Change Order;
- Unless otherwise agreed by Avaya in writing, such exclusion will not delay the Service Activation Date of the affected Supported Site and remaining Supported Products located at such Supported Sites nor will it affect the Minimum Monthly Revenue Commitment.

7 Staffing Model & Coverage Hours

Avaya leverages global resources for the delivery of the Managed Services and/or personnel in remote locations globally. Local personnel could include permanent residents or visa holders.

Business Hours are 8:00 a.m. to 5:00 p.m., in the time zone where a Supported Site is located, during Business Days.

Business Days are official working day at the relevant Supported Site, typically Monday through Friday, excluding public and Avaya observed holidays.

Avaya will provide the Managed Services during the Coverage Hours as set out in the table below:

Managed Service element	Coverage Hours
Service Transition	Business Hours except if otherwise agreed by the Parties in the Transition Plan
Avaya service desk	24x7
Event Monitoring	24x7
Incident Management	24x7
Remote Simple MACD Requests	Business Hours
Remote Complex MACD Requests	Business Hours or 24x7
All other Managed Services	Business Hours

8 Compliance & Security

8.1 HIPAA

The Managed Services can comply with the Health Insurance Portability (HIPAA) and Accountability Act and associated regulations, however the request must be reviewed and approved by Avaya prior to ordering the Managed service. Sales should work Avaya Contracting to reach out to Legal (Wes Sowell) for BAA language.

Unless otherwise agreed to by Avaya, the Customer agrees that it will not introduce Protected Health Information (as defined in HIPAA, PHI) into the Managed Service for any purposes and shall indemnify, defend and hold harmless Avaya against all actions, claims, losses, fines, penalties, damages and expenses (including reasonable attorneys' fees) arising out of Customer's use of the Managed Services with PHI.

8.2 PCI

The Managed Service are not designed to be compliant with the payment card industry (PCI) data security standard also referred to as PCI or PCI DSS.

8.3 Safeguards and security policies

Avaya will perform the Managed Services in accordance with the Avaya safeguards and security policies and procedures, which will be consistent with industry recognized standards, comprising ISO 27001 or ISO 20000. Avaya will establish and, throughout the Order Term, maintain the policies, processes, and controls with the aim to protect:

- Customer's systems and data in the possession or control of Avaya against unauthorized access, disclosure, alteration or destruction, resulting from performance by Avaya of the Managed Services and access to Customer's network and Supported Products; and
- Avaya systems and data used in performance of the Managed Services against unauthorized access, disclosure, alteration or destruction.

Avaya will follow its regular procedures and processes to prevent viruses from being introduced by Avaya into the Supported Products, Customer's network or information systems connected to or integrated with the Supported Products during the performance of the Managed Services. A virus is malicious software such as viruses, worms, Trojan horses, trapdoors, time, or logic bombs, corruptive or disabling codes and routines.

If Customer requires Avaya to make any modifications to the Avaya safeguards and security policies or procedures or comply with any additional security or compliance requirements in the performance of the Managed Services, such requirements will be reviewed by Avaya and, upon agreement by the Parties, implemented under and may entail additional Charges.

8.4 Audits

Avaya will engage an independent external auditor to perform industry standard audits on the Avaya safeguards and security policies and procedures, which may include industry standard certifications, with the aim to validate that the security controls are in place and operational. Upon Customer's written request, once a year, Avaya will provide Customer with a copy of the external audit report or certification in possession of Avaya. No other audits will be allowed on the Avaya policies, procedures, platforms, processes, facilities or infrastructure. At no time will Avaya permit any technical testing of the Avaya infrastructure, including vulnerability scans or penetration testing. Any changes to these audit provisions will be reviewed and implemented may entail additional Charges.

8.5 Password Management

To the extent Customer has given Avaya control and authority to change system level passwords for the Supported Products, Avaya will change such passwords on a recurring basis in accordance with the Avaya safeguards and security policies, unless a specific password management schedule has been agreed by the Parties in the Operations Guide. Avaya will retain ownership of all passwords to any Avaya-owned equipment located at the Supported Sites and will not provide such passwords to Customer, except were

deemed necessary by Avaya. Avaya will manage passwords to Avaya-owned equipment in accordance with its standard password management policy.

8.6 Customer Responsibilities

Customer responsibilities include:

- Providing Avaya with all passwords that Avaya requires to access the Supported Products and give Avaya the exclusive control of, and authority to change, such passwords;
- Ensuring that Customer's network and all Customer information systems, hardware and software that are required under this Service Description in connection with the Managed Services are available and operating in accordance with their specifications and are free from, and adequately secured against, viruses, unauthorized access, intrusion or attack. Customer practices include:
    - Conducting regular vulnerability scans (at least once per quarter) and sharing the results with Avaya upon request; and
    - Following Customer's regular procedures and processes to prevent viruses from being introduced into or remaining within Supported Products, Customer's network or any information systems connected with or integrated with the Supported Products.

9 Contract Terms and Billing

9.1 Contract Term & Billing Options

Managed Services Offer is available in a 1, 3 or 5 year Fixed Contract Term. The 1 year term is an exception requiring approval to quote and order for net new customers moving to the new Managed Service offer. For current Managed Services customer, migrating or renewing coverage into the new Managed Services offer a 12 month term is permitted. The Managed Services Offer contract will co-term with the Subscription or Support Advantage contract.

Billing is the frequency in which the Managed Service Offer is billed. Billing options are either monthly in advance or annual in advance.

9.2 Renewal

A prerequisite for this offer renewal is the Subscription or Support Advantage contract renewal.

This offer will automatically renew at the end of the term for a similar term length at then current pricing unless either party provides written notice of its intent not to renew such coverage at least 30 days prior to the renewal date.

If a customer is located in the EU, this Offer will automatically renew for another year at then current pricing unless either party provides written notice of its intent not to renew such coverage at least 30 days prior to the renewal date.

If shorter renewal terms are required by local country laws or regulations, the Managed Services Offer will automatically renew for the maximum term permitted by such local country laws or regulations, and Avaya will notify customer of same.

9.3 Termination Policy

The Customer may terminate the Managed Services Offer in its entirety during the Order term upon thirty (30) days' written notice subject to termination fees equal to 50% of the remaining balance of the Manages Services Offer term.

In no case will any prepaid fees be credited due to a contract terminated for convenience

9.4 Billing Start Date

For net new customers, the billing start date for the Managed Service Offer will begin 3 months from the Order Effective Date. The contract end date for the Managed Services Offer will co-term with the or Support Advantage contract.

For current customers already on Managed Services support contract, migrating or renewing to the new Managed Services offer, the 90 day Service Transition and Onboarding period will not apply and the billing start will begin on the order effective date.

The billing start date for Managed Service offer will align with what is documented in the Subscription and Support Advantage Offer Definition.

10 Contracting Considerations

10.1 Minimum Order

When adding Managed Services, Customers are required to have a minimum number of UC users or CC agents under coverage: These thresholds are:

- 500 UC users (sum total of UC Basic + UC Core + UC Power)
- 250 UC + 250 CC agents (sum total of CC Basic Voice + Digital Basic + Digital Premium)

10.2 No Mixing Perpectual and Subscription Licenses

The Managed Service Offer will follow the Avaya Subscription License Transaction direction and policies defined in the Avaya Subscription Offer Definition. A mix of perpetual and subscription licenses will not be supported by Managed Services. Only Subscription or Perpetual licenses will be supported at the same customer Sold To Location.

10.3 Expansion Allowance

The Managed Service Offer includes the Avaya Subscription 20% expansion allowance which can be leveraged during the contract period without impact to the billing.

Customers can also expand beyond the 20% allowance by ordering additional Avaya Subscription licenses and associated Managed Services offering co-terming to the existing contract expiration dates. Expansion allowance is supported in accordance with Avaya's Product Lifecycle Policy found at https://downloads.avaya.com/css/P8/documents/100081098

Revisions

Offer ➔	Avaya Managed Service Offer	GA Date	5-1-2021
Avaya Source Prime		**Target Audience**	
Chris Peterson		Internal Document: Product Management, Order Management, Sales and Partners	

CHANGE CONTROL RECORD			
Date (mm/dd/yy)	**Issue/Version #**	**Prime**	**Summary of Changes**
05/1/2021	1.0	Chris Peterson	Initial Version
08/01/2021	1.1	Chris Peterson	Updates to Reference Terms
09/08/2021	1.2	Chris Peterson	Corrections to references and links
4/01/2022	2.0	Chris Peterson	Updates to billing start date and Service Transition for existing and net new customers.
11/11/22	3.0	Chris Peterson	Further clarification that Security Certificate Management is excluded form support coverage.
1/10/2023	4.0	Chris Peterson	Removed reference of OneCloud. Added support for R10.
3/20/2023	5.0	Chris Peterson	Expanded to include availability for both Perpetual and Subscription offers.
10/12/2023	6.0	Chris Peterson	Added Scorecards as a value add