Service Description (SD)

Avaya Aura® Private Cloud

Avaya Experience Platform® Private Cloud

Dated: June 12, 2026

www.avaya.com

TABLE OF CONTENTS

1 Introduction

1.1 General

This Service Description describes the Avaya Aura Private Cloud and Avaya Experience Platform Private Cloud (collectively referred to as "Service") that is available to the Customer to purchase. It supersedes all prior descriptions or contract supplements relating to such support and includes all its attachments, exhibits and appendices. Notwithstanding the foregoing, to the extent Customer purchases the Service via Microsoft Azure Marketplace the Avaya Aura Private Cloud and Avaya Experience Platform Private Cloud Service Description Addendum for Sales Transacted Through the Microsoft Azure Marketplace, found at https://support.avaya.com or such or a successor site as designated by Avaya, shall supersede this Service Description. When a translated version of this document conflicts with the English version, the English version will take precedence.

In this Service Description:

- "Agent or Agents", means any contact center personnel.
- "Agreement" as the context implies the Customer's direct agreement.
- "Order" refers to an Avaya order document.
- "Azure" refers to Microsoft Azure data center.
- "Basic Activation Services" means the Avaya-provided feature activation and testing services that is included in each of the Avaya Aura Private Cloud and Avaya Experience Platform Private Cloud Bundles.
- "Contract Term" means the total period of use of Service allowed by the Customer beginning on the Service Operation Start Date ending at the conclusion of the Initial Services Term as specified in the Order.
- "Customer" "You" or "Your" is the customer contracting the Service from Avaya. The Customer must have executed Cloud Terms as part of the Agreement with Avaya.
- "End User or End Users" means Customer's employees, agents, permitted contractors or any other users of the Avaya Aura Private Cloud and Avaya Experience Platform Private Cloud Service.
- "Initial Services Term" means the services period indicated in the Order.
- "Monthly Overage Service" means monthly service usage volume charges above the Minimum Annual Revenue Commitment documented on the Order Form.
- "Order Effective Date" means the date the Order was countersigned by the last Party ("Order Effective Date").
- "Party" refers to Avaya or Customer individually and "Parties" refers to both Avaya and the Customer.
- "Provisioned" means End Users configured for the Service.
- "Renewal Term" means subsequent 1-year periods after the Initial Term of the agreement.

- “Service” or “Cloud Service” is Avaya Aura Private Cloud and Avaya Experience Platform Private Cloud.
- “SD” means Service Description.
- “Standard System” pertains exclusively to the features and functionalities that are described in the Avaya Aura Private Cloud and Avaya Experience Platform Private Cloud Service Description.

Features or functionality that are not explicitly documented in this SD are not offered as part of the Standard System. Avaya obligations are as specifically stated in this document.

The Customer is responsible for ensuring that any use of the Service is compliant with all applicable local, state, national, foreign, and international laws, and regulations.

Enabling Avaya Aura Private Cloud and Avaya Experience Platform Private Cloud solution depends on Customer fulfilling their responsibilities as detailed in this SD. In addition, the Customer is responsible for the costs and expenses incurred by Customer to satisfy all its responsibilities under this SD.

If the Customer has not timely performed any of its express obligations under this SD, then until such time as Customer has fulfilled the said delayed obligations, Avaya may charge Customer for any additional activities performed and costs incurred by Avaya as a result of the delay or failure; and Avaya’s failure to perform any of its express obligations is excused to the extent caused by Customer’s failure or delay.

1.2 External links

While reasonable efforts have been made to ensure that the external links contained in this SD are accurate and up to date as at the date of publication, from time-to-time Avaya may change or designate successor web sites to post the content referred to in this SD without notice to Customer or a need to change this SD. Changes to external links will not result in additional costs to Customer or degradation in available features and functionality.

1.3 Terms, Acronyms and Phrases

Those terms, acronyms and phrases not defined in this document but in common usage in the information technology (“IT”) industry, telecommunications industry or other pertinent business context shall have their generally understood meanings in such industries or other applicable business context.

2 Cloud Services Overview

The table below summarizes the key service elements included in Avaya Aura Private Cloud and Avaya Experience Platform (AXP) Private Cloud service. In all deployments, the core application environment is dedicated to each customer.

Avaya Aura Private Cloud Services	
Basic User	1 device + Voicemail + Basic Activation Services
Core User	3 devices + Voicemail + User client + IM/Presence + MS Teams Client Side integration + Basic Activation Services

Power User	3 devices + Voicemail + User client + IM/Presence + MS Teams Client Side and Direct Routing integration + Basic Activation Services
AXP Private Cloud Services	
Voice Agent with Workplace Client[2]	• Built on top of UC Core bundle environment • Agent client (Workplace) • Basic Activation Services • Skills-based routing • Real-time and historical reporting with custom report capabilities • IVR Foundation (Includes IVR port entitlement up to 1 port to 2 agent ratio).[3]
AXP Private Cloud Add-on Services	
Callback	Callback Agent- first capability
Support for 3rd party Integrations and APIs	TSAPI based, TSAPI Advanced DMCC 3rd Party Call Control, Real-Time Agent State API
Verint Workforce Engagement Cloud for Avaya Experience Platform Private Cloud	Workforce management capabilities as optional add-on • Voice Recording • Screen Recording • Automated Quality Management • Workforce Management • Speech Analytics • Desktop and Process Analytics
CMS Connectors and ODBC	CMS connectors and ODBC as an optional add-on Real Time Connectors (Nice IEX Real Time, Generic Real Time Adherence, Verint Real Time, RT Socket) ● Historical Connectors (Nice IEX Historical, ECH, Verint Historical, Payroll, Unload, Aux logging) ● ODBC
Other Add-on Services	
911inform Location Discovery Solution (LDS)[4]	• Tracks both landline and wireless telephone when user dials 911 • Mandatory one-time setup fee is required. • Interactive mapping and Rapid SOS as optional add-ons.
e-Bond	• Integration solution to interface Avaya's incident system with Customer's ticketing system.
Workplace Attendant	• Designed for front-desk personnel who receive & transfer calls to the appropriate individual or group
Avaya Aura® X for Zoom Workplace	• Optional add-on to UC Core and UC Power Bundles. Avaya Aura enables Zoom Workplace to natively integrate with Avaya Aura as Advanced SIP Telephony (AST) client.
Data Center Services	
Primary Hosting Platform	Microsoft Azure
Infrastructure Services	Single-Tenant, Dedicated[5]
High Availability Design	Yes
Availability SLA	99.99% for UC - 99.99% for CC
Network Services	
Bring your own carrier – Transport options	ExpressRoute (Microsoft Peering) or Internet are Customer transport options. Transport to Azure Data Centers must be contracted separately by the Customer.
Cloud Services and Support	

Basic Activation Services	The Basic Activation Services include activation of purchased features, configuration and testing of five (5) test stations for UC and five (5) test agents for CC, and a recorded Customer walk-through of the Admin Portal interface.
Cloud Support Services	Cloud services for the platform including monitoring, software release management (minor and major), and ongoing management of the service are included as part of the standard rate card. Maintenance for 3rd party applications is priced separately.
Service Management	A Service Delivery Manager (SDM) and Client Service Executive (CSE) are included in the standard rate card.

[2] Standard allocation of supervisors (admin only): 1 Supervisor per 10 Agents. Supervisors are contact center users that only work with CC reports and perform administrative duties associated with the contact center but do not participate in live calls / sessions. Supervisors are not billed as Agents.

[3] The number of IVR ports required will depend on the specific Customer requirement.

[4] Required add-on for all United States UC users and CC Agents.

[5] Unified Desktop and Digital Channels CC capabilities are provided through a multitenant infrastructure. The primary hosting platform is Microsoft Azure, with additional services leveraged from Google Cloud and/or Amazon Web Services.

The Service consists of Azure data center hosting, installation, and ongoing management of the Service. As part of the Service, Avaya provides:

- The data center (DC) facilities where the Service is deployed are in accordance with the Avaya safeguards and security policies, see section 8 for further details or refer to please refer to Avaya Trust Center and Privacy Fact Sheet for Avaya Aura Private Cloud and Avaya Experience Platform Private Cloud.
- Dedicated for Customer's use of the Service on a shared infrastructure:
  - Infrastructure components include virtualization, compute, storage, network, and firewalls as necessary components to host Avaya Aura Private Cloud and AXP Private Cloud Solution.
- Avaya applications and associated implementation of the Service.
- Management and maintenance of the Service.
- Working with the Customer, Azure, and Customer carrier to discuss the termination of Customer provided circuits.
  - Customer is responsible for contracting circuits for client/terminal connectivity to the Azure data centers.
- Defined self-service administration to Customer Administrators and Customer End Users via the Avaya Admin Portal.
- Customer designated IT contact access to the Avaya OneCare Portal Capabilities include:
  - Access to real-time and dynamic operational dashboards including Cloud Dashboard, Service health and a map view of Critical and Major incidents with click through capability.
  - Access to the Avaya service desk to open new and view existing service request tickets, including MACD requests.

3 Customer Responsibilities and Service Exclusions

The Customer is solely responsible for contracting and providing all SIP inbound, outbound and/or network connectivity (including network security) required by the Avaya Aura Private Cloud and AXP Private Cloud

solution to provide the Service to Customer. Customer shall provide or contract directly with third party telecommunications service providers for all connectivity to and from End Users and callers.

3.1 Customer Responsibilities

- Provide Avaya with circuit details for all client/terminal connectivity to Avaya Aura Private Cloud and AXP Private Cloud.
- Customer firewalls that transport traffic are required between the Azure provided data center and Customer's network and need to be able to support the bandwidth generated by Avaya providing and End Users using the Service.
- If Home/Mobile Worker is operating over the internet, it is the Customer's responsibility to obtain suitable internet service for the worker.

3.2 Service Exclusions

- Support for Customer's IPV6 network.
- Non-E.164 dial plan configuration services are excluded, unless explicitly quoted as an additional service engagement.
- Network Readiness Assessment
- Development/migration of Customer custom applications.
- Individual IT Security assessments, audits, and customizations.
- All on-site work or work related to on-site deployed applications, devices or software, unless contracted separately.
- Off-board hosting for any non-Avaya application required to be connected via Avaya Aura Private Cloud API.
- End User instructor-led training.
- Use of country-specific resources for deployment (i.e., pre-Service Activation effort) and/or support of the instance is excluded, unless explicitly quoted as a separate premium service.

4 Avaya Aura Private Cloud Services

Avaya Aura Private Cloud service is comprised of three UC bundles.

- **Basic**: A typical type is a user in a common area (e.g., lobby or manufacturing floor). Analog phones, FAX machines, paging systems, etc. will require a Basic User type and a supported analog terminal adapter (ATA). ATA is not included in the Avaya Aura Private Cloud rate card and must be purchased separately by the Customer if needed.

- **Core**: This user type builds on top of Basic UC Bundle adding in Unified Communication capabilities such as User Client and Microsoft Teams client-side integration. Typically, this user type will address most desktop and mobile users in the Customer's organization.

- **Power**: This user type builds on top of the Core UC bundle adding Microsoft Teams direct routing.

The following table summarizes the features available with each bundle.

Package Key	Symbol
Included in Package / Bundle	●
Available as Priced Option	o
Not Available in Package / Bundle	-

Features	Basic User	Core User	Power User
Cloud UC and Call Management			
E.164 dial plan	●	●	●
Registered Devices	1	3	3
Dial by Extension	●	●	●
Call Forwarding	●	●	●
Call Park	●	●	●
Call Transfer	●	●	●
Multiple Call Appearance/Call Waiting (3 lines)	●	●	●
Incoming Caller ID	●	●	●
Music on Hold (up to 10 entries)	●	●	●
Ad hoc 6-party Audio Conferencing	●	●	●
Hunt Groups	●	●	●
Opus Codec	●	●	●
MS Teams Integration - Client Side	-	●	●
MS Teams Integration - Direct Routing	-	-	●
Device Enrollment Services	●	●	●
Call Detail Recording (CDR)	●	●	●
Voicemail			
Voicemail	●	●	●
Auto Attendant	●	●	●
Mobility Features			
Multiple Device Access	-	●	●
Avaya Workplace Client (Windows or Mac)	-	●	●
Avaya Workplace Mobile (IOS or Android)	-	●	●
Other Services			
911inform Location Discovery Solution (LDS)	o	o	o
E-Bond	o	o	o
Workplace Attendant	o	o	o
Avaya Aura® X for Zoom Workplace	-	o	o

Dial-in available in the following countries: US/CANADA (Toll-Free), US (Toll), ARGENTINA, ARGENTINA, AUSTRALIA, BELGIUM, BRAZIL, CHILE, COLOMBIA (Bogota), CYPRUS, CZECH REPUBLIC, DENMARK, DOMINICAN REPUBLIC, FRANCE, GERMANY, GREECE, HONG KONG, HUNGARY, INDIA (Toll-Free), IRELAND, ISRAEL, ITALY, JAPAN, LUXEMBOURG, MALAYSIA, MEXICO, NETHERLANDS, NEW ZEALAND, NORWAY, PANAMA, PERU, POLAND, ROMANIA, SINGAPORE, SLOVAKIA, SLOVENIA, SPAIN, SWEDEN, SWITZERLAND.

4.1 Microsoft Teams Integration

4.1.1 Client-Side Integration

MS Teams Client-side integration is included as part of UC Core and UC Power Bundles. Client-side integration makes use of the Avaya Call application available in the MS Teams application store. The Avaya Call app provides contact information and a dial pad within MS teams. Users can click to dial from MS Teams with this solution.

The following features are provided with the Avaya Calling for MS Teams:

- Make outgoing Avaya Audio and Video Calls from MS Teams.
- Answer call via Avaya Workplace client.
- See all your Avaya Aura Private Cloud directory and Office 365 contacts in one MS teams.
- Use the dial pad for calling global numbers and extensions.
- Mark contacts from Avaya Aura Private Cloud as Favorites for quick access.
- Call handling via Avaya Workplace client.

Customer Responsibilities

- Enable MS Teams.
- Configure Avaya accounts - accounts.avayacloud.com.
- Install the Avaya Call app.
- Set up the client.

Not Supported or Included

- Avaya Call app for iOS does not support marking Avaya Aura Private Cloud contacts as Favorites and Avaya Aura Private Cloud Directory search.
- Answer call via MS Teams is not supported.
- Call handling in MS teams is not supported.
- Dialing from Avaya call chat is not supported.

4.1.2 Direct Routing Integration

Avaya Session Border Controller for Enterprise (ASBCE) provides direct SIP and media connectivity between Avaya Aura Private Cloud voice infrastructure, the Public Switched Telephone Network (PSTN) SIP trunking services, and the customers Microsoft Teams environment. Direct routing is MS certified at UC integration level.

ASBCE Direct Routing capabilities allows direct calling between Avaya Aura Private Cloud Aura environment and MS Teams as well as allowing MS Teams users access to the Aura PSTN services:

- PSTN Trunk calls for MS Teams users handled through Avaya Aura Private Cloud.
- Avaya Aura Private Cloud users calling MS Teams users or vice versa.
- PSTN Trunk calls or Aura users calling another Aura user which is forked to MS Teams using EC500 or Coverage.

MS Teams direct routing integration is included as part of UC Power Bundles. Any Avaya Aura Private Cloud user who wants to be able to make or receive a call from a user on MS Teams will require one (1) power license.

Customer Responsibilities

- Customer must obtain the appropriate license from Microsoft to support Direct Routing.
- Customer must configure MS Teams to integrate with Avaya Aura Private Cloud Solution.

Not Supported or Included

- Multitenancy is not supported by the Avaya Aura Private Cloud environment.
- Integration with on-premises or 3rd party directory services is not supported.
- Integration with 911inform service for MS-Teams users is not supported.

4.2 Device Enrollment Services

Avaya Aura Private Cloud includes automatic provisioning for the supported Avaya devices operated by Device Enrollment Services (DES). The provisioning is managed by Avaya and doesn't require any level of access for the end customer/partner.

Customer may be required to perform different steps to enable this service depending on whether the supported devices are new or existing, as follows:

- For new devices, no further action is required.
- For migration of existing devices install base, the Customer is required to perform one of the following actions depending on the applicable scenario:
  - DES was not used before: Customer needs to reset the devices to factory defaults.
  - DES was used before, and Customer has their own DES account: existing devices already enrolled by DES require to be released from the DES account to be able to benefit from automated provisioning. Please refer to the Device Enrollment Services Overview found at https://documentation.avaya.com/ for instructions.

    Note: If the Customer requires Avaya to perform the release of devices from their DES account, a service request can be open and additional charges may apply. The Customer may be required to provide a list of serial numbers or a list of MAC addresses for the devices being released.

For additional details on DES supported devices, please refer to "Appendix A" below.

4.3 Call Detail Recording (CDR)

Call Detail Recording (CDR) feature is included as part of Avaya Aura Private Cloud and AXP Private Cloud Bundles, it is an optional entitlement available in Avaya Store. CDR is essential for many telecommunications service providers, call centers, and organizations that rely on telephone communications. They are used for various purposes, including billing, accounting, troubleshooting, network optimization, and compliance with regulatory requirements.

CDR enables customers to access detailed call information, including caller and recipient identities, call time, and duration. Avaya will push CDR to a customer provided SFTP server that supports TLS 1.2 or higher and

secure key authentication. Connectivity can be through internet or ExpressRoute (Microsoft Peering).

Not Supported or included

- Non-SFTP server are not supported, only SFTP is supported. Customer is responsible to provide the SFTP server.
- Communication Manager CDR TCP is not included.

Avaya Responsibility

- CDR data is produced and transmitted to the customer provider SFTP location.

Customer Responsibility

- Provide SFTP destination server.
- Security of the data store in the SFTP server.
- Responsible to monitor the SFTP server and record retention. Avaya will push the data and will not retain CDR data in the solution.
- Provide access and credentials.

4.4 Voicemail

- Personalized voicemail inbox with assigned extension to capture, play, and manage voice messages.
- Access and manage voicemail from desktop or mobile application (Core or Power UC only).
- Record multiple personal greeting messages for use cases like out of office or holiday hours.
- Auto Attendant allowing callers to a main number to be automatically transferred to an extension without the intervention of an operator.

4.4.1 Voicemail Features

- Multiple Language Prompts - G14 Language Set + Hebrew, Dutch, Arabic and Taiwan.
- User Preferences.
- Messaging Web Access.
- Personal and Extended Absence Greeting.
- System Greeting Before Call Answer (optional).
- Auto Attendant.
- Site-Level Broadcast Messages.
- Personal and Enhanced Distribution List.
- GDPR system announcement.
- Notify Me (Call / MWI) - Phone Call and MWI Notification included.
- Phone Call to a Telephone or Mobile Device – “Outcall'.
- Pending Deletion of Messages.
- Transfer to Voicemail.
- Consultative Transfer from Call Sender.
- Disable Default Avaya Branding / Record Your Own Greeting.
- Variable Length Mailboxes.
- E-mail notification includes a link to access voicemail delivery.
- Find Me/Follow Me services.

Not Supported or Included

- Migration of voice mails from legacy systems into Avaya Aura Private Cloud voice mail is not included in the Bundles. Optional professional services are available for a one-time additional fee and would require a separate custom Statement of Work (SOW).
- Transfer and 'fit' of pre-existing voice mail recordings.
- IMAP integration with Avaya Messaging is not supported.
- Integration to TTY devices is not supported.
- Use of Google Cloud or Customer's Exchange server for voice mail message store is not supported.
- Other email integration such as for Avaya Messaging notification services.
- Text, pager or read receipt notification services are not supported.
- Fax receiving and sending configurations for Avaya Messaging are not supported.

4.5 Instant Messaging and Presence

- Instant Messaging and Presence are deployed in a non-HA single server.
- Send and receive instant messages with individuals and groups, conduct ongoing conversations, and retain conversation history.
- Create IM chat rooms for use with internal and external users.
- Share and view presence of other users whether in the office or working remotely.
- Avaya Workplace IM and Presence Client for Android, iOS, Mac, Windows devices.
- Workplace Attendant presence.

4.6 Mobility Features

UC Core and UC Power bundles include the following features:

- **Avaya Client:** SIP-based unified communications client with real time collaboration capabilities that enable users and Agents to work from anywhere and manage their day-to-day communications from a single interface. Users outside the network can securely access voice services without establishing a VPN connection. Avaya Workplace is supported on Windows, Mac, Android and iOS.

- **Multiple Device Access:** a user can access calls on multiple devices of various capabilities but using the same extension. All devices of the user will ring for an incoming call, and the user can answer with the chosen device or a paired mobile device and switch seamlessly between mobile and desk phone during a single call.

4.7 911inform Location Discovery Solution (LDS)

Avaya provides enhanced 911 services compliant with current US legislature (Kari's Law and Ray Baum Act) from Third Party Service provider 911inform, LLC. The 911inform LDS is available in Canada and US for UC users and CC Agents. The user bundle is priced separately and is a required add-on to the standard Service. A mandatory one-time setup fee is required.
The service provides the following capabilities:

- Browser based application in support of alarm notification and end user location management.
- Automated system that manages and tracks 911 records for both wireline and wireless devices.

- Device is tracked by their MAC address.
- Eliminates need of DIDs that are being assigned for 911 reporting purposes.
- Records are updated in near real-time as soon as a user has confirmed and saved their location information.
- Can share DID across remote workers.
- 933 Test Calling.
- Text and Email notifications.
- 20 Emergency Call Relay Center calls per year.

4.7.1 Optional features

Optional features below are available for an incremental price:

- **Interactive Mapping:** Floorplans are interactive allowing emergency locations to be updated real time.
- **Rapid SOS**: With Rapid SOS coverage, floorplans can be delivered to the PSAP at the time of emergency call. This will provide exact location of the device from which the 911 call was made.

4.7.2 Phone Location Tracking

User´s phones can be tracked via two methodologies:

1. **MAC Addresses.** Each device is tracked by their MAC address and not telephone number, allowing each device to be uniquely identified. Whether it is at the office, at home or on the road, 911inform LDS treats location reporting the same.

2. **IP Endpoint Location Tracking (911inform LDS).** Irrespective of the physical location of the device, within a facility or external to it, when an IP device registration event occurs, 911inform solution will monitor the registration of the device. If the device registers to an IP address with a known dispatchable location, it will automatically update the associated device location record. If the IP range is unknown the 911inform solution then sends an SMS message, email and/or desktop alert (requires software client to be loaded) to the user's registered contact method, prompting the user to click on an enclosed link.

4.7.3 933 Test Calling

911inform LDS also includes 933 test calling. Rather than having to make a live 911 test call ending at the local PSAP and letting them know it is a test call, the Service can be configured so that dialing 933 routes to a PSAP simulator to test 911 calls. The PSAP Simulator reads back the phone number and address that would have been presented to the PSAP.

4.7.4 Text and E-mail Messaging Alerts

At the time of emergency, 911inform can generate 911 alert emails and text messages to be sent with the location of the 911 caller to security personnel. These can be sent to a distribution list provided by the Customer.

4.7.5 Emergency Call Rely Center (ECRC) calls

ECRC calls are calls for which the caller's address has not been successfully provisioned in the 911 service. The location may not be set for several reasons. It could be the End User intentionally circumvented the 911 service to not report location, an existing hard phone End User changed location and did not initiate a MACD to report the new location or it could be a new user where the location has not been established yet. With un-provisioned calls, the caller must be able to relay their address information successfully to the 911 Emergency Control Center (ECC) for the call to be successfully routed to the correct PSAP. The ECC member must stay on the line until the call is connected to the PSAP. When the call connects to the PSAP, the ECC member must relay the caller's address information and then remain on the call until the PSAP operator has successfully established contact with the caller and confirmed transfer of the call to their control. If the caller hangs up or is unable to speak to the ECC member, 911 service is not able to successfully connect the call to the correct PSAP and deliver the caller's address. 20 ECRC calls per year are included.

4.7.6 Avaya Responsibilities

- Avaya shall provide the underline infrastructure to implement 911inform solution.
- Provide necessary forms, templates and questionnaires strictly for gathering the data that will need to be included in 911inform.
- Training for 6 participants for up to 4hours

4.7.7 Customer Responsibilities

- Provide at least 2 End Customer extensions for testing.
- Provide name of individual that the endpoint is assigned to, extension number, cellular phone number and/or email based on preferred contact method for updating location.
- Determine who will receive the alerts for 911 calls.
- Provide at least 1 DID per physical address.
- Initial provisioning of endpoint locations.
- Configuration of firewall rules for outbound connection if required (both LDS and connected building)
- Provide Network Diagram, if available.
- Installation, configuration, and testing of personal computers to meet the specifications provided by Avaya.
- Have thorough understanding of business requirements and technical environment.
- Verify and complete the necessary forms and questionnaires provided by Avaya.
- Provide IP Ranges and associated zones for database preparation.
- Support local testing at minimum three (if applicable) locations.
- Develop and perform detailed acceptance testing (e.g. User Acceptance Testing (UAT). Testing must include a minimum of two extensions using the 933 dial out to determine correct location information. Testing must also include a 911 call to ensure the correct call path to the relevant PSAP.

4.7.8 Service Exclusions

The following are exclusions and not provided with the Service:

- Local Survivability - should the End Customer's broadband connection, PSTN service, or electrical power fails or is suspended or interrupted, or any other issue interrupts Customer's network or geolocation service, the 911 service shall also fail. Avaya is not liable for any claims arising from such failures.

- 508 VPAT currently not available

4.7.9 Use of Emergency Services in the US Disclaimer

If the Customer does not configure an emergency response location for a US-based End User with 911inform LDS which is incorporated into Avaya Aura Private Cloud and AXP Private Cloud, a 911 call may default to a wrong customer's address or remain unregistered. Moreover, if the Customer's broadband connection, PSTN service, or electrical power fails or is temporarily suspended or interrupted, or any other issue interrupts Customer's network or geolocation service, the Service (including emergency calls) shall also fail. Avaya is not responsible or liable for any issues or claims arising from such failures.

4.7.10 Use of Emergency Services Outside of the US Disclaimer

Avaya Aura Private Cloud and AXP Private Cloud does not include emergency calling (e.g., 112) location services. Emergency Services calls are sent to the outbound SIP trunk group by the Service. The Customer is responsible for handing all emergency call processing and routing to the appropriate Public Service Answering Point (PSAP) emergency response location for End Users. If the Customer does not configure an emergency response location, it may default to the wrong customer's address or remain unregistered. Moreover, if customer's broadband connection, PSTN service, or electrical power fails or is temporarily suspended or interrupted, or any other issue interrupts customer's network or geolocation service, the Service (including emergency calls) will also fail. Avaya is not responsible or liable for any issues or claims arising from such failures.

4.8 E-Bond

The standard e-bond option is available for an incremental one time and monthly recurring price. This is accomplished via a e-Bond RESTful API specification that Avaya provides, and the Customer consumes. It provides an integration solution to interface Avaya's incident system with the Customer's ticketing system. E-bond provides a seamless exchange of the following information between the Avaya and the Customer.

- Incident record exchange
- Service Requests (e.g., MACDs) exchange

The standard e-Bond exchange is over the public internet secured through firewalls.

4.8.1 Avaya Responsibilities

- Provide e-Bond RESTful API specification that Customer consumes to submit new or update requests to Avaya.
- Provide support and testing as Customer establishes the consumption of the e-Bond RESTful API. Avaya will provide resources for user acceptance testing (UAT) test script creation and testing.
- Provide attribute and attribute value/data mapping consultation.
- Make the required configuration changes on the equipment that Avaya hosts.
- Provide configuration parameters in advance of the scheduled turn-up date/time.
- Log all e-Bond solution transactions within Avaya's incident system to assist in resolving connectivity errors or error scenarios.

- Work with Customer to troubleshoot, diagnose and fix issues with the e-Bond solution that are identified during the integration testing and/or implementation phase.
- Keep Customer abreast of any changes that could impact the functioning of the e-Bond to avoid outages or when new capability is introduced.

4.8.2 Customer Responsibilities

- Identify connectivity method - Internet (standard).
- Provide appropriate resources to support the development, testing, implementation and use of the e-Bond solution, including User Acceptance Testing (UAT) test script creation and testing.
- Publish e-Bond API specifications that Avaya consumes to inform Customer or update requests that Avaya is working on (within a defined set of Avaya supported capabilities).
- Consume e-Bond RESTful API published by Avaya.
- Support all inbound/outbound attribute and attribute value translations or transformations. Examples: Status/Status reasons, priorities, providing value to mandatory fields on customer side that may not be mandatory on Avaya side.
- Make the required configuration changes on the equipment located on the Customer's premises.
- Provide configuration parameters in advance of the scheduled turn-up date/time.
- Log all transactions within its system to assist in identifying issues when performing debugging activities.
- Work with Avaya to troubleshoot, diagnose and fix issues with the e-Bond solution that are identified during the integration testing and/or implementation phase.
- Keep Avaya abreast of upcoming changes to the e-Bond resulting from Avaya continuous improvements, changes on Avaya incident system affecting the Customer e-Bond on completion of implementation of e-Bond. This will ensure the e-Bond is functionally intact and change management is controlled.
- Support joint Avaya and Customer Testing.
- If there is any development work, it is the responsibility of the Customer to create that in their platform.

4.9 Workplace Attendant

Workplace Attendant is a separately priced add-on for Avaya Aura Private Cloud Bundles. Workplace Attendant client is a Windows-based user interface designed to meet the communications requirements of front-desk personnel and call receptionists whose responsibility includes receiving calls, often in large volumes, and routinely transferring the calls to the appropriate group or individual. Avaya Aura Private Cloud supports up to 25 Workplace Attendant clients.

The service provides the following capabilities:

- Accept incoming calls.
- Hold and retrieve calls.
- Mute calls.
- Make outgoing calls and terminate incoming calls.
- Control volume of audio in calls.
- Cherry pick calls from queue.

- Attendant recall.
- Call transfer.
- Ad-hoc conference.
- Rich presence.
- Conference.
- Night Service.
- Park on Busy.
- Statis Reporting.

4.9.1 Avaya Responsibilities

- Configure the ordered number attendants.

4.9.2 Customer Responsibilities

- Provide, upgrade and re-register existing hard and/or soft end points.
- Configure local setting options provided via the client.

4.9.3 Service Exclusions

- Database connection to external Databases for contacts

4.10 Avaya Aura X for Zoom Workplace

Avaya Aura X for Zoom Workplace is an optional add-on bundle to the UC Core and UC Power Bundles. It enables Zoom Workplace to natively integrate with Avaya Aura as Advanced SIP Telephony (AST) client. The Avaya Aura X for Zoom Workplace delivers:

- A single client to access Avaya Aura UC telephony and Zoom Collaboration.
- Native integration of Zoom Workplace client to Avaya Aura in cloud or on premises.
- Elevation of Voice UC experience to Zoom meeting in one click.

The following features are supported:

- Single Sign-On.
- Streamlined sign-on and automatic user provisioning.
- Multiple Call Appearances (Maximum two concurrent calls).
- Call hold, call transfer, ad-hoc conference (conference is limited to 3).
- Calling name/number (basic, Stir/Shaken).
- Centralized call history (call logs).
- Basic codec support (G.711, G.729, G.722, Opus).
- DTMF button signaling.
- Outlook Calendar Integration.
- Directory / Contacts Integration.
- Key language feature displays (Spanish, French, English, G11).
- Multiple Device Access: customer can register to an Avaya Aura phone number using several devices or clients at the same time. If you get a call, all devices or clients ring. When customer answers

using one, the others stop ringing. Customer can hand off a call from a Zoom client to an Avaya client.

- Message Waiting Lamp updates (on/off).
- Single-button access to voice mail.
- Elevate ad-hoc Aura audio conference to Zoom meeting (video, screen sharing).
- Call forwarding via DTMF.
- Music on hold.
- 911 emergency call location identification.
- Call coverage (to other local/remote users, groups of users, and/or voice mail).
- Call Detail Recording.
- UC hunt groups.
- EC500 (always enabled).
- Announcements.
- Authorization codes.
- Automatic Route Selection (ARS).
- Class of Service.
- Meet-me Conferencing.
- Night Service.
- Priority Calling.
- VIP Calling.

Avaya Responsibilities

- Create client-ID mapping.
- Push notifications enablement – generate key set and provide it to customer.
- Firewall changes to allow access Zoom OIDC discovery URL.
- Certificates to allow secure TLS connection to Zoom Push notification.

Customer Responsibilities

Zoom Prerequisites:

- Zoom Workplace bundle.
- Account owner or admin role for managing users and Phone System integration.
- Zoom Workplace app version 6.2.0 or higher.
- Add AADS domain in Zoom account.
- Add SM key set to Zoom account.

For additional details, please refer to the Application Notes.

5 Avaya Experience Platform Private Cloud Services

The Voice Agent Bundle is the baseline bundle for adding Contact Center functionality to AXP Private Cloud offer. The Voice Agent bundle supports configurable, conditional voice call routing commands (Call Vectors), agent selection algorithms, and call handling features. Call routing is skills-based.

AXP Private Cloud provides the following client options, available in Voice Agent bundle:

- **CC Voice Agent Bundle with Workplace Client:** Introduces call control and media using Avaya Workplace Client.

The following table summarizes the features and optional add-ons available with Voice Agent Bundle.

Features	Voice w/ Workplace
ACD with Intelligent skills-based routing and queuing	●
Voice Contact Center Reporting	●
Agent Client (Workplace)	●
IVR Foundation[1]	●
CRM integration with Salesforce, Microsoft Dynamics 365 and ServiceNow	-
Agent desktop through VDI (Citrix)	-
Callback Agent-first	o
TSAPI Basic	o
TSAPI Advanced	o
DMCC 3rd party call control	o
Real-Time Agent State API	o
Verint Workforce Engagement Cloud for AXP Private Cloud[2]	o
CMS connectors and ODBC	o

Package Key	Symbol
Included in Package / Bundle	•
Available as Priced Option	o
Not Available in Package / Bundle	-

[1] Includes IVR port entitlement up to 1 port to 2 Agent ratio. The number of IVR ports required will depend on the specific Customer requirement.

[2] Completed interviews are purchased in annual quantities. Available in North America, CALA, APAC (Philippines and India) only and supports English and Spanish languages.

5.1 Voice Contact Center Reporting

As part of the Voice Agent Bundles, Avaya provides Voice Contact Center reporting via Call Management System (CMS), supporting standard real time and historical reports, as well as the ability for call center supervisors to create custom reports using the CMS Supervisor web client. Th CMS web-based reporting tool is provided out-of-the-box, enabling customers to access all CMS reports directly from a web browser. For more details on available reports, please refer to Avaya CMS Supervisor Reports at https://support.avaya.com

5.2 IVR Foundation

Interactive Voice Response (IVR) capabilities are available in AXP Private Cloud. IVR provides the foundation platform for self-service experience and interactions that may be better handled by an automated system. It is based on web services and web communications standards like VoiceXML to allow lower cost, and simpler integration with Customer´s existing web and enterprise application environment.

The Voice Agent Bundle includes IVR entitlement (up to 1 port to 2 agent ratio). The number of IVR ports required will depend on the specific Customer requirement.

Provision of application servers within the AXP Private Cloud environment is not supported.

5.2.1 Supported IVR Integrations

This section describes the supported integration from Customer's existing inbound applications (custom-developed or 3rd Party VXML compatible service) to AXP Private Cloud IVR.

While AXP Private Cloud will host the IVR foundational platform, Customer provided application servers will be hosted on customer's premises or Customer/partner's cloud, outside of AXP Private Cloud environment, and will be made available to the IVR foundation platform as an external HTTPS based connection. An IVR foundation platform administration web-based interface will allow reporting and port assignment capabilities.

AXP Private Cloud offer only includes hosting the IVR foundation platform. Any required modification of custom-developed applications and/or functionality changes for integration with AXP Private Cloud are Customer´s responsibility. Customer is responsible for applications, application servers and link to AXP Private Cloud core and Avaya will not be responsible for outages caused by issues on these elements and these would not be part of the SLA.

An evaluation from the Cloud Sales Architecture team during Pre-sales will be required to assess the compatibility of Customer inbound IVR applications and ensure all technical requirements are met.

Optional professional services are available for a fee to assist Customer with evaluation and planning of IVR integration and call flow modifications of existing application(s) as required. These optional services will be documented in a separate custom SOW.

Not supported or included

- Provision of application servers within the AXP Private Cloud environment is not supported.
- Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) are not supported.
- Call flow migration is not included.
- Outbound Applications are not supported.

5.3 Callback Agent-First

Callback capabilities are available in AXP Private Cloud as an optional add-on to the Voice Agent Bundle. AXP Private Cloud currently supports SIP Agent-First strategy only. Customer administration web-based interface allows:

- Callback configuration management
- Daily summary report
- Pending callbacks report
- Pending callbacks summary report
- Call disposition summary report
- Hourly summary report
- Access dashboard as viewer

The number of ports required will depend on the specific Customer requirement.

Not supported or included

- Customer First strategy is not supported.
- Web Callback is not supported.
- External Orchestration Designer Applications are not supported.
- Avaya Business Rules Engine integration is not supported.
- Customer administration web-based interface doesn´t support:
  - License management
  - Role management
  - Site definitions
  - LOB configurations
  - User management
  - Global setting management
  - CCM API

Configuration and personalization of the Callback feature is available from Avaya for a one-time fee and will be documented in a separate custom SOW.

5.4 Supported of Third-party Interfaces

The following sections describes integration options from a customer premises or cloud third party systems into Avaya AXP Private Cloud.

5.4.1 CTI Applications

AXP Private Cloud provides the capability to allow inbound CTI connections for Customer-owned CTI applications (on-premises or cloud). Supported interfaces are available as optional add-ons to the Voice

Agent Bundle.

Any required modification of Customer-owned applications and/or functionality changes for integration with AXP Private Cloud are Customer´s responsibility.

- **Telephony Services API (TSAPI**): provides a full complement of third-party call control capabilities, such as controlling specific calls or stations, completing routing of incoming calls, receiving notifications of events, invoking Communication Manager features, and querying Communication Manager for information. This link can also be used to pull metric data that a Business Intelligence (BI) application can use. TSAPI provides 3rd party call control services for which two types are offered:

    - **TSAPI Basic** is intended for applications that monitor or control a station.

    - **TSAPI Advanced** is required for advanced call control supporting applications that launch or route calls.

- **Device, Media, and Call Control (DMCC):** provides third-party call control. The DMCC SDK provides a Java API as well as XML and .NET interfaces.

    - **DMCC third-party call control (3PCC):** DMCC with call control services uses the TSAPI service to provide an expanded set of third-party call control capabilities, such as the ability to place calls, create conference calls, deflect calls, reconnect calls, and monitor call control events.

    DMCC media is not supported.

- **Real-Time Agent State API**: provides event feed for real time Agent events such as “Ready” (Auto-in, Manual -in); “Not Ready” (Aux), “Work Not ready” (ACW) and “Pending Work Mode”. Customers can leverage this real time information for use cases like accurate business decisions, custom/AI apps, and various 3rd party CX integrations for existing and cloud services. These 3rd party applications can now receive the Agent state change feed as published events making it real-time.

    To enable this capability, the integration partner (CTI App Developer) needs to engage with Avaya to get the SDK.

5.4.2 CMS Connectors and ODBC

The CMS data is consumed by Avaya solutions, customer-created applications, and third-party systems for a wide variety of purposes, including workforce management, agent adherence, scheduling, forecasting, reporting, analytics, payroll, etc.

Real-time and historical CMS data are readily available to end users via native CMS reporting tools. When other systems, databases or applications need that same data, AXP Private offers access to the data by way of CMS interfaces or connectors. The connection on the interface is referred to as a session which is the connection between CMS and the external destination. Think of a session as a "point-to-point" connection.

CMS connector connectivity can be over Public Internet or ExpressRoute (Microsoft Peering) based on customer´s requirements.
CMS ODBC connectivity will only be offered over an ExpressRoute (Microsoft Peering) connection from Customer network to AXP Private Cloud.

Supported CMS connectors and ODBC are separately priced add-on to the AXP Private Cloud Bundles. Professional Services are mandatory for personalization of the CMS connectors and ODBC. These services will be provided for an additional fee to the Customer and will be documented in a separate SOW.

Real Time	Nice IEX Real Time Generic RT Adherence Verint Real time RT Socket
Historical	Nice IEX Historical ECH Verint Historical Payroll Unload Aux logging
ODBC	

For additional details please refer to the CMS Connectors Overview at https://support.avaya.com.

5.4.3 Security Requirements and Considerations

These are general capabilities supported by AXP Private Cloud CMS connectors, ODBC, and APIs:

- TLS 1.2 (TLS 1.3 where supported) for API integrations, CMS connectors and ODBC unless otherwise stated.
- For some CMS historical connectors only SFTP is supported, customer is responsible to provide SFTP server.
- Industry best practice secure cipher suites supporting Perfect Forward Secrecy (PFS)
  - New connection throttling based on source IP.
  - HTTP URL validation – protection against malformed URLs – malformed URLs are discarded.
  - HTTP header validation – incoming packets are inspected for valid header and invalid headers are discarded.
- Whitelisting and Blacklisting based on:
  - Source IP or subnet.
- Access to APIs can limited to specific IPs or subnets.
- Web API Whitelisting - Access to APIs can be limited based on:
  - Allowed URL paths.
  - Allowed URL parameters.
- Access to the API must meet configured path and parameter rules to be granted access to the API.
- Web API - authorization decision.

    - API access is authenticated by AXP Private Cloud.
- Other options available for AXP Private Cloud:
    - Bandwidth throttling options on individual connections or services, if required, on both ingress and egress from AXP Private Cloud.

5.4.4 Not supported or included

- Avaya does not supply IaaS space as well as connectivity to AXP Private Cloud for any 3rd party application.
- Non-secure protocols are not supported.
- SMS Service, Telephony Web Service, CVLAN and DLG are not supported.
- DMCC media is not supported.

5.5 Verint Workforce Engagement Cloud for Avaya Experience Platform Private Cloud

The Verint Workforce Engagement Cloud for Avaya Experience Platform Private Cloud is a separately priced Third-Party Service add-on to AXP Private Cloud. This offer, sold by Avaya, is a solution that leverages the latest Verint Workforce Engagement release as a primary component in this public cloud-based offer. It is an integrated public cloud-based solution that enables the contact center and customer to achieve corporate objectives.

Features include but are not limited to[1] :

- Voice Recording
- Screen Recording
- Quality Management
- Automated Quality Management
- Automated Quality Management Transcription
- Speech Analytics
- Speech Analytics Additional Line of Business
- Speech Analytics Additional Language
- Real Time Agent Assist
- Workforce Management
- Operations Visualizer
- Desktop and Process Analytics
- Application Triggers
- Application Visualizer
- Capture Verification
- Da Vinci Speech Transcription
- Da Vinci Summary
- Da Vinci Redaction
- Interaction Export with Processing
- Cloud Storage - 1TB
- Intelligent Interviewing[2]

[1] Verint capabilities are governed by the Verint Workforce Engagement cloud Service Description.
[2] Completed interviews are purchased in annual quantities. Available in North America, CALA, APAC (Philippines and India) only and supports English and Spanish languages.

Please refer to Verint Workforce Engagement Cloud for Avaya Experience Platform Private Cloud Description for complete services details.

In the event that the Customer fails to fulfill any of its obligations under this Service Description within the designated timeframe, Avaya reserves the right to charge the Customer for any additional activities undertaken and costs incurred due to such delay or failure. Furthermore, Avaya's inability to fulfill its obligations in providing the service is excused to the extent that such failure is caused by the Customer's delay.

6 Basic Activation Services

The Basic Activation Services include activation and testing of purchased features, configuration and testing of five (5) test stations/agents for UC and/or CC, as applicable for the bundle purchased.

At the completion of the Basic Activation service, the Avaya Aura Private Cloud and AXP Private Cloud Solution is ready for production use by the Customer and the billing Ramp Period shall begin. Administration of stations, agents, and personalization of features Admin Portal by Customer, via Monthly MACD entitlements, by Partner or by Avaya for an additional fee.

The table below summarizes the Basic Activation Services that are included with the Avaya Aura Private Cloud and AXP Private Cloud Bundles. Avaya will provide the services described below at no charge to the Customer.

Additional professional services are available from Avaya for a fee and will be documented in an Avaya Statement of Work (SOW), delivered under a separate project, and will commence once the Basic Activation services are completed.

Basic Activation Services Deliverables	UC Basic	UC Core	UC Power	CC Voice w/ Workplace
Unified Communications (UC)				
Configure up to five (5) test stations with five (5) corresponding test mailboxes.	●	●	●	●
Configure of Direct Inward Dial (DID) for testing purposes.	●	●	●	●
Configure and test one (1) test VDN (Vector Directory Number).	●	●	●	●
Configure and test one (1) test vector for auto-attendant.	●	●	●	●
Configure and test one (1) test hunt group.	●	●	●	●
Configure up to one (1) SIP trunk integration (Tie trunk from customer´s premises or carrier).	●	●	●	●
Activation of Avaya Workplace Client (Windows or Mac)	-	●	●	●

Activation of Avaya Workplace Mobile (IOS or Android)	-	•	•	•
Provide recorded walk-through session for demonstration on how to configure UC functionality.	•	•	•	•
Contact Center (CC)				
Configure up to five (5) test voice call center agents, and one (1) test supervisor.	-	-	-	•
Configuration of (1) sample call flow and one (1) sample CC report.	-	-	-	•
Configuration of (1) test CC vector with Time-of-Day routing for ACD (Automated Call Distribution) queuing.	-	-	-	•
Configuration of (1) test CC announcement.	-	-	-	•
Test login/logout/aux work, After Call Work (ACW), call transfer within Avaya agent client.	-		-	•
Provide recorded walk-through session for demonstration on how to configure CC functionality.	-	-	-	•
Configuration of supported CRMs only.	-	-	-	-

Package Key	Symbol
Included in Package / Bundle	•
Not Available in Package / Bundle	-

6.1.1 Basic Activation Services Exclusions

Any work not described as a deliverable under Basic Activation Services section of this document is out of scope and may be available from Avaya via optional fee-based offers. Exclusions include but are not limited to the following:

- Network Readiness Assessment
- Personalization and customized professional services.
- Installation of telephone sets, conference room phones, ATAs and fax.
- Lift and shift of existing on-premises based programming.
- Dial plan changes made from the base dial plan configuration provided with the solution will need to have an ACES engagement to evaluate and implement. This includes a multinational dial plan setup if a gateway or users are in a different region to the core and require different dialing for things such as emergency calling.
- Non-E-164 dial plan changes.
- Failover testing of any other application integrated outside of the solution implemented by Avaya.
- Configuration changes or add-on´s to Customer´s premise-based systems.
- Performance/Load testing.
- User deployment of Avaya Workplace Client or Avaya Workplace Mobile.
- Deployment of interfaces, connectors, or output to other solutions.
- Third party integrations and/or certificate installation.
- Custom report or CC dataset development and/or migration.
- Migration of existing IVR workflows, or virtual assistants. Development of new self-service, pre-route, or AI-based call flows.
- Transfer and ‘fit’ of pre-existing reports (i.e., CMS reports).
- Export of contact center reporting data to a Customer business intelligence tool.

- CRM Integration:
    - User-To-User Information (UUI) for screen pop purposes.
    - Modification or changes to Customer's CRM systems.

Note: Use of country-specific resources for deployment (i.e., pre-Service Activation effort) and/or support of the instance must be quoted as a separate premium service

6.1.2 Basic Activation Services for Cloud Migration Tool

Basic Activation Services for Cloud Migration Tool are included with Cloud Migration Tool optional entitlement. Avaya will provide the services described below at no charge to the Customer.

- Deployment of the migration tool.
- Adding Migration engineer role for Admin portal suite and enabling a customer contact.
- Setup connectors and establish connectivity between AXP Private and Aura system on prem.
- Establish SIP trunk and routing requirements.
- Setup required nightly jobs to perform systems synchronization.

Customer Responsibilities:

- Work with Avaya to allow connectivity from Cloud Migration Tool to Aura system on prem (open ports, provide required information like FQDNs, ports, etc.).
- Acquire internal security approval in advance for all network modifications.

7 Network Services

7.1 Transport

Customer is responsible for bringing their own carrier for interconnection to Avaya Aura Private Cloud and AXP Private Cloud. The Customer is solely responsible for contracting and providing all SIP inbound, outbound and/or network connectivity (including network security) required by the Avaya Aura Private Cloud and AXP Private Cloud solution to provide the Service to Customer. Customer shall provide or contract directly with third party telecommunications service providers for all connectivity to and from End Users/callers.

Avaya Aura Private Cloud and AXP Private Cloud supports two types of Customer and carrier connectivity models: public (over the internet) and private (using Azure ExpressRoute (Microsoft Peering)).

- **Internet Model:** is the quickest method to consume the Service. This is the standard connectivity model and is available out of the box. All external services are exposed via Azure Application Gateways and Load Balancers, with appropriate access control policies to ensure high quality service. This connectivity model requires minimal Customer network work aside from possible whitelisting of service endpoints.

- **ExpressRoute (Microsoft Peering) Model:** private connectivity model requires more time and Customer responsibility to deploy and configure. The Customer is responsible for establishing the ExpressRoute (Microsoft Peering) circuit, including all associated networking to support the

Customer network environment. Furthermore, in the case of carrier (PSTN) termination, the customer would work with their carrier to ensure delivery of the PSTN service to the Azure cloud. The Service include working with the Customer to establish the network attachment to the Azure Network. This model typically requires a longer lead time which should be factored into any service delivery commitment.

Avaya Aura Private Cloud and AXP Private Cloud can pass call verification status (STIR/SHAKEN) to Avaya Workplace Client and J1XX handset endpoints when provided through the SIP trunk (Carrier or Tie trunk). This feature enables the user to view the verification status of incoming calls on the display. Customer contracted PSTN service must provide the information for it to display. Avaya Aura Private Cloud and AXP Private Cloud will not block any calls based on status. This feature can be activated during the personalization process and must be requested if required.
Currently, associated WFM integrations do not support this feature.

7.1.1 Not Supported or Included

- Avaya SIP Trunk is not supported.

7.1.2 Avaya responsibilities:

- Configure up to one (1) SIP trunk integration (Tie trunk from customer´s premises or carrier)
- Work with the Customer, Azure, and/or Customer carrier to discuss the termination of Customer provided circuits.

7.1.3 Customer responsibilities:

- Contract carrier for all network connectivity to Avaya Aura Private Cloud and AXP Private Cloud. Third party telecommunications service providers and on-premises SBCs must be certified.
- Work with the Avaya, Azure, and/or selected carrier to discuss the termination of Customer provided circuits.
- Provide circuit details for client/terminal connectivity to Avaya Aura Private Cloud and AXP Private Cloud:
    - Option selected (e.g., Internet, ExpressRoute)
    - Carrier(s) selected.
    - Number of circuits.
    - Size of circuits.
    - Networking protocol.
    - Implementation timeline associated with circuit termination.
    - Provide the necessary information for testing all connectivity to Avaya Aura Private Cloud and AXP Private Cloud; testing must be conducted prior to onboarding users to the system.
- Customer firewalls that transport traffic are required between the Azure provided data center and Customer's network and need to be able to support the bandwidth generated by Avaya providing and End Users using the Service.
- If Home/Mobile Worker is operating over the internet, it is the Customer's responsibility to provide suitable internet service for the worker.
- For any other 3rd party services (e.g. 911 services) not included in the offer, a

certification/validation approval is required, and all connectivity charges are customer responsibility.

7.2 Network Readiness

While circuit sizing requirements may differ between the data center and branch locations, accurate network and link sizing is crucial for efficient traffic support. To ensure quality and successful support of the IP enabled Service, the Customer must provide a network diagram that captures all links and traffic flows. All network traffic to and from the Avaya Aura Private Cloud /AXP Private Cloud instance is the customer responsibility. Avaya SLAs are not tied to, and Avaya shall not be liable for, any deficiencies in connections provided by customer. Avaya will assist in determining the appropriate codec calculations by providing the necessary codec and data information for network bandwidth calculations.

Network Readiness Assessment (NRA) services are available for an additional fee to the Customer from ACES professional services and will be included in a custom quote and SOW from the ACES team.

The table below outlines the minimum network requirements for Avaya Aura Private Cloud and AXP Private Cloud.

Metric	Acceptable	Recommend
One Way Network Delay	< 180 milliseconds	< 80 milliseconds
Network Jitter	< 20 milliseconds	< 10 milliseconds
Network Packet Loss (Voice)	< 3.0%	< 1.0%
Network Packet Loss (Video)	< 0.2%	< 0.1%

If Avaya determines that Customer's network does not comply with any Network Requirement then, until such time as all Network Requirements have been met and compliance evidence provided to Avaya in accordance with the Network Readiness Policy, Avaya will aim to continue to provide the Service subject to the following limitations and exclusions:

- In certain cases, Avaya may not be able to restore Normal Service Operation or resolve functionality issues until such time as Customer has upgraded, reconfigured, or otherwise ensured that its network infrastructure complies with the Network Requirements. Normal Service Operation is when the Service and/or functionality provided by and AXP Private Cloud solution is not impacted by an Incident.
- Service Levels and associated Service Level Credits as detailed in Section 11.5 are not included.

8 Security and Compliance

8.1 HIPAA Compliance

Unless agreed upon in writing by the Parties and accompanied by an appropriate Business Associate Agreement, and stated in the Avaya Aura Private Cloud and AXP Private Cloud Order, Customer agrees that it will not introduce Protected Health Information (as defined in HIPAA, PHI) into the 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 Service with PHI.

8.2 PCI Compliance

Unless specified in the Avaya Aura Private Cloud and AXP Private Cloud Order, the Service is not compliant with the Payment Card Industry Data Security Standard also referred to as PCI or "PCI DSS".

If Customer´s Avaya Aura Private Cloud and AXP Private Cloud Order specifies PCI DSS compliance then during the Service Term, Avaya shall maintain Payment Card Industry Data Security Standards ("PCI DSS") compliance for the Service. Upon request Avaya will submit an Attestation of Compliance ("AOC"), which is evidence of a successfully completed PCI DSS assessment. Customer is responsible for ensuring that its use of the Service to store or process credit card data complies with applicable PCI DSS requirements. Any Customer use that includes Customer (or Avaya, at Customer's instruction) deployment of any other service or functionality (including Avaya add-ons) in Customer's instance may affect the Service's PCI DSS compliance, and Customer is solely responsible for ensuring that any such deployment meets Customer's compliance and security requirements.

8.3 ISO Standards

AXP Private Cloud and Avaya Aura® Private Cloud Microsoft Azure installations comply with the following standards:

- ISO 27001:2022
  - To establish, implement, maintain, and continuously improve the Information Security Management System (ISMS).
- ISO 27017:2015
  - To provide information security controls based on ISO/IEC 27002, designed for cloud services.
- ISO 27018:2019
  - To protect Personally Identifiable Information (PII) in public clouds where the cloud service provider acts as a PII processor.

Note: The Business Continuity practices of Avaya align with ISO 22301 requirements.

8.4 Safeguards and Security Policies

Avaya will perform the Service in accordance with the Avaya safeguards and security policies and procedures.

Avaya will follow its regular procedures and processes to prevent viruses from being introduced by Avaya into the Avaya Aura Private Cloud and AXP Private Cloud solution, Customer's network or information systems connected to or integrated with the Avaya Aura Private Cloud and AXP Private Cloud solution during the performance of the Service.

Notwithstanding the foregoing, Customer acknowledges that Customer is responsible for its portion of the privacy and security inside the Service and that Customer will establish and, throughout the Term in the Avaya Aura Private Cloud and AXP Private Cloud Order, maintain the policies, processes, and controls that prevent introduction of viruses into the Avaya Aura Private Cloud and AXP Private Cloud solution or unauthorized access, disclosure, alteration or destruction of Customer data and/or data used by Avaya in the performance of the Service through actions of End Users and Customer in how the Service is used.

8.5 Password Management

Avaya will change system level passwords for the Avaya Aura Private Cloud and AXP Private solution on a recurring basis in accordance with the Avaya safeguards and security policies. Avaya will retain ownership and full control of all passwords to any Avaya-owned equipment and will not provide such passwords to Customer.

8.6 Customer Data

Customer data will always remain the property of Customer. Upon termination or expiry of the Avaya Aura Private Cloud and AXP Private Cloud Order Term, Avaya will delete any Customer data stored on any Avaya Aura Private Cloud and AXP Private Cloud solution, Avaya systems or other devices or media in accordance with Avaya safeguards and security policies and procedures.

Alternatively, if so, requested in writing by Customer, Avaya will retain specific Customer data for a period of time using reasonable commercial efforts to meet Customer's request but, unless the Parties expressly agree otherwise in writing, Avaya is not in any way obligated to store Customer data following termination or expiry of the Term. In the absence of such Agreement in writing, Avaya reserves the right to delete Customer data within reasonable time frames following termination or expiry of the Avaya Aura Private Cloud and AXP Private Cloud Order Initial Term or Renewal. Avaya deleting, or not deleting, Customer data will always be subject to local law.

For the avoidance of doubt, Customer can access and retrieve Customer data which may contain personal data, such as call recordings, at any time before the termination or expiry of the Avaya Aura Private Cloud and AXP Private Cloud Order Initial Term or Renewal and for a period of fifteen (15) days after such termination or expiration.

Additionally, if Customer requires Avaya to securely destroy any Customer data stored on the Avaya Aura Private Cloud and AXP Private Cloud solution, Avaya systems or other devices or media, such requests will be subject to additional charges.

9 Service Implementation

The Service will be implemented in three stages: Service Activation, Ramp Period and Service Operation. A description of the stages follows in the table below:

Delivery Stage	Description
Service Activation	Service Activation planning will commence promptly following Avaya acceptance of Customer's Order. Avaya will build a new instance and begin to provision and configure the Avaya Aura Private Cloud and/or AXP Private Cloud solution and activate the software supporting the contracted bundles. Service Activation for Standard Systems requires approximately 7 weeks from the initiation of the Avaya Aura Private Cloud and/or AXP Private Cloud build process. Service Activation is the date when the software supporting the ordered Avaya Aura Private Cloud and/or AXP Private Cloud services bundles is activated, and the included Basic Activation Services scope is completed to enable the Ramp Period. This stage does not include any Customer Personalization1. Avaya will notify the

Delivery Stage	Description
	Customer in writing once the Service Activation milestone has been achieved.
Ramp Period	Ramp Period is defined as the period where end users/Agents are onboarded onto the Avaya Aura Private Cloud and/or AXP Private Cloud service. Following the Service Activation notice, Customer will have a 90-day Ramp Period. **Avaya will invoice the Customer for the actual Service Usage Volume during Ramp Period.**
Service Operation	Upon completion of the 90-day Service Ramp Period, Service Operation and the Contract Term will commence on the Service Operation Start Date, at which point **Avaya will invoice the Customer as follows:** ● **Monthly: the greater of the Minimum Monthly Revenue Commitment or the Service Usage Volume; or** ● **Annual Prepay: the Minimum Annual Revenue Commitment and the Monthly Overage Service Usage Volume.**

[1] Customer Personalization is related to Customer-provided items and responsibilities to access and configure the Service for the Customer's specific needs. Personalization and/or onboarding activities are Customer responsibility, unless purchased from Avaya or from a Partner, and can commence at any point following Service Activation but do not prevent completion of the Ramp period.

9.1.1 Avaya Responsibilities

Avaya will assign a Cloud Delivery Project Manager to oversee the delivery of the Avaya Aura Private Cloud and AXP Private Cloud instance, which includes the build out of the infrastructure and the applications as well as delivery of the Basic Activation Services.

9.1.2 Customer Responsibilities

- Customer will designate a single point of contact (SPOC) that Avaya may contact in relation to all general aspects of the 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. In addition, the Customer SPOC will:
    - Communicate to Avaya all decisions, applicable approvals and permissions relating to Customer's acts and activities that may impact the ability of Avaya to provide the Service in accordance with this SD and Avaya Aura Private Cloud and AXP Private Cloud Order.
    - Cooperate with Avaya and provide all information, as may be reasonably required by Avaya, to perform the Service.

10 Cloud Support Services

The Service includes end-to-end operational delivery and support aligned with ITIL service framework, including the services described below. All Cloud Services are included in the rate card pricing.

Note: Use of country-specific resources for deployment (i.e., pre-Service Activation effort) and/or support of the instance must be quoted as a separate premium service

10.1 Service Hours

As part of the Service, Avaya will manage and operationalize the Service using a global support model.

Service Desk	24x7x365 (English Language Only)
Proactive Monitoring	24x7x365; Events received from Avaya's monitoring system
Service Request Fulfillment	8x5 M-F; Excludes weekends and Avaya holidays

10.2 Operations Guide

An Operations Guide will be produced by Avaya to govern the delivery of the Service. The Operations Guide will include key contacts for performing the Service and escalation contacts and processes.

10.3 Service Desk

The Avaya Service Desk handles incident and service requests (including MACDs) from Customer designated IT contacts. Service Desk engineers classify and route these requests to the appropriate support groups for resolution. Customer can primarily reach the Service Desk by accessing the Avaya OneCare Portal. Alternatively, they have the option to contact Service Desk directly by phone.

10.4 Proactive Monitoring

Avaya proactively manages the Service 24x7x365 performing event correlation and submitting alarms to the Avaya Team. Avaya uses an automated incident system integrated with Avaya monitoring systems. Through Avaya OneCare Portal, the Customer has visibility to the cloud operational dashboard. All alarms are addressed through the Avaya incident management process.

10.5 Avaya Admin Portal

The Avaya Admin Portal is a management interface suite that delivers self-service capabilities for Avaya Aura Private Cloud and AXP Private Cloud deployments. Once Service Activation stage is completed, the Customer administrator can perform Template Management, Number Management, Role Bases Access Control (RBAC) and frequently executed Moves, Adds, Changes and Deletes (MACDs) without having to open an Avaya ticket. Tickets are still required for certain functions not exposed or supported in the Avaya Admin Portal.

The portal also provides a self-care for End Users to provide personalization of their UC and CC experience and change their passwords.

The Release information along with latest release and release notes for Admin Portal can be found at https://support.avaya.com/support/en/products/P1785/avaya-enterprise-cloud8482-admin-portal/4.x.

10.5.1 End User Self Care Portal Capabilities

End users can access their personalized self-care portal to modify their UC and CC experience:

End User Self Service Capabilities	**Station**	• Phone button assignment • Update EC-500 • Reset station security code • Setting default station • Reset SIP Password
	Voicemail	• Reset Password

		• Reset web access password
	Supervisor/Agent	• Reset Password

10.5.2 System Administration Capabilities

This interface provides enhanced admin capabilities for the user to perform Number Management, Template Management and Role Bases Access Control.

System Administrator Capabilities	
General Configurations of company locations and different organization units.	• Define location • Organization Units • 911inform integration per location • Multiple-CMs • Verint WFO Integration
Authorization Add Role Based Access Control for Admin Portal users to provide different level of access permissions for different resources.	• RBAC for Admin Portal users • Group scope
Number Management Configure extensions ranges and their mapping to Agents, Stations.	• Extensions • Extension ranges • Analog/Digital ports
Template Management Create or customize template as per business need	• Template and their customization
Logs Access to all the logs for the activities across Admin Portal suite	• Workflow logs • Transaction logs • System logs

10.5.3 Customer Administrator Capabilities

A Customer Administrator can manage users for one of more groups of users, site, or location specific. Their access will be based on pre-defined access criteria. They have the ability to:

Customer Administrator Capabilities	
General Configurations	• 911inform integration per location • Verint WFO Integration • Multiple CMs • Registered station list view, status station view • List trace, List Usage, List agent staffed
Provision a user Create and configure resources for a user based on user profile	• User profiles • Stations • Agent login ID, CMS dictionary • Voicemail (primary, secondary) • CMS Supervisor accounts and permissions
Manage a user	• Re-assign user • Rename user • Change bundle • Change AD security group
De-provision a user	• Removal of all dependencies (like bridge appearances, coverage path MWI)

Manage user resources[1] Add, delete, modify associated with a user	• **Station**: COR, COS, Security Code, Feature Button Assignment, Hunt Group membership, Coverage path, Workplace Attendant, Renumber station, Enhanced call forwarding. • **Agent login ID**: Skills, Security Code, Password, COR, Coverage path • **Voice mailbox**: Password, Web Password. • **CMS Supervisor**: Password, permissions for VDN, Vectors, Skills		
Manage stand-alone resources	• Station • Agent • CMS Supervisor • Coverage Path • Call Pick-up group • Coverage answer group • Verint User	• VDN • Hunt group and Skills • Holiday Table • Service Hours Table • Vector Routing Table • 911inform • Verint Extension Recording	• Voicemail • Vectors • Vector Variables • Announcements • Music on hold • Remote Call Coverage
Bulk-operations Provisioning, de-provisioning, update stations and agents	• Execute workflows in bulk by reading a text input file • On-demand or scheduled workflow execution		

[1] Only assignment and view of existing COR, COS Coverage path is present.

10.5.4 Not Supported or Included

Intercept treatment announcement is not included in Avaya Aura Private Cloud and AXP Private Cloud offer. Professional services are available a one-time fee and will be documented in a separate custom SOW.

10.6 Avaya Service Request Fulfillment

Customer is entitled to a monthly allotment of remote MACD hours to be performed by Avaya. The entitlement of MACD changes is based on the contracted user volume or Agent volume in the customer's Order.

Unused monthly hours may be carried forward to the following month but must be used within the next 2 months or they will be forfeited. Avaya will track and report to Customer the achieved MACD Service Requests on monthly basis as a Service Level Objective (SLO.)

Monthly MACD Entitlement Calculations		
UC Bundles	● UC Volume x 0.7% x 0.25 hours = UC Monthly MACD Entitlement ● For example: UC Volume is 5,000 x 0.7% x 0.25 hours = 8.75 hours per month.	
CC Bundles	**CC Usage Volume**	**Monthly MACD Entitlement Hours per Month**
	100 – 249	10
	250 - 1,500	20
	1,501 - 5,000	40
	5,001 - 10,000	60
	10,001 - 20,000	90
	20,001 +	110

The customer may exhaust the allocated MACD entitlements and still require additional MACD work to be

done before the next MACD entitlement replenishment. These extra hours will be billable with billing charged as Time & Material (T&M) or as additional MACD Block of Hours (BOH) purchased by the customer. The customer's Order will contain the pricing for T&M and for BOH.

Considerations:

- The monthly MACDs entitlement does not apply to on-site MACDs or Projects.
- If a customer chooses not to self-serve through the Avaya Admin Portal and requests Avaya to perform the MACDs instead, the hours of the corresponding effort will be deducted from the Monthly MACDs entitlement.

10.6.1 MACD Categories

MACD requests are classified by Avaya in accordance with the table below:

Type	Description	Time Period
User Level (Simple MACD)	MACDs performed at the user level, including adding, changing, or deleting user mailboxes and phone extensions and resetting passwords	For MACDs that require Avaya support, Avaya targets completion the next Business Day for 95% of MACDs for requests submitted by 3pm local DC site time to Avaya via the OneCare portal. Requests that include more than 15 activities are considered Complex MACDs and completion time is determined on a case-by-case basis.
System Level (Complex MACD)	Changes that are performed at system, or application level, including moves, additions, changes or deletion of users, call-flows, and dial plans, provided they: ● Can be completed within 1 change window. ● Require no project management. ● Do not include new features or Services. ● Require no additional professional services. MACDs performed at the system or application level only through ticket requests.	completion timeframes are mutually agreed on a case-by-case basis depending on the scope of the request.
Project	Changes which are solution or system wide only through ticket requests.	Project MACD completion timeframes are mutually agreed on a case-by-case basis depending on the scope of Project MACD request.

10.7 Avaya Cloud Migration Tool

An enterprise solution designed to transition existing resources from Aura on-premises systems to the Avaya Aura Private Cloud and AXP Private Cloud offer. This tool enables an efficient and secure migration process. Cloud Migration Tool is an optional entitlement included in Avaya Aura Private Cloud and AXP Private Cloud Bundles. As part of the Service, Avaya will enable the tool while customers are responsible to perform the data migration from on-premises to the Avaya Aura Private Cloud and AXP Private Cloud solution.

The following features are provided:

- Tool will convert H.323 station to SIP; add required profiles in the system, convert feature buttons.
- Call routing (dial patterns) will be added to both on premises and cloud systems correspondingly to ensure the proper call routing to migrated users.
- Support exclusions to omit certain data to be copied from the system on premises.
- Dependency check and report to prevent issues.
- User migration in groups. Note: users who belong to a group must be migrated at the same time.

Cloud Migration Tool supports the migration of the following data:

Communication Manager (CM)	• Dial plan analysis table • CM Locations • COS • COR • Coverage paths • Hunt groups • Pickup groups • Stations, including bridged appearance groups • VDNs • Agent Login IDs • Vectors • Holiday Tables • Service Hour Tables • Vector Variables • VRT • CAG • Abbreviates Dial Lists
Voicemail	• Voicemail boxes
Call Management System (CMS)	• Dictionary • Supervisors

The Customer Migration tool requires secure access to the migrating system Communication Manager, System Manager and CMS. Avaya recommends this connection traffic is restricted to the ExpressRoute Connection to Avaya Aura Private Cloud and AXP Private Cloud and firewalled to only the Avaya accessing IPs. This link is required for operation of the migration tool and Avaya recommends ensuring this link is able to be provided before progressing with the migration tool including any security approvals that may be required for the customer's IT processes.

Compatibility

- Aura release supported is Aura 6.3 or higher.
- CMS release supported is CMS 15 or higher.

Limitations

- Cloud Migration Tool Release supports one to one CM migration.
- Voicemail messages are not copied over during the migration of voicemail boxes.
- Announcements migration is not supported.
- Dial plan is not modified during migration. Change of phone number is not supported.
- DCP and Analog phones migration is not supported.

10.8 Release Management

Avaya Release Management determines and deploys Service updates. Avaya engineers proactively monitor updates for infrastructure supported that are relevant for the Customer's environment.

10.9 Maintenance and Updates

Regular maintenance, updates, and upgrades are fundamental to ensure the Service operates at its peak performance and remains secure. These ongoing activities help address software vulnerabilities, enhance features, improve system stability, and ensure compatibility with emerging technologies and industry standards. Customer will be notified based on the scope of these activities.

10.9.1 Maintenance

Avaya will perform regular, recurring as well as ad-hoc updates and upgrades to help ensure the Service remains reliable and performant. Every effort will be made to avoid the customer's peak business hours. Maintenance that does not impact the customer's business operations will be performed at Avaya's discretion and without prior notification.

10.9.2 Security Scan and Network Penetration Testing

Avaya will perform quarterly security scans and annually network penetration testing. Every effort will be made to avoid the customer's peak business hours. Deployment of compensating controls or direct remediation that does not impact the customer's business operations will be performed at Avaya's discretion and without prior notification.

10.9.3 Emergency Changes

Avaya will notify the customer of time and scope as needed. Avaya will attempt to provide advance notice for Emergency windows if Avaya deems the change may be service impacting.

10.9.4 Major Release Change

Major Release Changes are at the sole discretion of Avaya. If Avaya plans a change on the Service that will affect End Users use of the system, it will be referred to as a "Major Release Change". Avaya will:

- Endeavor to notify Customer at least 30 days in advance.
- Provide Customer with an analysis of any predicted changes to feature functionality.

10.9.5 Notification Reminders

Reminders of such windows occurring will be sent to the Customer ahead of time. Should Avaya determine in its judgment that shorter or concurrent notice is necessary to protect the Service or other Customers

from imminent and significant operational or security risk, then Avaya reserves the right to change the windows provided. Communication on these windows will be done by the Service Delivery Manager.

10.10 Service Management

Avaya assigns a shared Service Delivery Manager (SDM) to all Avaya Aura Private Cloud and AXP Private Cloud customers. The SDM is focused on ensuring the seamless and effective delivery of service to their assigned customer, aligned with Avaya's contractual commitments. As the Customer's advocate within the Avaya Services organization, the SDM works to elevate Customer satisfaction relative to the Avaya-managed solution. To be most effective, the SDM works to establish trusted relationships with Customer stakeholders while partnering directly with the Avaya account team and others as well as is positioned to understand and represent Avaya in all aspects of the Customer's in-service Avaya solution. SDMs are closely involved with all aspects of Operational Service Delivery, providing service per ITIL guidance such as Performance Management, Change Management, Capacity and Availability Management. The SDM leads Avaya's response in the event of Major Incidents, partnering with key Avaya teams to rapidly restore service where required.

10.11 Customer Responsibilities

- Provide an End User Help Desk to assist with general usability and operational support queries and perform initial triage and remediation efforts before opening an Incident or Service Request ticket with Avaya.
- Accept and provide required Avaya designated maintenance windows for the Service (including updates and upgrades to the Service).
- Notify Avaya of any changes to Customer’s network or products and solutions connected to, or integrated with, the Avaya Aura Private Cloud and AXP Private Cloud solution that may impact performance of the Platform, including network configuration or changes to IP addresses.
- Provide Avaya with Letter of Agency (LOA) when required. A LOA authorizes Avaya to act on Customer’s behalf within the scope of Vendor Management activities.

11 Service Levels and Reporting

This Section sets forth the applicable Service Levels Agreements (SLAs) for Avaya Aura Private Cloud and AXP Private Cloud. The SLAs detail the objectives to be measured and circumstances under which Avaya will be responsible for Service Credits for failure to achieve specified SLAs. Service Levels will start on the next Business Day following the Service Operation Start Date and will be measured monthly based exclusively on the information stored by Avaya.

11.1 Severity and Service Level Definitions

The following table provides the guidelines for the severity levels assigned to trouble tickets associated with the services that are delivered as part of the Customer’s Order.

Severity Level	Service Level	Target Incident Response
Critical Business Impact Customer's business suffers a complete loss or degradation of services that impacts all End Users assigned to a DC; and/or complete loss of core functionality such as call processing.	Time to notify	≤15 minutes for 95% of Incidents
	Time to restore	MTTR ≤ 4 hours
Moderate Business Impact Customer's business suffers partial loss or severe degradation of services that impacts a large number of End Users, typically more than 25% of End Users. Partial loss or severe degradation of core functionality such as call processing.	Time to notify	≤60 minutes for 95% of Incidents
	Time to restore	MTTR ≤ 6 hours
Minimal business impact Customer's normal business is not significantly affected. A small number of End Users, including single End User affecting incidents; or availability/operation of a particular feature or functionality.	Time to restore	Next Business Day for 85% of Incidents

Avaya will track and report to Customer the achieved remote response time on a monthly basis per the service defined as follows:

Time to Notify: Elapsed time from creation of an Incident Record until Avaya has provided an electronic notification to Customer.
Time to Restore: Elapsed time from creation of an Incident Record until Avaya has restored Normal Service Operation

Calculation:

MTTR is 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 the month; and
- Y is equal to the total number of Incidents with the same Incident Severity that have occurred during the month.

11.2 Core Service Availability

Avaya will provide a monthly availability report of the core service elements. The following availability targets apply to the provision of Avaya Aura Private Cloud and AXP Private Cloud:

Core Service Elements	Availability Target
UC Basic, UC Core and UC Power bundles	99.99%
Contact Center – Voice bundle	99.99%

Elements not listed as a core service element are not covered by core SLA.

The monthly Availability performance (%) for an Avaya Aura Private Cloud and AXP core service element will be calculated in accordance with the following formula:

Formula:	Monthly Availability performance (%) = (A – B- C) / (A – C) × 100% where: A = total number of minutes in a month B = total number of minutes the Service has been Out of Service during a month C = Scheduled maintenance time or planned downtime
Example:	A = 31 days × 24 hours × 60 minutes = 44640 minutes B = 15 minutes C = 120 minutes Monthly Availability performance (%) = ((44640-15-120) / (44640-120)) * 100% = 99.966%

Out of Service for each Avaya Aura Private Cloud and AXP Private Cloud core service element is defined as follows:

Core Service Element	Definition Out of Service
UC Basic, UC Core, UC Power	Loss of call processing functionality due to a Critical Incident.
Contact Center – Voice	Loss of call routing functionality due to a Critical Incident.

11.2.1 Excluded Downtime

Total minutes in a month that can be attributed to Scheduled Downtime or Downtime caused by factors outside of Avaya's control. Examples include:

- Any time during which Avaya has been awaiting a Customer or third party (acting on Customer's behalf) deliverable, action, dependency, or prerequisite, including Customer testing or verification of Incident solutions prior to implementation.
- Anytime Customer withholds access for required updates, patches, or bug fixes to restore normal Service operation.
- Incidents caused, or contributed to, by:
  - Actions or omissions of Customer or third parties, including carrier and service providers.
  - Reasons external to the Avaya Aura Private Cloud and AXP Private Cloud solution and Azure cloud infrastructure on which the Avaya Aura Private Cloud and AXP Private Cloud solution is hosted, including power failures and shutdowns, third party products and applications, networks, and network service interruptions.
- Customer provided and/or procured SBCs or SIP gateways that do not satisfy the eligibility requirements.
- Any other reasons or events beyond the reasonable control of Avaya.

11.3 Exclusions

While Avaya will use commercially reasonable efforts to achieve the Service Level targets prior to Service Operation Start Date, Avaya will not be responsible, and disclaims any liability, for any SLA failure that has occurred before the Service Operation Start Date.

11.4 Reporting

Avaya will continuously track and monitor compliance with the Service Levels targets and will provide the monitoring results to Customer as part of the standard reports.

The monthly reports listed below will be provided electronically which may include posting reports on the Avaya web portal:

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 set out above including a 6-month rolling trend analysis.

Customer will review each Service Level Report within 2 weeks from the date it has been made available to Customer. If not rejected 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 governance meetings. Any unresolved matters will be escalated pursuant to the escalation process agreed in the Operations Guide.

11.5 Service Credits

11.5.1 Availability

If at any time after Service Operation Start Date during any monthly period, Avaya has failed to achieve the Availability target for one or more Avaya Aura Private Cloud and AXP Private Cloud core service elements defined above, the applicable Service Credit will amount to 5% of the Recurring Charges for the affected Avaya Aura Private Cloud and AXP Private Cloud Bundle(s) for the impacted monthly period.

11.5.2 Incident Notification and Restoration

The following Service Credits will apply if, during any monthly 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 monthly period
Major	2% of the Recurring Charges payable for the affected monthly period

11.5.3 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 30 days after the end of the relevant monthly period.
- Services Credits due will be paid by Avaya within 90 days from receipt of Customer's request.

- Except as otherwise agreed by the Parties in writing, payment of Service Credits will be made in the form of a credit against future amounts due from Customer to Avaya under this SD.
- The total amount of all Service Credits due from Avaya for any monthly period may not exceed 5% of all Recurring Charges due for that monthly 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.

12 Service Charges

This Section details how Avaya will determine the charges applicable to Avaya Aura Private Cloud and AXP Private Cloud. The applicable charges will be comprised of recurring charges and other charges.

12.1 Recurring Charges

12.1.1 Minimum Revenue Commitment

Avaya Aura Private Cloud and AXP Private Cloud Bundles will be invoiced subject to Minimum Revenue Commitment and Minimum Order Quantities as documented on the Order Form. The Total Minimum Revenue Commitment is also established on the Avaya Aura Private Cloud and AXP Private Cloud Order for the Customer.

- **Monthly**: Starting on the Service Operation Date, Avaya will invoice on recurring basis in arrears the greater of the Minimum Monthly Revenue Commitment or the Service Usage Volume.

- **Annual Prepay:** Starting on the Service Operation Date, Avaya will invoice the Customer for the Minimum Annual Revenue Commitment for the first year. Monthly Overage Service will be invoiced monthly. Subsequent annual prepayments are to be invoiced on the anniversary of the first Annual Prepay.

12.1.2 Determination of Service Usage Volume

Avaya measures usage of each usage-based service element based on the quantity of units used by the Customer during each monthly billing cycle. On the first day of every month, the Cloud Management System will calculate the Usage Volume for the previous month that will be used to calculate the usage charges due for the associated invoicing cycle.
Note: Avaya does not provide metering per site or per country.

12.1.3 Avaya Aura Private Cloud Service Usage

Daily, the Cloud Management System will count the peak usage of each hour for the Avaya Aura Private Cloud service and then store the count for the peak hour. Monthly Peak will be highest daily peak usage volume for a Unit during a month. For Avaya Aura Private Cloud service, the peak usage is based on Provisioned stations.

A ***Provisioned Station*** for Basic, Core and/or Power is an extension configured on the Avaya Aura Private Cloud solution with an assigned phone number. The unit count is the **monthly peak of Provisioned stations** for UC Basic, UC Core, UC Power.

- A Provisioned station is an extension configured on the Avaya Aura Private Cloud solution with an assigned phone number.
- A station is not always associated with a person but any extension, DID, virtual meeting room, mailbox, etc. that is programmed. For example, commonly, conference room phones and lobby phones consume a station while not being associated with any particular person.
- Avaya tracks Provisioned stations with no concept of tracking active or registered stations. Even if a phone is not active or registered, if it is Provisioned, it is counted as a used unit for the periods while a station remains Provisioned.

12.1.4 AXP Private Cloud Service Usage

Daily, the Cloud Management System will count the peak usage of each hour for the AXP Private Cloud service and then store the count for the peak hour. Monthly Peak will be highest daily peak usage volume for a Unit during a month. For AXP Private Cloud service, the usage is based on concurrent Agents or is fixed.

Fixed Recurring rate carded items are not dynamically metered for billing purposes and are charged in the same quantity each month as that set out in the Order. For any application not dynamically metered, no daily counts appear on the AXP Private Cloud billing reports.

Generally, for AXP Private Cloud service elements, tracking logged-in Agents does not discern whether an Agent is active or not. A logged-in Agent is counted even if no calls are handled by that Agent. Agents should log out when not using the AXP Private Cloud service to reduce metered usage count.

Avaya measures the usage service volume based on the quantity of units used by the Customer during each monthly billing cycle based on Monthly Peak of Concurrent Voice Agents.

12.1.5 Use of Generic Customer Identifiers

Customer acknowledges and agrees that Avaya will collect and use generic information concerning Customer's usage of the Service and will store such information including Customer's identifiers solely for the purpose of providing the Service.
Avaya reserves the right to audit any entity hosting the Avaya Aura Private Cloud and AXP Private Cloud solution for the proper use of all features and billing profiles to ensure that all features in use are measured, billed, and paid in accordance with the Cloud Contract and applicable Cloud Orders.

12.2 Usage Above Order Quantities

Any usage in excess of the Order quantities defined in the Customer's Order will be billed at the same rate as the Customer's Order tier price per unit.

12.3 Other Charges

Avaya will invoice all other charges and fees due in relation to the Service as set out in Avaya Aura Private

Cloud and AXP Private Cloud Order and any applicable Project or Termination Assistance statement of work.

13 Initial Term, Renewal and Termination

13.1 Initial Term

The Initial Term will be indicated in the Order. Typically, the Term ends 36 or 60 months after the Service Operation Start Date.
Where both Avaya Aura Private Cloud and AXP Private Cloud are contracted, the Service Operation Start Dates may or may not be concurrent, and in those cases, the Contract Term will begin with the later Service Operation Start Date.

13.2 Renewal

Unless either Party provides ninety (90) days advance written notice prior to the end of the initial Term of their intent not to renew, accept where prohibited by applicable law or otherwise agreed in writing by Avaya, the initial Service Term will renew, and continue to renew automatically, (i.e., Renewal Term) subject to the then current i) rate and ii) Service Description.

13.3 Termination for Convenience

Customer may terminate an Order for convenience upon 90 days written notice (email not sufficient), subject to Customer's payment of the termination charges described below. Termination will be effective at the end of the month in which the 90-day period has ended.

Customer will pay Avaya a termination charge calculated in accordance with the following formula based on the Order Effective Date:

Time Period	Charge
0-24 months	Minimum Remaining Charge X 100%
25 months – end of Contract Term	Minimum Remaining Charge X 60%

Charge is the Minimum Revenue Commitment (MRC) for the period starting from the effective date of termination until the end of the Contract Term.

Any partial termination of an Order must be agreed by both Parties in writing, including their Agreement on the new charges and Minimum Commitments.

13.4 Termination for Material Breach

If Avaya terminates an Avaya Aura Private Cloud and AXP Private Cloud Order due to Customer's uncured material breach, Customer will pay Avaya a Termination Charge calculated in accordance with the following formula:

Period in which the effective date of termination occurs	Formula

Any time from the Effective Date of Avaya Aura Private Cloud and AXP Private Cloud Order until end of the Term.	***Minimum Remaining Charge* × *100%***

14 Exit Management

14.1 Termination Assistance

Upon termination or expiration of an Avaya Aura Private Cloud and AXP Private Cloud Order, Avaya may provide Termination Assistance. Termination Assistance will be provided pursuant to a separate Order or statement of work agreed by the Parties which will define:

- Scope of Termination Assistance.
- Duration of Termination Assistance (up to a maximum period of 120 days following termination or expiry of an Avaya Aura Private Cloud and AXP Private Cloud Order).
- Any data or information that will be handed over to Customer or successor provider.
- Charges payable by Customer to Avaya; and
- Invoicing schedule.

Avaya may condition its cooperation with, or provision of any information or materials to, a successor provider upon execution of a non-disclosure Agreement on such terms as reasonably required by Avaya.

14.2 Exclusions and Limitations

Avaya will not be obligated to provide any Termination Assistance and/or ongoing Services if the Order has been terminated for: (i) Customer's material breach; (ii) Customer's breach of the Avaya license terms or intellectual property rights; or (iii) Customer's failure to make timely payments of any charges or other fees due to Avaya.

There is no obligation for Avaya to provide any proprietary, confidential, or commercially sensitive information of Avaya, its suppliers, subcontractors or Customers, or any information regarding the charges or cost of the Service.

15 Appendix A: Supported Devices

Avaya supports compatible Avaya SIP phones that support MAC level detail and TLS 1.2. Customer is responsible for installation and providing the supported devices and ongoing maintenance support.

Device Type	Basic User	Core User	Power User
Avaya J Series Phones. Note J169 is End of Sale	•	•	•
Avaya IP SIP Desk Phones 96x1 series; minimum firmware vintage: 7.1.3. Note: Phones are End of Manufacturing Support - Only basic calling capabilities are supported.[1]	•	•	•
Avaya B100 Series SIP conference phones	•	•	•
Avaya Vantage 3 - minimum firmware version 3.1 (includes K175 and K155).	•	•	•
Avaya Workplace client for iOS, Mac, Android, and Windows.[1]	-	•	•
Flying Voice ATA G508.[1]	•	•	•
Avaya Edge Friendly Gateway [1]			
Avaya G430 and G450 chasses – Vintage 1, 2, 3, 4 Note: The firmware for the gateways must be upgraded to a compatible release.	•	•	•
DSP models MP40, MP120 and MP160	•	•	•
Supported with Avaya Edge Friendly Gateway (G430/G450) [1]			
Avaya 2500 Series Analog Phones. Note: some phones may offer features that are not 100 percent compatible with line quality.	•	•	•
Avaya Digital Phones: 14xx series: (model1408) and 94xx series: (model 9408)	•	•	•

Package Key	Symbol
Supported	•
Not Supported	-

[1] Not supported by Device Enrollment Services

15.1.1 Analog Telephone Adapter

Avaya Aura Private Cloud supports Analog Telephone Adapters which allow Customers using small number of analog equipment like fax machines, endpoints, and analog paging systems to work with Cloud services over IP. Supported ATAs (Flying Voice ATA G508) can be purchased separately by the Customer when placing Avaya Aura Private Cloud Order.

Any ATAs not listed are not supported.

15.1.2 Edge Friendly Gateway

Avaya legacy gateways (G430/G450) can become cloud friendly (or edge friendly) and connect natively to the Avaya Aura Private Cloud SIP core. Customers can re-use existing G450s/G430s with their digital (2-wire)

and analogue stations as well as local trunk setups (ISDN PRI/BRI). The firmware of the gateways and media modules must be at the compatible release level.

Avaya Aura Private Cloud offer does not include installation, firmware upgrades or gateways integration to the Avaya Aura Private Cloud environment. These services are available from Avaya for a one-time fee and will be documented in a separate custom SOW.
Avaya S8300 servers deployed with G430 or G450 Media Gateways can now provide local survivability when connected to AXP Private. In the event of a connection failure to the central Avaya system, these gateways can automatically transition to local call processing mode, allowing users configured on the local system to continue to make and receive calls, access voicemail, and utilize basic telephony features.

For implementation details, configuration requirements, or supported deployment topologies, please contact your Avaya representative or refer to the latest Avaya documentation.

15.1.3 Customer Responsibilities

- Purchase, provision and install all required phones that are compatible with the Service.
- Arrange and pay for any required fees for firmware updates or vintage upgrades.
- Replace phones, if required.
- Flash phones to SIP and point them to Avaya Aura Private Cloud. This includes migrating all the private data from an end user's phone (e.g., personal contacts, ringing levels).
- PCs, laptops, or mobile devices that support Avaya clients.
- For Local survivability (if required):
    - must provide and pay for certificates - 3 certificates per survivable remote.
    - Premises SBC for the SIP trunk and it must meet the Avaya requirements for that SBC

15.1.4 Not Supported or Included

- Any H.323 endpoints.
- J100 endpoints are not supported with Local Survivability (ESS, S8300) and Simple Local Survivability
- Digital endpoints are not supported unless through G430/450 (Edge Friendly Gateway).
- Avaya DECT phones are not supported.

16 Appendix B: Avaya and Customer RACI

The following shows the responsibilities of Avaya and the End Customer.

Responsibility	Details	Avaya	End Customer
Project Management Office (PMO)	Customer interface for project, service and technical	●	
Customer Service Exec / Service Delivery Manager	Interface to Customer	●	
Monthly Reporting on Service Performance (Tickets, SLAs, etc.)	Reporting to Customer designated contacts	●	
All Network traffic to and from the Avaya Aura Private Cloud /AXP Private Cloud instance (e.g. SIP Trunking)	Architecture Design, Deployment, Interconnect		●
Procure Internet, ExpressRoute	Connect Customer to cloud		●
Network Readiness Assessment			● (If not performed by Avaya)
Meet Network Requirements			●
Data Center Asset Ownership and Security		●	
Cloud Core Hardware and Software Ownership		●	
Updates and Upgrades to Cloud Core Hardware and Software		●	
Cloud Core Hardware and Software Security		●	
Network Connection between Avaya Cloud Core		●	
3rd Party apps which are offboard hosted			● (build / procure)
On-Prem Connected Products	Phones, PBX remaining on-prem – may be procured from Avaya or 3rd Party – asset ownership is with Customer		● (procure & install if not partner provided)
Customer-owned IVR applications or application servers (on-prem or cloud)	IVR Application servers remaining on-prem or cloud asset ownership is with Customer		● (procure & install if not partner provided)
Customer-owned CTI applications (on-prem or cloud)	CTI Application servers remaining on-prem or cloud asset ownership is with Customer		● (procure & install if not partner provided)
Installation, auto-configuration of soft clients, and MS Teams client			●
MS Direct Routing – MS License	Appropriate Microsoft license to support Direct Routing		●

Customer Data Gathering Cloud Solution Level	Call flows, station data		● (gather)
Logistical Per Seat Data Gathering	Phone Templates, for example	● (provide station template)	● (Complete station template for each user/Agent)
End-to-end Solution Design		●	●
Cloud Core Design, Install and Configure		●	
Onboarding of users/Agents into Avaya Aura Private Cloud and Avaya Experience Platform Private Cloud solution		● (Optional, if purchased personalization)	● (Available with self-service)
Cloud Core Data Backup	Customer specific configuration	●	
Scheduled Maintenance	Scheduling and production impact review	●	
Service Management for Avaya Aura Private Cloud and Avaya Experience Platform Private Cloud		●	
Level 1 Service Desk	Customer provides Service Desk for initial triage		●
Level 2 Service Desk	Avaya provides Level 2 Service Desk to designated IT Customer contacts	●	
User Simple Level MACDs	Avaya Admin Portal	● (If not available with self-service)	● (Available with self-service)
Complex System Level MACDs	Customer IT contacts submit tickets to Avaya Level 2 Service Desk via OneCare Portal.	● (If not available with self-service)	● (Available with self-service)
Customer On-premises Endpoints Management (phones)		Remote Monitoring only	On-Site Support / Install / Parts/ Updates
Level 2 Ticket input for MACD requests	Level 1 Service Desk performs Ticket Entry to OneCare Portal		●
Training Customer Users/Agents	Custom priced curriculum for incremental fee	●	