



November 27, 2018

Department of Administration, Purchasing Division  
2019 Washington Street East  
Charleston, WV 25305-0130

**Re: Carahsoft's Response to the State of West Virginia's Request for Proposal for Managed and Hosted Voice Services, Solicitation # CRFP 0212 SWC1900000001**

Dear Mr. Atkins,

Carahsoft Technology Corp. appreciates the opportunity to respond to the State of West Virginia (State)'s Request for Proposals for Managed and Hosted Voice Services. Carahsoft is proposing Genesys which meets State's requirements. Our team has fully considered the State's requirements outlined in the RFP, and has carefully put together a solution that will best meet your needs.

Since opening its doors in 2004, Carahsoft has successfully executed over 85,000 orders to State and Local Government entities. As a top-ranked partner for Genesys, Carahsoft has delivered best value solutions to our public sector clients for over 14 years.

Please feel free to contact me directly at 703.921.4059/[Zachary.Kutyn@Carahsoft.com](mailto:Zachary.Kutyn@Carahsoft.com) with any questions or communications that will assist the State in the evaluation of our response.

This proposal is valid for 90 days from the date of submission.

Thank you for your time and consideration.

Sincerely,

Zachary Kutyn  
Account Representative

RECEIVED

2018 NOV 27 PM 12:06

WV PURCHASING  
DIVISION

# TABLE OF CONTENTS

<b>Executive Summary</b> .....	<b>2</b>
Prime Contractor: Carahsoft Technology Corp.....	2
References & Past Performance .....	7
Architecture Summary .....	11
<b>Requirements Response</b> .....	<b>16</b>
<b>Attachments</b> .....	<b>64</b>
Signature Pages.....	64
Addendum Acknowledgement Form.....	67
Purchasing Affidavit .....	69
Attachment 4.2.1.1.1-7 - Avtex - State of West Virginia Support Handbook.....	71
Attachment 4.2.1.1.1.4 - Presidio Service Transition Management v2.....	110
Attachment 4.2.2.1.1-1 - Avtex - SoWV - Base Configuration Premier CSA.....	115
Attachment 4.2.2.1.1-2 Avtex - SoWV - Managed and Hosted Voice Services Agreement...	122
Attachment 4.2.2.4.3 - Avtex - State of West Virginia - SOC 2 Letter .....	133
Attachment 4.2.2.5.2 - Avtex Project Process Overview 2018.....	135
Attachment SO-1 - Avtex - SoWV - Managed and Hosted Voice Services - Base Configuration SOW_Redacted .....	143
Attachment SO-2 - State of WV – Carahsoft SOW (Legacy Cisco UC) .....	172

## Privacy

All intellectual property rights are owned by Genesys.

## Trademarks

The PureEngage and PureConnect names are trademarks of Genesys.

The PureCloud name is a registered trademark of Genesys.

The PureEngage, PureConnect and PureCloud logos are trademarks of Genesys.

All third-party trademarks or registered trademarks are the property of their respective owners.

Genesys retains all rights regarding its trade dress, trademarks, service marks, and trade names.

## Copyright

Copyright 2018 Genesys. All rights reserved.

## EXECUTIVE SUMMARY

### Prime Contractor: Carahsoft Technology Corp.

Carahsoft Technology Corp. is an IT solutions provider delivering best-of-breed hardware, software, and support solutions to federal, state and local government agencies since 2004. Carahsoft has built a reputation as a customer-centric real-time organization with unparalleled experience and depth in government sales, marketing, and contract program management. This experience has enabled Carahsoft to achieve the top spot in leading public sector software license resellers.

**VENDOR RELATIONSHIPS** – Carahsoft has a unique business model focusing on providing superior sales and marketing execution, a track record of success, high integrity, and a focus on strategic vendor relationships, of which Genesys is an important part.

**PROVEN EXECUTION** – Carahsoft has leveraged its vast contracting experience and extended it to quoting and order management. Carahsoft seamlessly generates quotes within 30 minutes or less and processed over 85,000 orders in 2017 that were each completed the same day received.

**CONTRACT VEHICLES** – Over the past 14 years Carahsoft has acquired and maintained a wide variety of purchasing contract vehicles for agencies at the state, local, and federal levels. Associated with all contracts are dedicated and experienced contract management resources. A list of available contracts can be found at [www.carahsoft.com/contracts/index.php](http://www.carahsoft.com/contracts/index.php).

**GROWTH & STABILITY** – Carahsoft has continued to show impressive growth year after year, with annual revenue of \$3.4 million in our first year in 2004 to \$4.4 billion in 2017. In September of 2017, 10,705 orders were processed worth over \$1 billion. We are a stable, conservative, and profitable company and have received numerous accolades, as detailed on our awards page: <http://www.carahsoft.com/awards>.

### What You Want to Achieve

The infrastructure for The State of West Virginia (SoWV) is aging and soon to be unsupported and SoWV leadership has embraced the fact that there is a limited time to identify the best solution to meet existing and evolving needs of highly diverse agencies and departments, while providing new, modern capabilities that will meet evolving citizen demands.

The SoWV is seeking to deliver existing and new features and utilize a new support model for their contact center platform. The challenge when embarking on a transformation like this is finding the right partner which provides leading technology, expertise in transformation projects and ability to execute. This is no easy task many offers in the market do not have the experience necessary to deliver or provide a cobbled together solution which requires significant effort on the side of the customer and does not meet the desired business outcomes. Genesys will provide the experience and platform the SoWV will need to not only transition to a hosted contact center but execute on a brand differentiated customer experience that is expected of the Mountain State! The Genesys solution will be able to leverage your existing Cisco hardware and integrate seamlessly to what you are using today as we have done for thousands of other customers.

SoWV requires a highly scalable, flexible solution that will allow departments to deliver services to their citizens in an efficient and reliable manner, while improving the overall experience, whether communication is internal to a state employee or with a resident of the SoWV.

Carahsoft, along with our partners Genesys, Avtex and Presidio will deliver an integrated solution that exceeds the requirements outlined in this RFP. Our solution goes far beyond the basic voice and ACD functionality and addresses bigger picture needs that that can only be met by leveraging Genesys's Omnichannel platform and our team's experience.

A few highlights on our solution:

- Our solution is a Hybrid Software as a Service / Cloud architecture for the Voice and Contact Center. Deployments which combines local survivability and the ability to scale in times of need
- Enterprise-grade voice platform with 99.99+% uptime
- Omnichannel engagement platform that enables citizens to interact with the SoWV in their preferred method
- Ability to integrate into and with SoWV's Skype applications and any other application needed
- Support for remote access and operations in the event of a natural disaster
- Support for bursting of Inbound and Outbound channels in times of need (legislative changes, etc.)
- **Enterprise Grade Security and Reliability**
- Effortlessly manage SoWV's interactions with its 10,000 business users and ability to scale to 20,000+ users with a comprehensive omnichannel experience platform.
- An interaction management approach that is comprehensive and seamless. Whether voice, fax, email, or web-based communications, Genesys Cloud takes a total, customer-centric approach to improving service and customer satisfaction.
- Flexibility inside and outside the contact center. Our licensed solution is priced to allow enterprises to deploy Genesys Cloud as an organization's total communications solution including executive, administrative, and remote office staff.
- All-in-one platform consolidates the entire multi-vendor voice and contact center stack. Operates seamlessly within your enterprise - the Genesys solution is designed to either replace or fully engage with your telephony, data and applications infrastructure.

## Genesys Highlights

Genesys is the most advanced software and service provider in the customer experience market today. Since 1990, Genesys has brought innovation to the customer experience market from software-based CTI through cross-channel routing and continuing with advanced analytics, modern desktops and the ever-growing integrations that allow companies to define their branded experience, always with an eye towards standards and open platforms.



Our spirit of innovation makes Genesys a future-proof platform that demonstrates our promise to you and our financial ties to this commitment – and to maintaining our leadership in the call center industry.



Gartner has rated Genesys a Magic Quadrant leader 10 years running for Contact Center infrastructure, 4 years running for Contact Center as a Service<sup>1</sup>, and for the first time, Genesys is a leader in the Market Share Analysis: Customer Experience and Relationship Management Software, Worldwide, 2017<sup>2</sup>. Frost & Sullivan recognized Genesys as their 2018 North American Contact Center Company of the Year<sup>3</sup>. Ovum Decision Matrix ranked Genesys as leader in their 2017-2018 report on Selecting a Multichannel Cloud Contact Center Solution<sup>4</sup>. Over 40% of the Fortune 500 and 50% of global 200 companies use Genesys to improve their CX processes.



**The Only Pure Play Customer Experience Vendor**

- ✓ **1990** Incorporated
- ✓ **45** Countries with Offices
- ✓ **120** Countries Served
- ✓ **5,000+** Employees
- ✓ **11,000+** Customers
- ✓ **1,200+** Partners
- ✓ **1,000** Patents
- ✓ **\$250m** Annual R&D Investment
- ✓ **\$1.4B** Revenue

**Figure 1: Magic Quadrant for Contact Center as a Service, North America**

Our spirit of innovation makes Genesys a future-proof platform and maintains our leadership in the CX marketplace. Combining the best of technology and human ingenuity, *we work the way you think.*

Genesys has worked with associations, federal, state and local government agencies that offer a complex and varied array of programs to a wide segment of the population. Even as budgets shrink and

<sup>1</sup> These reports are available at <http://www.genesys.com/about/resources/2017-gartner-magic-quadrant-for-contact-center-infrastructure-worldwide>

<sup>2</sup> This report available on <https://www.genesys.com/resources/gartner-market-share-analysis-cerm-worldwide?cid=7010d00000mYNf>.

<sup>3</sup> This report is available at <http://www.genesys.com/about/resources/2018-contact-center-company-of-the-year>

<sup>4</sup> This report is available at <http://www.genesys.com/about/resources/2017-ovum-decision-matrix>

regulation increases, organizations are facing unprecedented pressures to provide services quickly and with an expected higher level of service.

The SoWV has been challenged in multiple areas with their voice and contact center services. The state is challenged with aging systems, multiple systems that are not integrated causing siloed environments, increased complexity, and limited resources to deliver an Enterprise-Level of service to their constituents. This leads to abandonment and restarting interactions again on alternate channels. Administrative tasks, such as address changes or service requests, can be difficult to track efficiently. And, keeping citizens informed at the masses or individually is a challenging task made more complex by the use of multiple channels.

This is where Genesys can help the SoWV by aligning its communications and contact center solutions with key priorities like managed services to support the legacy IP environment, successfully transition the legacy IP environment in a phased approach, create hosted voice services to support 10,000 users and add functionality to the hosted voice services to support 25 contact centers with 550 agents scalable to 800.

### **Avtex Highlights:**

At Avtex, our mission is to fuel exceptional customer experiences. From the way our company is architected, to the DNA of our everyday activities, our vision lives and breathes within our employees. We strive every day to make the lives of our individual clients and their citizens easier and simpler. The combination of Avtex and Genesys make up a world leader in contact center platform development, implementation, support and continuous innovation. We are proud to be heading into our 21st year of partnership in delivering solutions that transform the way organizations communicate with their citizens. Our combined team provides an end-to-end, integrated customer experience portfolio including CX strategy consulting, contact center technology solutions, CRM and business application integration, and overall application development.



With over 30 years of experience, the Avtex team supports 989 CX technology implementations including State of Tennessee, State of California, Pentagon Federal Credit Union, and US Department of Veteran Affairs to name a few. Partnered with the West Virginia team, Avtex will be the key to the success of the West Virginia vision for a holistic, integrated, and adaptive communications platform. From consulting, design, implementation, testing, and training, our objective is to reduce complexity and create a great learning environment for your team. We also understand that although the contact center is the core of the citizen experience, your entire ecosystem directly impacts the experiences you provide. Making sure the appropriate technology platforms and processes are working together is critical and our expertise and technology know-how allow us to help bridge the gap between overall citizen experience strategy and the technology you use to deliver that experience.

### **Presidio Highlights:**

Presidio is one of the largest and most adept providers of advanced technology solutions and services. We are passionate about driving results for our clients, delivering the highest quality of products and services to help them unlock the unlimited potential of a completely connected world.



Presidio collaborates with technology vendors who drive innovation and are indisputable leaders of the IT industry. Our significant investment with select strategic partners allows us to achieve broad and deep sets of technical capabilities. Presidio has more than 2,800 IT professionals, 1,600+ of which are highly certified consulting engineers, based conveniently in 60+ offices throughout the U.S. Our 97% client retention rate and double-digit annual growth rates for 15+ years demonstrate our passion for driving client results.

Today, IT organizations face a difficult balancing act. They must focus on planning and deploying technologies to optimize organizational efficiency and reliability, while at the same time managing, operating, and optimizing highly complex, integrated, multi-vendor, multi-platform environments.

Presidio Managed Services offers industry knowledge, robust processes, and best practices to support our clients' daily IT management needs. Collectively, our services will provide West Virginia control and maintenance of your Collaboration environment. With more than 200 experienced professionals dedicated to providing excellent expertise and support for more than 600 clients nationwide. Our team holds a combined 621 technology certifications, allowing us to ensure optimal IT infrastructure services levels.

Presidio's Global Service Desk, the core of our Managed Services operation, has locations in Orlando, Florida and Lewisville, Texas that operate 24x7x365. Our secondary site, located in Hauppauge, New York, operates Monday through Friday from 8 a.m. to 5 p.m. Our Global Service Desk manages 40,000 network devices, 400,000 managed end points, and 3,000,000 unique incidents yearly.

## Proposed Architecture

Based on the information you have provided, our team's architects and engineers have developed the following Architectural Diagram.

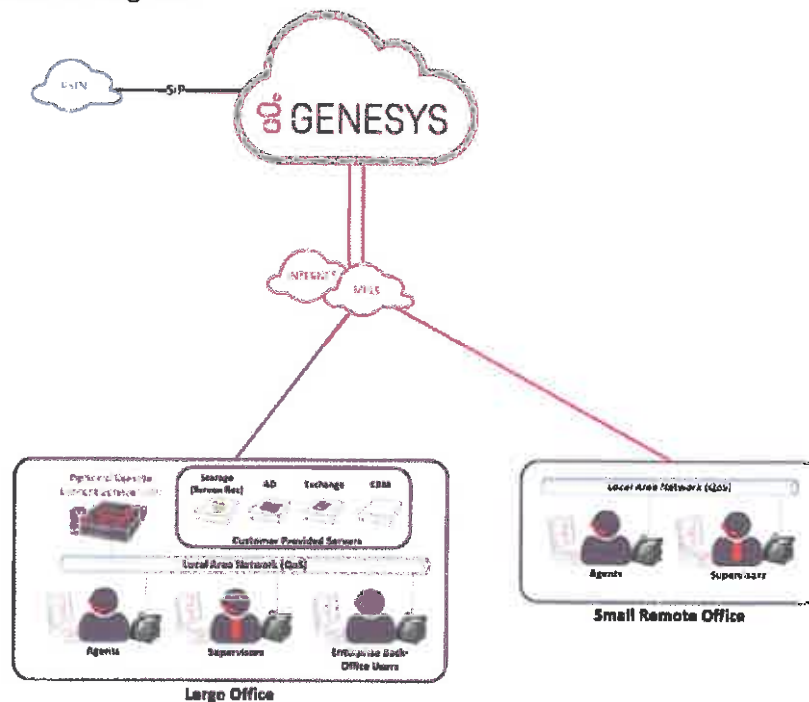


Figure 1: Proposed Architecture

## Impacting the Lives of Everyday People, Every Day

Genesys technology helps State Governments like the SoWV make a positive impact on the lives of their customers... and we have customer success stories that prove it! Please visit [www.genesys.com/about/customer-stories](http://www.genesys.com/about/customer-stories) for more information.

The Genesys Cloud solution meets your combined need for growth and great Citizen Experience with a solution that:

- Integrates with SoWV's current systems
- Supports branded CX delivery
- Deploys as an all-in-one platform
- Provides scalability and flexibility
- Ensures high availability (HA)

The Genesys consolidated solution simplifies the business of being in business. The remainder of this document outlines the details of that solution.

We look forward to advancing to the next stage of your procurement process and welcome the opportunity to present our solution and the value it can bring to your business.



Figure 3: Some of our Genesys Cloud Customers

## References & Past Performance

Genesys powers more than 25 billion of the world's best customer experiences each year. Our success comes from connecting employee and customer conversations on any channel, every day. Over 10,000 companies in more than 100 countries trust our #1 customer experience platform to drive great business outcomes.

PureCloud was released for general availability June 30, 2015. PureCloud is the second generation cloud solution originally developed by Interactive Intelligence and now marketed by Genesys. As of Q4 2017, Genesys has approximately 850 PureCloud customers worldwide to provide leading edge contact center and unified communications functionality.

## Solution Overview

Carahsoft, along with our partners Genesys, Avtex and Presidio will deliver an integrated solution that exceeds the requirements outlined in this RFP. Our solution goes far beyond the basic voice and ACD functionality and addresses bigger picture needs that can only be met by leveraging Genesys's Omnichannel platform and our team's experience.

## Genesys Solution

The Genesys Cloud platform offers SoWV many benefits that help boost customer experience, improve competitive advantage, streamline operations and reduce cost, including:

- **Powerful All-in-one solution.** Genesys Cloud's simple, elegant all-in-one architecture lets you consolidate contact center and business communications infrastructure. Speed up deployment, reduce complexity, simplify administration, improve efficiency and reduce your total cost of ownership.
- **Broad capabilities.** Genesys Cloud offers the most extensive single set of omnichannel and business communications solutions built from the start to work together to connect moments on a single platform. You can add new capabilities and channels quickly and easily with a simple license — without needing to deploy and integrate third-party applications.
- **Improved performance.** By consolidating multiple systems to a single, reliable platform, Genesys Cloud gives you a complete and accurate view of performance across channels, groups and locations — boosting overall contact center productivity.
- **Direct control.** Urgent, non-technical changes no longer require IT. Genesys Cloud offers those leading the contact center direct control over making real-time adjustments to agent groups, contact flows, channels, schedules, and self-service. This allows contact centers to adapt quickly to changing conditions and solve problems faster.
- **Unmatched flexibility.** Genesys Cloud allows you to tailor solutions, services — and even how you pay — to meet your unique business needs, today and in the future. Applications and integrations can be highly customized. Services are tailored to meet the level of involvement that fits your business.
- **Cloud or on-premise deployment.** Genesys Cloud is the only contact center and communications platform recognized as a market leading offer in both cloud and on-premise markets. The same rich customer communications functionality is available in the cloud or on-premise. No tradeoff or compromise necessary. Customers can also migrate between environments with zero impact to users.



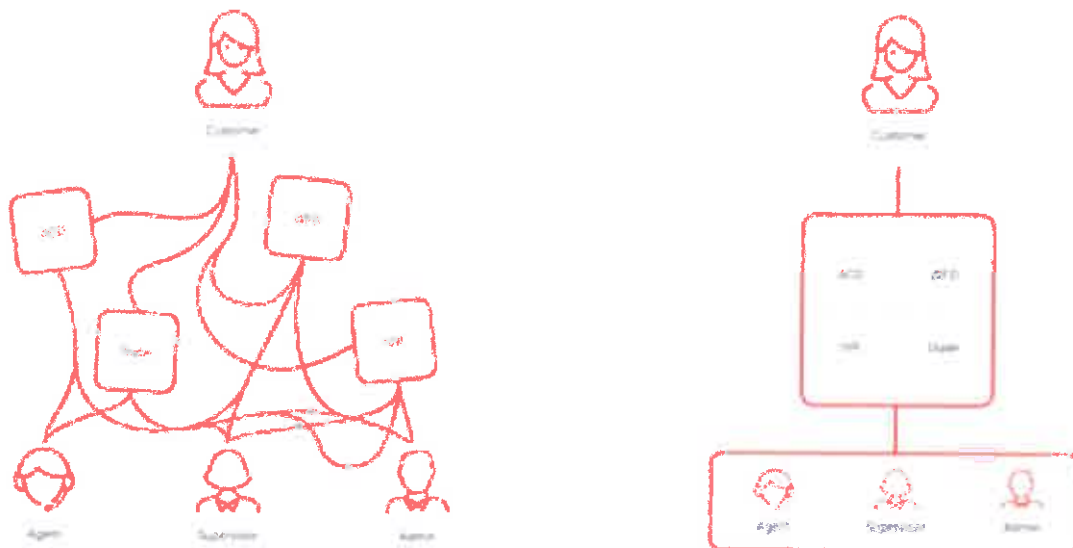


Figure 4: Comparing loosely connected all-in-one vendor solutions vs Genesys Cloud all-in-one platform.

#### Key Capabilities

The key capabilities of the proposed Genesys Cloud solution are:

- **Omnichannel routing.** Customer inquiries of all kinds are delivered in the right order to the most appropriate agent using skills-based routing. This includes calls, web chats, emails, faxes, voice mails, texts, and social media.
- **Self-service.** Callers can perform a variety of self-service functions using either touch tones or spoken phrases. Native speech recognition and text-to-speech is provided, minimizing complexity and cost. Other popular speech recognition systems from companies such as Nuance can be used too.
- **Outbound.** Outbound campaigns for telemarketing and collections make use of powerful predictive algorithms to move quickly through lists and keep agents busy.
- **Workforce optimization (WFO).** A wide variety of WFO capabilities are built-in, including workforce management (WFM), recording, quality management, customer feedback, strategic planning and speech analytics.
- **Real-time speech analytics.** Voice interactions are recorded and analyzed in real-time. Keywords are identified, spotted and scored. Scores are aggregated and displayed. Keywords are bookmarked in recordings to help with evaluations.
- **Real-time supervision.** Supervisors can listen to an agent's call, "whisper" in their ear for coaching, take over the call, initiate a recording, and so on — even if the agent is located thousands of miles away. There's even an iPad app to enable mobility.
- **Analytics.** Every event associated with an interaction processed is logged for a complete view of what happened, beginning to end. A graphical report viewer allows managers to easily create ad hoc reports across every aspect of the operation — contact center, enterprise, branch office and at-home.
- **Built-in Business Communications.** Genesys Cloud offers rich IP PBX functionality, together with basic unified communications features. This includes: IP PBX call processing,

auto attendant, full-featured operator console, desktop phone features, enhanced desktop client features, SIP softphone, real-time presence management, on-demand call recording and monitoring, conferencing, corporate and workgroup directories, embedded call controls for desktop applications, instant messaging, voice mail and unified messaging.

- **Integration.** The open nature of the Genesys Cloud platform enables you to leverage existing investments and easily innovate within our partner ecosystem. The Genesys AppFoundry Marketplace has over 200 applications including pre-built integrations to CRMs such as Salesforce, Oracle Service Cloud, Oracle Siebel CRM, Microsoft Dynamics, and SAP CRM. Additionally, Genesys Cloud APIs make it easy to integrate other business applications as needed.
- **Multi-lingual.** User interfaces are localized in 19 languages. System administration is localized for 10 strategic languages. There are 21 out-of-box language and dialect combinations for system IVR prompts. We support 9 languages with our native speech recognition engine and can integrate with third-party speech engines such as Nuance, for additional languages.

Our all-in-one software solution is based on an open, standards-based, non-proprietary architecture. This software architecture allows us to integrate with other leading software companies. Our software runs on industry standard hardware from HP, Polycom, and AudioCodes. Genesys Cloud also runs on hardware/devices such as virtual server environments.

## **Avtex Solution**

Avtex is an end-to-end CX technology deployment partner that provides professional services (PS) and solutions. Our customers receive unique CX technology deployment delivered with accuracy, consistency and vision specific to their organization to ensure an integrated customer experience for every point of interaction. Avtex provides PS and strategic consulting encompassing a full 360 suite of solutions ranging from unified communications, contact centers, portals, custom applications, infrastructure and CRM. Driven by technology know-how and passionate about customer experience, Avtex is uniquely qualified to help clients deliver exceptional experiences to their customers using technology.

Avtex will help to deliver the proposed Genesys Cloud solution and provide SoWV with the following capabilities:

The proposed Genesys Cloud solution will provide State of West Virginia with the following capabilities. The Project Scope section includes additional details.

- Resident/Citizen Experience Consulting – CX Engagement
- Business User Client Access
- Attendant/IVR less than 30 selections includes 6 queues under 3 routing criteria. Single data dip less than 3 self-service entry read back only add-on.
- Dialer, 1 agent based basic scripting and 1 agentless campaign.
- Recording and Quality Management
- Supervisor dashboard
- Skype server integration – Best effort based on Genesys Cloud and Selected Skype Platform capabilities

- Voice Readiness Assessment for 2 locations plus the Data Center on page 28 of Attachment SO-1 - Avtex - SoWV - Managed and Hosted Voice Services - Base Configuration SOW.
- Development Environment
- Single cutover project

## Architecture Summary

- A geo-redundant design will be provided, leveraging Genesys data centers in Carmel, Indiana; and Denver, Colorado.
- Genesys will provision Genesys Cloud systems in a PCI Zone to support State of West Virginia's requirements for PCI compliance.
- A "Remote Control Media" design is proposed. This is a full-cloud architecture in which a hosted PSTN connection is provided in the Genesys Cloud data centers. The benefit to State of West Virginia is the lack of premise-based hardware and telephony infrastructure to purchase and maintain. A network connection and phone are all that an agent needs to begin using the platform.
- Genesys will provide SIP circuits in the Genesys Cloud data centers for PSTN access.
- An MPLS connection is required between the State of West Virginia and Genesys networks. State of West Virginia will maintain their existing MPLS-carrier relationship and have their carrier bring MPLS circuits into the Genesys Cloud data centers to connect the networks.
- Skype for Business
- End-User Voice Endpoints: AudioCodes, Polycom VVX and SIP Softphones
- Uncompressed G.711 RTP codec will be used for all call paths. If there are bandwidth constraints, licensing for G.729 compression may be added to the system.
- Telephony Port licenses are required for SIP circuits terminating in the Genesys data centers. A non-blocking architecture is based on an agreed-upon need for (910) Telephony Ports to support the required number of simultaneous contact center calls. State of West Virginia will commit to a minimum number of ports in their service contract with Genesys, however the architecture will scale to support periods of increased volume, with overage billed as applicable.
- Remote Content servers will be in the Genesys data centers.
- The Interaction Dialer configuration will include two Central Campaign servers configured in a geo-redundant failover configuration.
- Upon deployment, the Genesys Cloud Services team can provide a one-time transfer of production configuration to the development server. Going forward, there will not be any automatic synchronization, although this is an optional service that Interactive could provide for an additional fee. It is expected that future (applicable) customizations will be completed and tested in development prior to being moved to production.
- 911 Calls
- Standard configuration is as follows: Each user/station location can be assigned an Outbound ANI that is sent to the carrier when a user dials 911. If the carrier can accept a

call “from” the specified ANI, they will route the call to a Public Service Access Point (PSAP). The PSAP must have the correct corporate address on file for the ANI received in order to determine the *general* location of the caller. It is the customer’s responsibility to provide ANI to Location mappings to the carrier.

- Please see Attachment SO-1 - Avtex - SoWV - Managed and Hosted Voice Services - Base Configuration SOW for detailed description.

## Presidio Solution

Presidio is offering the State of West Virginia our Managed Services for providing maintenance and support of the Cisco environment as required by this solicitation and described in Appendix A. As a Cisco Gold partner and Cisco 2018 SLED State and Local Government Partner of the year, Presidio has the credentials and experience necessary to support the State of West Virginia.

Presidio Managed Services is offering our Select tier of service for the State of West Virginia’s Cisco environment until the transition to the fully hosted solution is complete. See table below that provides an overview of Presidio’s Managed Service elements for each of our offering tiers: Standard and Select. Full details of the Select Tier offering for State of West Virginia, is provided in Attachment SO-1 - State of WV-Presidio SOW for Carahsoft (Legacy Cisco UC).

### Presidio’s Managed Services Elements

Element	Overview	Service Tier
Proactive Monitoring and Notification (Alert and Notify)	Monitors events from each device under management and provides notification of specific events to the client. Key events include outages, performance bottlenecks (via thresholds), and security incidents (for security services). Proactive monitoring provides remote advisory services covering performance, availability, and usage information to provide recommendations and best practice suggestions to the client. This covers monitoring status of device/service to prevent future malfunctions or disruptions. Out of Scope: Management of the functional availability of device.	Standard Select

Element	Overview	Service Tier
Standard Reporting	Provides online access to standard reports. This is typically available through self-service portal for each customer. The standard reports are defined within specific tools, such as NimSoft, JasperSoft, and Prognosis. Sample reports include uptime/availability, performance, and usage information.	Standard Select
Online Customer Portal	Provides online access to service ticket information, service status, and event reporting. At this time, the portal does not include order/provisioning functionality; this will be added in future release.	Standard Select
Service Desk (Full Remediation and third-party Triage where applicable)	Covers troubleshooting calls into the Presidio Managed Services service centers for P1 through P3 service calls. Presidio takes on overall ownership of resolving the issue end-to-end. This service desk activity is used to troubleshoot hardware, software, and tools issues applicable to the specific service offered to the client. Where applicable for third-party devices and products, Presidio will collaborate with the specific vendor to resolve the issue for the client.	Standard Select
Quarterly Service Performance Review	This is a regularly scheduled service also known as a Quarterly Business Review (QBR). The review is provided by the Managed Services team to a sub-set of customers. Analyzes incidents and problems that jeopardize Presidio's ability to meet agreed SLA norms. This is not a customer satisfaction survey.	Select



Element	Overview	Service Tier
Telco Vendor Management	<p>Provides operational handling of third-party data and voice carriers. Third-party data and voice carrier is contracted by customer and financial management is by customer. For most customers under management by Presidio, there is a strong telecommunication vendor dependency. This service element enables Presidio to support the Moves, Adds, Changes, and Deletes (MACD) for Telco services on behalf of the customer.</p>	Select
Change Management (Moves, Adds, Changes, and Deletions)	<p>Presidio agrees to provide MACD in the number and frequency specified in the proposal. MACD support is provided to only the equipment specified in the covered equipment list. A single MACD will be defined as one change per device; multiple changes to a single device will be considered multiple MACDs regardless if it is made on the same service request. Presidio reserves the right to determine whether the activity qualifies as a MACD activity.</p> <p>In general, a MACD is any single activity on an individual covered device that meets the following criteria:</p> <ul style="list-style-type: none"> <li>• Activity takes less than 2 hours of time to complete.</li> <li>• Does not require design changes.</li> <li>• Does not include any activity with a material operational impact. (i.e., the change cannot affect the normal operation of the device).</li> <li>• Does not require change control approval.</li> <li>• Is not an upgrade or feature addition.</li> <li>• Is not a project or part of a project.</li> <li>• Is not specifically excluded based on the service portfolio specified in the proposal.</li> </ul>	Select

Element	Overview	Service Tier
Patch Management	Covers "basic" patch management for interim releases of software for each hardware component under management. Urgent security patches are included. Roll-up security patches are not included. For full releases or major dot releases, these require Professional Services to complete the work. Includes 2 interim release updates per year in the base offering.	Select
Smart Hands (Onsite Break/Fix)	Provides scheduling and dispatch of subcontracted Smart Hands resources for break/fix and RMA work. Includes travel time. Also includes scheduling and dispatch to handle incidents relating to equipment not meeting original/agreed specifications of equipment manufacturer.	Select

Presidio's robust Managed Services organization offers State of West Virginia the following:

- Over 200 experienced professionals, with a combined 621 technology certifications, dedicated to ensuring optimal IT infrastructure services levels for more than 400 clients nationwide.
- Service Desk staffed with three tiers of expertise around the clock, allowing State of West Virginia to rest assured that experts are actively managing critical assets. This ensures the State of West Virginia's technology and operational activities are amply and aptly managed, regardless of the time of day
- Dedicated team provides personalized IT operations and support experience, allowing the Presidio team to know customers and their environments and resulting in rapid problem resolution and improved adherence to Service Level Agreements (SLAs).

## REQUIREMENTS RESPONSE

### SECTION 4: PROJECT SPECIFICATIONS

**4.1. Background and Current Operating Environment :** As outlined in the West Virginia State Code §5A-6-4e "the Chief Technology Officer shall oversee telecommunications services used by state spending units for the purpose of maximizing efficiency to the fullest possible extent".

*Additionally, per State Code §5A-6-4a (11), the Chief Technology Officer develops a "unified and integrated structure for information systems for all executive agencies." In pursuance of those objectives, the West Virginia Office of Technology is seeking proposals from Vendors to establish an open-end, Statewide Contract for Managed Voice Services and Hosted Voice over Internet Protocol ("VoIP") Services, encompassing Unified Communications as a Service ("UCaaS"), and Hosted Contact Center Services.*

*It is the State's intent to establish a contract with a single Vendor to provide maintenance, management, and support for the State's current IP Telephony platforms while working to migrate those telephony services to a fully managed and hosted VoIP solution. Additionally, the Vendor will be expected to provide daily management and operational support for multiple Contact Centers while working to migrate those Contact Centers to its hosted solution.*

*Currently, the State of West Virginia has an estimated 10,000 phones on multiple Cisco VoIP solutions - 3x Cisco Unified Call Manager and Unity Express, 4x Cisco Unified Call Manager and Unity, 7x Cisco Unified Call Manager and Unity Connection, 10x Cisco Unified Call Manager and Unity Connection, Cisco Call Manager Express, ten (10) Cisco Contact Center Version 7 sites, and a Hosted VoIP Solution with Verizon Business Solutions (UCaaS and Contact Center); it is anticipated all of those sites currently utilizing a VoIP solution will be migrated to the Vendor's proposed hosted solution. In addition to the current VoIP Agencies, the State also requires the flexibility to implement a VoIP solution at sites where one does not currently exist. Potentially, the State may leverage the awarded contract to implement another estimated 10,000 users where traditional telephony services exist.*

*The State of WV's current environments consist of the following:*

- Cisco Unified Messaging
- Cisco Unity Connection
- Cisco Unity Express
- Cisco Call Manager Express
- Cisco Contact Center Express
- Cisco Expressway C&E
- Cisco Presence
- Cisco Jabber
- Cisco Gateways using VoIP Session Initiation Protocol ("SIP") Trunks, Primary Rate Interface ("PRI") Circuits, and Analog POTS ("Plain Old Telephone Service") lines
- Microsoft Skype for Business 2016
- Microsoft Active Directory
- Microsoft Office 365
- Cisco Survivable Remote Site Telephony ("SRST")
- Bridge Communications Operator Console

- Singlewire Informacast Paging
- Verizon hosted solution- Unified Communications and Collaborations as a Service (UCCaaS)
- Verizon hosted solution - Virtual Contact Center (VCC)

*More information regarding the State's current telephony infrastructure can be found in Appendix A.*

*Meanwhile, the State's current Wide Area Network ("WAN") is undergoing a conversion from Switched Ethernet to Multiprotocol Label Switching ("MPLS") services, which may impact how the Vendor's proposed solution will be implemented. The WVOT is working with Verizon Business to migrate an estimated 500 data circuits across the State with a projected completion of December 2018. Thus far, approximately 275 circuits have been migrated, meaning that the proposed VoIP solution may be implemented at those sites using MPLS circuits to ensure quality of service. The State has deployed Cisco routers for WAN communications. Local Area Networks ("LANs") are comprised of various switches manufactured by Cisco, Hewlett Packard, Brocade, and Extreme.*

Genesys has read and understands.

**4.2. Project Goals and Mandatory Requirements:** *The State of West Virginia is seeking to establish a contract with a Vendor for the management of the State's current Legacy Environment and to migrate its Legacy Environment to a Hosted VoIP Solution, including Contact Center Services. Vendor should describe its approach and methodology to providing the service or solving the problem described by meeting the goals/objectives identified below. Vendor's response should include any information about how the proposed approach is superior or inferior to other possible approaches as well as identify areas where the proposed solution exceeds the project expectations.*

**4.2.1. Goals and Objectives –** *The project goals and objectives are listed below.*

**4.2.1.1 Voice Services**

**4.2.1.1.1 Managed Voice Services - Support of State's Legacy IP Environment**

**4.2.1.1.1.1** *The State's goal is to contract with a single Vendor for all application, hardware, and MACD management, maintenance, and support of its current IP Telephony platforms (as described in Appendix A), with the goal of the Vendor migrating the State's current IP telephony infrastructure, excluding network infrastructure, to a unified, hosted IP platform within 24 months. The State further desires an economical monthly per phone cost for these support services. As such:*

*The State is proposing the following division of duties for the support of its Legacy IP Environment:*

**Vendor Duties:**

1. *Create an operational plan of the State's Legacy IP Environment for the State's review and approval*
2. *Daily management, operational support, and ongoing maintenance of the State's current telephony environment, as outlined in Appendix A.*

Vendor will provide the following management and operational support elements:

- 24x7x365 Access to Service Delivery Center (NOC)

- 24x7x365 Monitoring
- Client Portal
- Standard Reports
- Change Management
- Move, Add, Change, Delete (MACD)
- Problem Management
- Patch Management
- Dispatch Services
- Vendor Management
- Carrier Case Management

Ongoing maintenance (Cisco SMARTnet) will be maintained by the State for all eligible devices. All end-of-life/end-of-support equipment is supported on a business reasonable-effort basis.

**3. *MACD changes to the State's current telephony infrastructure.***

Presidio offers Request Management for Managed Configuration Items (CIs) for the State's current Cisco telephony infrastructure. The MACD process provides a model for managing and executing moves, additions, changes and deletions of hardware and software configuration items in the Client's environment. MACD service is defined within two categories: 1) Device-level changes and 2) User changes per contracted UC/Collaboration services. Definitions for each category are provided below with additional details for contracted services within the Service Appendices (if applicable).

**Device Level Changes**

Device-level changes are defined as configuration requests that typically impact multiple users based on the change, such as configuration. Presidio reviews the Contract for each device level request and determines if it falls outside of the scope as defined below:

1. Takes less than 2 hours of time to complete.
2. Does not require planning or design efforts.
3. Does not include any activity with a material operational impact. (i.e., the change cannot affect the normal physical operation of the device).
4. Is not an upgrade or feature addition.
5. Is not a project or part of a project.

For changes not covered by this agreement, Presidio provides a separate Contract from Professional Services. Device-level MACD support is only provided to equipment specified in the CEL.

A single device level change (MACD) is defined as one change per device; multiple changes to a single device are considered multiple MACDs regardless of whether it is made on the same service request. Presidio reserves the right to determine if the activity qualifies as a MACD activity. Device level MACD work does not apply to the Security Incident and Event Management Service which is defined in the separate contract.

For device-level changes, up to two changes per CI per month are allowed. Changes are allotted monthly and must be used during the target month of service. Any change allocations remaining at the end of a service month are considered forfeited and do not roll to subsequent service months.



### User Changes

A User Change is change for Collaboration services impacting any single user-based configuration, including remote moves, additions, changes or deletions; e.g., a request to add/delete a user profile.

The MACD option for the Users must be included in the covered device list for Presidio to perform user changes. The monthly allotment of MACDs is 5% of the managed Users per month and requires 100% of managed Users to be covered in agreement.

Presidio tracks the MACD tickets for the 3-month period and notifies the Client of trends. If the average MACD counts are exceeding the target limits, it may show evidence of an operational or training issue Presidio can address with the Client. If no operational issues exist and the MACD requests from the Client normally exceed the 5% limit for Users by more than 10%, Presidio will work with the customer to adjust the billing for user changes.

4. *Replacement of failed parts where feasible, outdated telephony equipment, or other telephony components. If the Vendor is unable to furnish parts or replace equipment, the State expects the Vendor to migrate that site to the Vendor's Hosted VoIP platform.*

Presidio provides support of all end-of-life/end-of-support equipment is on a business reasonable-effort basis.

Avtex will work with the State to reprioritize deployment of users to the new Hosted VoIP platform that may be impacted by failed equipment on the legacy system.

5. *Set-up mutually agreed upon standing meetings with the State to address concerns, changes, service interruptions, and project progress.*

Read and comply as it relates to the State's current Cisco telephony environment.

6. *The Vendor should alert the State points of contact after being notified of any service interruptions, in writing, that exceed sixty (60) minutes. The Vendor should provide updates to the State every sixty (60) minutes thereafter until the issue is resolved.*

Avtex will notify the State in writing of interruptions that exceed 60 minutes and continue to update every 60 minutes as requested.

7. *The Vendor should have a 24x7x365 operations center that includes Tier 1 support to receive trouble tickets and onsite operational support for critical failures.*

Understood. Attachment 4.2.1.1.1.1-7 - Avtex - State of West Virginia Support Handbook describes the support offering in detail. Where Avtex offers multiple offerings, the proposed solution includes Premier enhanced with Managed Services MAC and Tier 1 services.

Presidio's Service Delivery Center (SDC) is the central point-of-contact to Presidio Managed Services for daily support activity and is also generally referred to as the Network Operations Center (NOC). It is the main point of contact for reporting incidents (disruptions or potential disruptions in service availability and/or quality) and for Clients making service requests (routine requests for services). Presidio's Service Delivery Center team is staffed 24 hours a day, 365 days a year in three US-based locations.

The SDC will deliver Tier 1 through Tier 3 technical support using Presidio's Information Technology Infrastructure Library (ITIL)-based processes. This support assumes that the State has an end-user help

desk in place to handle end-user calls and only authorized technical contacts will contact the Service Delivery Center. Presidio defines technical support levels as follows:

**Tier 1: Technician Support**

The Service Delivery Technician (Tier 1) is responsible for effective Client service support using workflow and incident management tools. Tier 1 technicians follow Presidio's standard ITIL-based processes, as well as specific Client processes as defined by Service Delivery Management. Technicians utilize our incident management system to manage the incident queue for resolution or follow up, interface with Tier 2 engineering for advanced engineering support as needed and maintain Client communication during escalations. Initial support for basic Client issues is supported at Tier 1.

**Tier 2: Engineering Support**

The Service Delivery Engineer (Tier 2) is responsible for effective Client service using advanced engineering skills. Tier 2 engineers use defined ITIL-based processes for effective Incident and Change Management. In addition, the engineer interfaces with vendor support engineering or Presidio Professional Services to provide timely resolution.

**Tier 3: Advanced Technical Support**

Tier 3 is the highest level of support in a three-tiered technical support model responsible for handling the most difficult or advanced incidents and overseeing problem management for Clients.

The Client may communicate incidents to the Service Delivery Center using the following methods (in addition to auto-generated incidents):

- Telephone (P1 Incidents must be opened via a call into the SDC)
- Opening a ticket on the Client Portal (defaults to a Priority 4 incident)
- Email (defaults to a Priority 4 incident)

Client personnel contacting the Presidio SDC must be authorized to do so as defined in the Run Book. The Run Book is a set of defined procedures developed during the Service Transition Management process for maintaining the everyday operation of the Client environment. The SDC cannot respond to support requests from non-authorized personnel and will not engage with the Client through indirect methods for incident notification. Client personnel authorized to contact the SDC must be qualified to interact on a technical basis at a level required to support efforts by Managed Services.

Once an incident has been opened, an email notification will be sent to the caller and all contacts subscribed to receive notifications that match the conditions of the incident.

***State Duties:***

1. *Management of State's LAN/WAN Network Infrastructure*
2. *Ordering, disconnecting, and billing services*

Read and understood.

**4.2.1.1.1.2** *The State desires the Vendor provide the State with its proposed Operations Plan within 30 calendar days of contract effective date, outlining its plan for managing, supporting, and maintaining the State's current IP telephony infrastructure.*

*The Vendor's Operations Plan should include a strategy for assuming its duties, as outlined above. Please describe your company's experience and strategy in developing operations plans for supporting legacy environments.*

Avtex is prepared to provide the project plan in the time outlined.

**4.2.1.1.1.3** *The State desires that the State and Vendor finalize and agree upon an Operations Plan within 60 calendar days of contract effective date for the management, support, and maintenance of the State's current telephony infrastructure. Please describe your company's ability to deliver the finalized Operations Plan to the State within 60 calendar days of contract effective date with scheduling the appropriate meetings, making changes after State input, and meeting deadlines.*

Yes, the typical Avtex project will transition from the "Initiate & Design" phase to "Build" phase within 60 days. Without extraordinary circumstances, the Avtex average project runs 24-36 weeks.

**4.2.1.1.1.4** *The State desires the Vendor to be fully managing its Legacy Environment within 90 calendar days of contract effective date and until all sites wishing to adopt these services have been migrated to a Hosted VoIP solution. Please describe your company's experience in providing support of a Legacy Environment, its experience in taking over existing infrastructure, and provide a plan showing how this goal can be met.*

Avtex understands that the legacy system will be transitioned to Avtex and Presidio support within the 90-day period.

Please see Attachment 4.2.1.1.1.4 - Presidio Service Transition Management.

**4.2.1.1.1.5** *It is the State's desire that the awarded Vendor of this contract will establish a local support system to continue support and maintenance of the State's Legacy IP systems. Please describe your company's ability to provide maintenance and support of the State's Legacy Environment.*

Presidio has the capability to support the legacy Cisco environment as we have supported these systems for over 15 years. In the event any of the legacy equipment is no longer supported by the OEM, Presidio will provide commercially reasonable efforts to support that equipment but will be limited where the OEM no longer offers replacement hardware and software patches and updates.

**4.2.1.1.1.6** *The State desires all application, hardware, and MACD support for the State's current telephony infrastructure will be entered via the Vendor's self-service web portal and/or a Vendor-provided toll-free number within 90 calendar days from contract effective date. If the Vendor determines that an issue or problem falls within the State's purview, the Vendor should notify the State's points of contact in writing within one hour of reaching this determination. Please describe your company's support offerings or its ability/plan to accomplish this.*

Please see Attachment 4.2.1.1.1.4 - Presidio Service Transition Management.

Please see Attachment 4.2.1.1.1.1-7 - Avtex - State of West Virginia Support Handbook.

**4.2.1.1.2 Transition from the State's Legacy IP Environment to the Vendor's Hosted Solution**

4.2.1.1.2.1 The State desires all sites listed in Appendix A be migrated to a Hosted VoIP solution within 730 calendar days from contract effective date. The State reserves the right to reprioritize this list as necessary. Please describe your company's plan to accomplish these migrations.

Avtex fully understands the 730-day migration requirement.

4.2.1.1.2.2 The Vendor should include site preparation and coordination services to implement a turn-key solution at various State locations, including simultaneous deployments to the Vendor's hosted solution. These services should be provided by Vendor personnel knowledgeable in both the Vendor's solution and legacy public switched telephone services. The State desires the Vendor perform site assessment and readiness work for the implementation of its hosted solution, at no additional cost, including a proposed division of duties (Vendor, State), which results in a Statement of Work for each site, as follows:

The implementation of the proposed Genesys Cloud Hosted Solution includes one to many sites to be assessed, implemented and cut over at the same time. Adding additional sites to the initial implementation will use the TCR process. The provided estimation calculator (Attachment 4.2.1.1.2.2 - West Virginia Additional Sites Calculator) should be used to estimate the secondary site implementations. The calculator was used to establish the fixed cost of the Small Site Option (see our response to 4.2.1.1.3.7).

**VENDOR duties:**

- Gather site's end-user data in order to get site ready for Vendor's hosted solution;

Understood; this occurs in the Initiate and Design phase of the implementation.

- Provide list of equipment/specifications needed for site readiness, including cabling infrastructure requirements;

Understood; Initiate and Design phase.

- Conduct review to move, at a minimum, existing telephony system to new environment;

Understood; Initiate and Design phase.

- Provide the State with necessary ordering information for TCRs;

Understood, the TCR process will be followed for the entire project.

- The State owns all data gathered under the scope of the contract and is able to obtain copies of all configuration files gathered as part of this contract. The Vendor should update, maintain the data repository in a manner negotiated with the State upon award, and provide information upon request in an Excel or csv format;

Understood; Initiate and Design phase.

- Configure, tag, label, and drop-ship phones to site;

Understood; Build phase.

**STATE duties:**

- *Confirm site readiness;*

Understood, Build phase.

- *Coordinate between the Agency, Vendor, and other applicable parties;*

Understood, entire project.

- *Purchase, configure, update and refresh network hardware;*

Understood; Build phase and entire project.

- *Prepare, process, and submit TCR to Vendor based on information provided;*

Understood; entire project.

- *Place physical phones.*

Understood; Build phase.

*The Vendor should describe its solution's capability to meet or exceed each of these objectives.*

Please see our responses above.

**4.2.1.1.3 Hosted Voice Services**

*The State's goal is to obtain a reliable, customizable, and scalable UCaaS solution providing hosted voice-over-IP (VOIP) services for an estimated 10,000 state employees located at various sites throughout the State. The State desires these services be provided at no additional cost, except where noted in this section. To that end:*

*4.2.1.1.3.1 The Vendor's solution should offer four voice packages. These packages should include: A Basic Package with at least Ad Hoc Conferencing, Call Forwarding, Call History, Call Hold, Call Waiting, Caller ID, and Do Not Disturb; an Enhanced Package including at least all features in the Basic package plus Voice Mail (including Immediate Divert to Voicemail and Message Waiting Indicator); a Premium Package including at least all of the features in the Enhanced Package plus Extension Mobility; and an Analog line option. All packages should be available with high and standard security options. Equipment for the analog line package will not be required for this contract.*

*Please describe your Company's offerings.*

Avtex understands the four voice packages requested.

Genesys has provided pricing in Attachment A - Genesys Pricing Addendum. The Basic Package includes and is the same price as analog, Enhanced and Premium.

The Genesys Cloud can support Ad Hoc Conferencing, Call Forwarding, Call History, Call Hold, Call Waiting, Caller ID, Do Not Disturb, Voice Mail (including Immediate Divert to Voicemail and Message Waiting Indicator), Extension Mobility; and an Analog line option. Offers will be made to support these in different packages.



*4.2.1.1.3.2 The State desires six handset options for use under this contract: a 2-line phone, a 5-line phone with sidecar capabilities, a conference phone, a softphone, a wireless phone, and an ADA-compliant hardware option. The State further desires a leasing option for all handsets on this contract, by which the State will pay a monthly lease price to be added to the price of the monthly voice package. In the event that a phone is broken or stops functioning, the State desires the Vendor replace that phone, at no additional cost. Additionally, the State desires that the Vendor refresh equipment in-line with the Original Equipment Manufacturer's refresh program, at no additional cost. At the end of the contract, the State will own all of the phones. Please describe your company's leasing options, refresh programs, and ability to meet this goal.*

Pricing is reflected in Attachment A - Genesys Pricing Addendum.

*4.2.1.1.3.3 The State utilizes Cisco SRST and local voice services in case of data network failure. At the initial deployment of the site to the Vendor's hosted solution, if requested, the Vendor should work with an Agency to implement call control and PSTN connectivity, in case the data network fails at a State location. This should include the provisioning of at least one local phone line for 911 calling. The Vendor should include the provisioning of one failover line in the cost of its monthly package. If the site requests more than one failover line, the State understands there may be additional charges for that work.*

Avtex understands that SRST will be implemented for agencies that request the functionality through TCR.

We can configure Genesys Cloud to comply with Cisco SRST and local voice services in case of data network failure. 911 functionality must be handled by the Cisco SRST and/or local voice services at all times to support e911 functionality.

*Please describe your solution's ability to meet this goal and any additional costs.*

Typically, customers terminate circuits (or utilize the Genesys PSTN offering) for each Genesys Cloud region data center pair. In this case, the region is the USA. Customers can provision for separate circuits for outbound as required based on telephony design for that customer. Each Genesys Cloud region is set up with twin data center facilities (Regional Pairs). Each site is scaled to handle the full call load for its Region, and as such each can serve as a full backup for the other. With wide geographic dispersion, risk of simultaneous outages is minimized. If an issue with PSTN connectivity arises in one facility, the traffic is shifted to the other facility until the issue is corrected.

*4.2.1.1.3.4 The Vendor's solution should support station-to-station calling that remains "on-net" (on the State's private data network) at no additional cost. Please describe your solution's ability to meet this goal.*

Genesys Cloud uses MPLS to achieve station-to-station calling as "on-net" to link agents to the core Genesys Cloud. In this way, all calls are handled within the controlled network and no external calling is required.

*4.2.1.1.3.5 The Vendor's solution should provide at least two PSTN connections via SIP Trunks over secure private connections engineered for voice quality of service. These PSTN connections should adhere to the industry standard of 150 ms latency or better, and jitter of 40 ms or better. Please describe your network engineering architecture and your practices to continuously achieve these standards.*

Typically, customers terminate circuits (or provision Genesys PSTN) for each Genesys Cloud region data center pair. Customers can provision for separate circuits for outbound as required based on telephony design for that customer. Each Genesys Cloud region is set up with twin data center facilities (Regional Pairs). There are two Genesys Cloud datacenters in Indiana and Colorado. Each site is scaled to handle the full call load for its Region, and as such each can serve as a full backup for the other. With wide geographic dispersion, risk of simultaneous outages is minimized. If an issue with PSTN connectivity arises in one facility, the traffic is shifted to the other facility until the issue is corrected.

The Genesys Network is designed to maintain a MOS score of 3.5 or better by limiting the latency and jitter that impacts voice quality.

*4.2.1.1.3.6 The Vendor's solution should provide a MPLS network connection to Verizon's MPLS core to reduce and/or eliminate the backhaul of traffic to the State's core network. The State has provided a column on the Attachment A Cost Sheet for both one-time installation costs and for monthly recurring costs for these connections. Please describe your ability to meet this goal.*

Genesys Cloud provides telecommunication and long-distance services from preferred providers L3 and Verizon, and MPLS data services from L3. Additionally, Customers can bring their own MPLS if preferred.

*4.2.1.1.3.7 As an option for small sites with non-private network handoffs, the State desires a solution utilizing public networking with the ability to securely transmit sensitive data. Please describe any offerings to support this goal.*

The Genesys Cloud supports small sites with non-private network handoffs. The Genesys Cloud secures/encrypts the data transferred between the core cloud infrastructure and the end interfaces used by the agents.

There are multiple options allowing the delivery of voice using the public internet. While not in scope these options include the use of Skype for Business endpoints and Microsoft Edge, Session Border Controllers and NAT Traversal and the use of Genesys Cloud WebRTC. Native Genesys WebRTC is a roadmap item.

*4.2.1.1.3.8 The Vendor's solution should include Caller ID services (inbound traffic) and custom number and naming (outbound traffic) that State Agencies may utilize to customize their displayed information. The Vendor should provide this capability at no additional cost. Please describe your solution's ability to provide these services.*

Genesys Cloud supports both features.

*4.2.1.1.3.9 The Vendor's solution should include unlimited local and nationwide calling at no additional charge. Please describe your no cost offerings.*

Genesys offers flexible Telephony arrangements (Inbound & Outbound) or MPLS circuits with its cloud solution offering. All can be provided by either Genesys or the State. While Genesys has not included unlimited local and nationwide calling at no additional charge, Genesys would welcome the opportunity to identify strategic areas where we could make our offer more economically beneficial to the State.

This could include, but not limited, to a volume usage arrangement based upon a minimum telco commit, tier discounting, or potential flexible overage options. Genesys telco usage is typically billed as follows:

Domestic U.S. Outbound and Inbound Call Traffic established over PSTN is billed at \$0.012 per minute (billed in one second increments.)

Intrastate Call Traffic is billed at \$0.0151 per minute (billed in one second increments.)

Please see Attachment A - Genesys Pricing Addendum.

*4.2.1.1.3.10 The Vendor's solution should provide international calling. The State understands fees may be associated with international calling. The Vendor should provide its per minute international calling rates for Mexico, Canada, and Jamaica in the Attachment A Cost Sheet. These will be used as part of the cost evaluation. The Vendor should also attach an appendix of its international calling rates for all countries. This appendix will be used to establish the international calling rates per country in the awarded contract and will be required prior to award. Please describe your solution's international calling offerings.*

Genesys supports this functionality.

*4.2.1.1.3.11 The Vendor's solution should provide comprehensive site coverage to meet the State's local and long-distance IP-based calling requirements. Please describe your coverage, as well as how you plan to meet the State's coverage needs.*

Genesys can support 10 and 11-digit long distance phone numbers.

*4.2.1.1.3.12 The Vendor's solution should provide load balancing for all traffic in-bound from the PSTN. Please describe your solution's ability to meet this goal.*

To support voice load balancing, Genesys Cloud terminates carrier circuits at multiple Genesys Cloud GTNs or POPs. We rely on the carrier to perform the load balancing for incoming calls. Genesys provides load balancing for outgoing calls through our call routing technology using the Genesys SIP Server.

*4.2.1.1.3.13 The Vendor's solution should ensure 911 call delivery to the appropriate local PSAPS. Additionally, the State desires support for Private Switch/Automatic Location Identification (PS/ALI) services for 911 calls. Please describe your process for ensuring the accuracy of 911 call delivery, as well as the process to support PS/ALL*

With the Genesys Cloud, there is no local footprint to support appropriate local PSAPS or Private Switch/Automatic Location Identification (PS/ALI) services for 911. 911 services must be supported by a local line at the facilities.

*4.2.1.1.3.14 The Vendor's solution should support the following industry standard protocols: G.711 (uncompressed), G.729 (compression), and T.38 (fax). Please describe the protocols supported by your solution.*

Genesys Cloud supports G.711 and G.729 compressed audio calls end-to-end. Re-negotiation from the higher bandwidth G.711, which is more suitable for IVR calls, to a compressed G.729

call for agents, is fully supported. This allows administrators to fine-tune cost, quality, and WAN utilization. Inbound and outbound capabilities are provided.

*4.2.1.1.3.15 The Vendor's solution should have the ability to scale the number of simultaneous concurrent calls on a monthly and/or seasonal basis at the State's request. Please describe your solution's ability and your process to accomplish this, including division of duties.*

With the Genesys Cloud solution, agents can place a caller on hold and then dial out to either another team member or external vendor. Once connected to the third-party, the agent can either transfer the call or conference the third-party on with the customer to continue the interaction.

The Genesys Cloud solution is provisioned for robustness and flexibility to allow our customers with seasonal high call rate demands (regulatory deadlines, retail, health care open enrollment, etc.) to 'burst' beyond their prescribed configuration and allow for increased simultaneous concurrent call volumes. The customer merely pays for what they have consumed in any given month. If there are known seasonal calling patterns, whether specific months or timeframes, Genesys will work with the State to build these periods into the formal contract agreement to ensure that we engineer the Cloud solution to the State's forecasted requirements with complete availability.

Please see Attachment A - Genesys Pricing Addendum.

*4.2.1.1.3.16 The Vendor's solution should include interoperability with the following: IPv4 addressing (RFC 791), RFC 1918 for private IP addressing, and support SIP over TCP or UDP. Carrier grade NAT (RFC 6598), link-local IP addresses (RFC 3927), and Multicast addresses (RFC 3171) will not be accepted. Please describe your solution's interoperability to accomplish this goal.*

Genesys Cloud communication protocols used with external systems are all Transmission Control Protocol (TCP). This includes SIP and RTP over TCP.

*4.2.1.1.3.17 The Vendor's solution should provide the following quality and reliability standards: QoS tagging IEEE 802.1Q2011; not rewriting, marking, or remarking any VLAN tags affixed to packets by the State, without the State's expressed consent; at a minimum, one Class of Service (COS) marking per Ethernet service. Please describe your solution's ability to meet this goal.*

Genesys Cloud supports QoS settings on the level of the network and the local station's Windows operating system. This support allows administrators to configure policies to mark all the packets sent by a particular application with the desired level of service.

In addition, the Genesys portion of the platform has QoS applied at all levels of the transaction. Information can be given to customer for the QoS settings needed on the customer's networks.

Genesys Cloud products use Differentiated Services (DiffServ), and Class Selector PHB in some cases, to mark packets on an IP Network. RTP Packets, which use UDP, and SIP Packets, which through configuration can use UDP, TCP, or TLS, are QoS marked by the endpoints. The QoS markings are in the 6-bit DSCP field of the ToS Byte of the IP header. The recommended (Default) value for RTP (voice) is 101110, which is EF / Expedited Forwarding. The recommended (Default) value for SIP Signaling is 011000, which is CS3 / Class Selector.



*4.2.1.1.3.18 The State desires a Unified Messaging solution; therefore, the Vendor's solution should fully integrate with Microsoft 0365, allowing users to listen, forward, and delete voicemails from both 0365 and the hosted environment. Voicemails should be retained in the solution for 15 days or longer. In addition, the Vendor's solution should be provisioned to fully integrate with the State's Active Directory and Active Directory Federated Services. Please describe your abilities to meet these goals.*

The Genesys Cloud supports the ability to integrate with AD in the customer's environment. In addition to this, the Genesys Cloud can utilize Microsoft's 0365 Skype for Business (S4B) to deliver the voice path from the Genesys Cloud to the agent alleviating the need for an additional hard phone.

Voicemail is retained in the Genesys Cloud for a configurable amount of time.

*4.2.1.1.3.19 Some State Agencies utilize paging and notification to the PC desktop, over-head paging, or through-the-phone-speaker paging. The Vendor's solution should include an option for providing, maintaining, and supporting a paging solution, including any associated hardware, software, and licenses, and if requested by Agency, or integrate with an existing or Agency-owned paging solution. The State understands there may be fees associated with this offering. Please describe your offerings with respect to these deployments.*

The Genesys Cloud allows for notifications to be sent to the agent's desktop. The phone device is not used in this functionality.

Zone paging is supported with Polycom phones.

*4.2.1.1.3.20 The State desires an option for Agencies with high call volume and receptionist personnel that will utilize an Operator Console for fast and efficient call control. The State understands there may be fees associated with this offering. Please describe your solution's Operator Console offerings.*

No additional fees for this feature, it is included in the agent price for our Genesys Cloud offer.

*4.2.1.1.3.21 If requested by an Agency, the State desires the ability to integrate a third-party call recording solution with the Vendor's hosted solution. Please describe your solution's ability to meet this goal.*

Any third-party recording solution can integrate with Genesys Cloud. Verint is a company on our pricelist that we have integrated with in the past.

*4.2.1.1.3.22 The State desires that the Vendor use currently-owned State IP telephony handsets where the handset is still supported on the Vendor's solution. Please describe your company's ability to use the State's current handsets and its ability to meet this objective.*

Genesys Cloud can use any headsets that you currently use with your PCs.

**4.2.1.1.4 Hosted Contact Center Services**

**4.2.1.1.4.1** *The State's goal is to obtain a reliable, customizable, and scalable solution to provide hosted contact center services for an estimated twenty-five (25) individual contact center sites that works in conjunction with the Vendor's proposed Hosted VoIP solution. Certain sites require the capability to transmit and/or store call recordings that may contain sensitive data (such as PHI or PII). For ease of deployment and maintenance, the State prefers the contact center solution be web-based. The solution should provide the following capabilities:*

- *Ability for a simple, drag-and-drop, easy-to-understand interface to create customized call routing and role-based queues that can be deployed to sites with non-technical administration*

Genesys Cloud includes drag-and-drop based tools to create customer self-service applications/IVR applications and assisted service (Routing) applications that run on the Genesys platform.

The Genesys Cloud provides easy to use, highly functional blocks that enable common tasks in a simple and straightforward manner. The Genesys Cloud utilizes a drag and drop approach where the developer can simply drag the desired block from the Palette menu into the call flow (Application Flow) to build self-service applications.

The Genesys Cloud provides layered access roles ensuring that your users only have access that is appropriate for your business needs — such as the ability to make changes to prompts, business hours, or set an emergency routing flag — without exposing control to the overall application logic.

- *Should provide chat capabilities*

Genesys Cloud Chat application lets your agents provide live assistance to constituents via the web. The chat interactions are managed by the same business rules that are applied to all other contact channels and enables integrated monitoring and reporting. Chat interaction management also gives agents access to the same customer data they have for other channel interactions, providing constituents the same personalized service regardless of the media used for contact and reducing handling times.

- *Should provide live data reporting*

The Genesys Cloud provides performance dashboard solutions that offers contact center managers and supervisors real-time access to key performance indicators. The dashboard includes pre-defined widgets that can be configured by authorized users. These may be present any object across any channel.

- *If requested by an Agency, the solution should have the ability to interface with an Agency's database to populate information based on data provided by the caller*

Genesys Cloud supports integrations with many third-party solutions, development architectures, and custom client applications using a RESTful (Representational State Transfer) Application Programming Interface (API). The integration framework provides web services and APIs to support a broad range of integrations with third-party solutions across interaction services, data services, and agent services. The Cloud solution also provides productized adapters for leading CRM providers, including Salesforce.com and Oracle Service Cloud as well as supporting URL-based screen pops for browser-based solutions, managed as part of the call-attached data.



- *If requested by an Agency, the solution should provide the flexibility for agents to use a public-switched- telephone-network (PSTN) phone to utilize the solution*

Typically, customers terminate circuits (or provision Genesys PSTN) for each Genesys Cloud region data center pair. Customers can provision for separate circuits for outbound as required based on telephony design for that customer. Each Genesys Cloud region is set up with twin data center facilities (Regional Pairs). For example, in the US there are data centers in Colorado and Indiana. Each site is scaled to handle the full call load for its Region, and as such each can serve as a full backup for the other. With wide geographic dispersion, risk of simultaneous outages is minimized. If an issue with PSTN connectivity arises in one facility, the traffic is shifted to the other facility until the issue is corrected.

- *Should provide scalability for up to 800 agents and the ability to expand in the future*

The Genesys Cloud capacity is planned and constantly managed to meet the needs of all our customers. We are always able to handle the capacity of our customers. We do require our customers to inform us of their usage. Although bursting above agreed traffic is allowed, it is better to advise Genesys as to your maximum usage.

*Please describe your solution and identify any areas in your solution that exceed the items requested above.*

Genesys Cloud can scale to tens of thousands of agents and is built into a telephony infrastructure to supply industry leading security and reliability.

*4.2.1.1.4.2 Some of the State's call centers operate on a 24x7x365 basis, delivering critical services to the communities. As such, the State prefers the Vendor's solution have inherent redundancy and survivability characteristics that will ensure minimal service disruptions, such as data centers in geographically diverse regions allowing for failover, equipment and power redundancies in those data centers, etc. Please describe your solution's redundancy and its ability to meet and/or exceed this goal.*

The Genesys Network Operations Centers control and monitor all Genesys Cloud service 24/7/365. Genesys uses a distributed performance and availability monitoring solution that covers all aspects of the SaaS infrastructure. The system is capable of monitoring Genesys components as well as specific connectivity to client systems, including the MPLS network, circuits, and application servers, based on the specific deployment model. The monitoring system offers advanced alerting and visualization to allow us to obtain notification of any issues and immediately begin taking appropriate action.

*4.2.1.1.4.3 The Vendor's solution should include enhanced features for Administrators, Supervisors, and Agents to effectively meet the needs of their customers. As such, the solution should provide the following capabilities:*

- *Agent and Supervisor client that provides Blended agents: Inbound and outbound capability*

The Genesys Cloud solution supports multimedia queuing and routing that allows queuing of non-voice interactions along with live calls, queue callback requests, and queued voice messages.

The concept of a "Universal Queue" allows an enterprise to route all incoming customers, regardless of channel, through a single, integrated queue.

With Genesys routing, administrators can configure capacity rules to allow one advisor to handle one voice interaction at a time or/and multiple off-line interactions (email and chat) at the same time. Capacity rules make it simple to define and configure the simultaneous offline sessions allowing agents

to handle as many offline sessions as the administrator configures. For example, this allows administrators to configure the agent's capacity to handle four to five simultaneous emails, or one voice call.

Genesys Cloud also supports multimodal interactions; the cloud can update calling lists or send SMS to the customer using the Genesys Outbound cloud.

- *With your cloud solution, in a blended queue, do inbound calls override an outbound preview calls prior to the dial being initiated:*

Inbound calls can take precedence over outbound calls if desired. All priorities in the platform are configurable and controlled by the customer.

- *Ability to monitor critical performance metrics allowing managers to coach, train, and encourage agent behavior*

The Supervisor Desktop supports Genesys Cloud Chat functions via agent group views. Supervisors can select an enabled for chat agent and monitor the next interaction. Supervisors can silently monitor, whisper coach, or join in on a chat session, and can easily switch between the three. During silent monitoring, the agent cannot see anything that the supervisor types; however, the supervisor sees the content of what both the agent and the customer type in the chat window. For whisper coaching, the customer does not hear any instructions the supervisor gives the agent. The supervisor can choose to monitor only one chat interaction or all chat interactions for a specified agent.

- *Ability for Supervisors to change an agent's status*

Supervisors cannot change an agent's state, but managers can activate and deactivate queues for agents who are already a member of those queues. Agents can also activate and deactivate queues themselves. Note that agents must be a member of the queue before they can activate on the queue. The system will automatically show them as "not available" if the agent does not answer.

- *Ability for Supervisors to silently monitor inbound and outbound calls*

The Supervisor Desktop supports Genesys Cloud via agent group views. Supervisors can select an agent and monitor the next interaction. Supervisors can silently monitor, whisper coach, or join in on a session, and can easily switch between the three. During silent monitoring, the agent cannot see anything that the supervisor types; however, the supervisor sees the content of what both the agent and the customer type in the chat window. For whisper coaching, the customer does not hear any instructions the supervisor gives the agent. The supervisor can choose to monitor only one interaction or all interactions for a specified agent.

- *Ability to interrupt an agent's call to interact with both the caller and the agent*

Supervisors can silently monitor, whisper coach, or join in on a session, and can easily switch between the three.

- *Ability for Supervisors to remove an agent from a call*

Supervisors have the ability, once on a call, to drop an agent from an existing call.

• *Ability to change an agent's skill profile in real-time*

Genesys Cloud provides very granular means for changing user profiles and roles. The administrator can edit user profiles as necessary with skills, location, management, including the ability to add phones, as well as add or remove permissions for people within the organization. Administrators can also create roles for assigning customized sets of permissions as required. All of this is handled quickly and easily and to a very granular level. Administrators can make changes on-the-fly in real-time, and without disrupting agent or queue activity. Valid changes take effect immediately.

*Please describe your solution and identify any areas in your solution that exceed the items requested above.*

The Genesys Cloud includes a rich set of monitoring, and supervising tools with reporting tools to allow for the management of the agents.

*Some State agencies require the ability to utilize call recording, both on-demand and session-initiated. Certain call recordings will contain sensitive data (PHI, PII, etc.) and will require proper security protocols when transmitting or storing this information, with role-based access as defined by the State. Please describe your solution's call recording capabilities, and any additional requirements for the State in order to utilize these features.*

The Genesys Cloud can record 100% of all Genesys Cloud interactions, ensuring nothing critical is ever missed.

Depending on their roles (administrator, supervisor or other), users have access to one or more of the following features:

- Recording via a monitored telephony number or driven by a routing strategy based on attached data
- Play back a stored call recording or multiple call segments
- Download a stored call recording, either singly or in bulk
- Search for one or more call recordings based on various criteria
- Delete one or more recordings
- View audit logs related to access of the recordings and actions related to them
- Storage and archiving
- Policy-based recording by tenant
- Real-time monitoring
- IVR recording provides true end-to-end call recording
- Permalinks are sent via email so that a user outside the system may listen to the recordings

*4.2.1.1.4.4 The State may utilize an outbound predictive dialing campaign, at an Agency's request. Please describe your solution's capabilities in providing predictive dialing campaigns.*

The Genesys Cloud Dialer offers multiple dialing modes to accommodate a variety of calling strategies and situations, including: Predictive Dialing – Calls are automatically paced to match anticipated agent availability. Genesys platform dials calls to consumers and, as soon as consumer picks up the phone, it bridges the call back to the agent.

**4.2.1.2 Security for Vendor's Hosted Solution**

*The State's goal is to ensure the Vendor's solution adheres to industry standard security practices and provides for sensitive data protection (where required) as it relates to cloud-based services. As such, the Vendor should:*

**4.2.1.2.1** *Describe how its solution leverages high security standards associated with regulated data and/or high availability requirements, but also offers a cost-effective, standard-security solution option to the state.*

Our information security program is a risk-based program using the framework of ISO 27001. A formal risk assessment including both quantitative and qualitative methods is performed, management evaluates the risks based on company and customer requirements, and formal controls are established to address the risks. Our architecture is multi-faceted and follows the framework of ISO 27002 guidelines, SOC 2 (SSAE18) Trusted Security Principles, PCI-DSS and various other privacy and regulatory compliance requirements.

We manage our security through a management governance function that drives policy and risk management. We employ a well-trained and knowledgeable security team that encompasses all environments. We have defined asset handling requirements based on clear classifications of assets in our environment. We maintain strong controls around our personnel and third-parties to ensure their integrity and awareness of security responsibilities. We have implemented strong network, systems, database and application controls that include network access controls, configuration standards, authentication standards and user access controls to ensure the security of our environment is protected. We maintain strong operational controls to operate, monitor the environment, detect vulnerabilities and weaknesses, and respond to events and incidents. We operate a rigorous change control process to provide integrity, stability, and awareness in our environment. Our software development lifecycle not only includes strong controls around our development process, product security requirements and testing, but also a feedback loop from our operational groups and environment. Throughout the lifecycle of our program we maintain a continuous feedback loop of data that informs us of the status of our controls, our efforts and the results we see. This feedback loop includes both internal and external audits to ensure our program aligns with our objectives.

**4.2.1.2.2** *Describe its policies and procedures for conducting sub-contractor assurance, validating both the capability of the vendor to fulfill contracted responsibilities and adhere to all applicable to security & privacy policies and controls of all parties.*

Contractual arrangements set out the requirements for the employees of the contracted company, including security, and are treated and measured in the same way as internal staff. Contractual agreements are considered confidential and not shared externally.

**4.2.1.2.3** *Describe its company's cyber security and privacy management program including an overview of the governance structure, cyber security strategy, and the experience of personnel in key security and privacy roles.*

Our information security program is a risk-based program using the framework of ISO 27001. A formal risk assessment including both quantitative and qualitative methods is performed, management evaluates the risks based on company and customer requirements, and formal controls are established to address the risks. Our architecture is multi-faceted and follows the framework of ISO 27002 guidelines, SOC 2 (SSAE18) Trusted Security Principles, PCI-DSS and various other privacy and regulatory compliance requirements.

We manage our security through a management governance function that drives policy and risk management. We employ a well-trained and knowledgeable security team that encompasses all environments. We have defined asset handling requirements based on clear classifications of assets in our environment. We maintain strong controls around our personnel and third-parties to ensure their integrity and awareness of security responsibilities. We have implemented strong network, systems, database and application controls that include network access controls, configuration standards, authentication standards and user access controls to ensure the security of our environment is protected. We maintain strong operational controls to operate, monitor the environment, detect vulnerabilities and weaknesses, and respond to events and incidents. We operate a rigorous change control process to provide integrity, stability, and awareness in our environment. Our software development lifecycle not only includes strong controls around our development process, product security requirements and testing, but also a feedback loop from our operational groups and environment. Throughout the lifecycle of our program we maintain a continuous feedback loop of data that informs us of the status of our controls, our efforts and the results we see. This feedback loop includes both internal and external audits to ensure our program aligns with our objectives.

Please refer to our policies at <http://www.genesys.com/about-genesys/legal>.

**4.2.1.3 Service and Support for Vendor's Hosted Solution**

*The State's goal is to partner with a Vendor whose service and support structures allow the State to focus on its core services, while ensuring telephony and contact center systems are available to State Agencies, with certain Agency sites (hospitals, jails, etc.) operating critical services 24x7x365. The State desires a Vendor to provide all levels of tiered support, including Tier 1 support for end-users. To this end, the Vendor's service and support structure for the Vendor's hosted solution should provide for the following:*

*4.2.1.3.1 Performance monitoring, capacity planning, and real-time surveillance of the Vendor's network to ensure 99.9% availability of services and provide network utilization reports upon request. Please describe your company's process and ability for providing this information upon request, including any lead times needed and how the State submits these requests.*

Genesys Cloud provides proactive monitoring using automated test probes that continually validate the performance and availability of all critical components. These include the use of Empirix voice test probes that place automated calls into the system to check the voice quality and report on Mean Opinion Score (MOS).

We have defined alarms and alerts based on key measures, indicators, and triggers. We characterize these alarms by alarm type and severity to indicate different steps to be taken based upon alarm type. When we receive an alarm, we automatically classified and reacted to as appropriate.



**4.2.1.3.2** *The State desires regularly scheduled meetings and/or calls to discuss the following areas:*

- *Architecture and Design*
- *Implementation*
- *Ordering and Billing*
- *Service and Support*
- *Project Management*

*Please describe your company's ability to hold regular meetings on each of these topics, as well as your company's implementation plans for starting these discussions.*

The following types of meetings are typical within the Genesys Cloud project implementation:

- **Project Kick-off** – this occurs at the start of the project and includes the Project Team Members from both Avtex and the Client.
- **Design Meetings** – these are scheduled shortly after the Project Kick-off. A typical project consists of two – three design meetings over the space of one to two weeks. Those meetings are attended by the Avtex Project Manager and appropriate Technical Resource(s) and the client Project Manager/Lead, Contact Center Manager, and appropriate Technical Resources.
- **Status Meetings** – these are scheduled weekly, generally once the design is completed. These would include the Avtex Project Team and the key Client Project Team Members.
- **Transition to Support Meeting** – after the system is successfully in production the Avtex Project Manager, Avtex Support Manager and the Telephony and Contact Center System Administrator meet to transition support from the Project Team to the Avtex 24 x 7 Technical Assistance Center team.
- Post project the Avtex Client Account Manager (CAM) is responsible for maintaining and enhancing the client relationship. The CAM will schedule many ad hoc and standard meetings to reach that goal. The CAM role is described in page 15 of Attachment 4.2.1.1.1.1-7 –Avtex - State of West Virginia Support Handbook. Avtex will provide the SoWV with at least monthly Support Statistics via your personalized Power BI view to review support statics ad-hoc
- Avtex will meet onsite with the SoWV quarterly to review Support Statistics
- Avtex and the SoWV will meet on a reoccurring scheduled cadence to review open incidents
- Avtex and the SoWV will meet after 3 months, 6 months and 9 months
  - Evaluate hours consumed and determine if this agreement hours needs to be adjusted.
  - Should the quarterly Managed Services hours show a ten-percent (10%) increase or decrease the parties agree to review and discuss an increase or decrease in the terms.

**4.2.1.3.3** *Vendor should contact the State's engineering points of contact by phone within 30 minutes of a Vendor network outage that affects multiple sites on the State's network. This verbal notification should be followed with a written report that provides an explanation of the problem, the cause of the problem, the solution to the problem, the estimated time for recovery, and the steps taken or to be taken to prevent a reoccurrence. To that end, please describe your company's notification procedures in the case of an outage.*

Avtex support service level objectives deliver the States requested response time. For more detail please see of Attachment 4.2.1.1.1.1-7 –Avtex - State of West Virginia Support Handbook, page 9.



Priority	Business hours	Non-Business hours and Holidays	Hours of Activity
<b>Emergency</b> <i>Requires live call into queue</i>	Initial Contact: Immediate Follow-up: Constant	Contact: 30 min Follow-up: Hourly Escalation: 4 Hours	24 x 7
<b>High</b> <i>Live call into queue</i>	Initial Contact: Immediate Follow-up Service Level: Daily	Contact: 10:00 AM Central next business day Follow-up Service Level: Daily	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>High</b> <i>OnPoint or E-Mail</i>	Initial Contact: 4 Hours Follow-up Service Level: Daily	Contact: 10:00 AM Central next business day Follow-up Service Level: Daily	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Medium</b> <i>All interaction types</i>	Initial Contact: 4 Hours Follow-up Service Level: 3 business Days	Contact: 10:00 AM Central next business day Follow-up Service Level: 3 business Days	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Low</b> <i>All interaction types</i>	Initial Contact: 4 Hours Follow-up Service Level: 5 Business Days	Contact: 10:00 AM Central next business day Follow-up Service Level: 5 Business Days	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Move, Add, Change</b> <i>All interaction types</i>	Requests will be completed within 2 business days after receipt of the request	Changes will be scheduled during Avtex business hours and will be completed within 2 business days after receipt of the request	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays

Figure 2: Service Level Objectives

4.2.1.3.4: *Vendor should provide written notification of ten (10) business days or more in advance of any planned upgrades, modifications, etc. that may affect the State's customers to the State's engineering points of contact. Please describe your company's notification process for planned maintenance.*

Avtex fully understands the 10-day notification requirement and will be managed by the Customer Account Manager CAM.

The Genesys Cloud planned outages involve any activity (this includes operating system patches, service updates, equipment reboot) where it is anticipated to have interruption to the operational functioning of the Genesys Cloud Services. Genesys will provide customer with at least two (2) weeks advanced posted notification and email notice prior to conducting any planned outage. Additional email notification will be provided forty-eight (48) hours prior to any planned outage event. Genesys will perform planned outages between the hours of 12:00 a.m. (midnight) and 5:00 a.m. within the time zone of the customer's primary Genesys Cloud data center. Alternatively, the Genesys Cloud team can work with a customer on a preferred schedule to perform their upgrade. This can be arranged through their account representative or Service Delivery Manager.

Best practices are followed to ensure minimum impact to normal operations occur during planned upgrades. The Genesys team will methodically upgrade media servers to ensure, if possible, that at no time are all media servers unavailable. This will allow calls to continue to be processed as normal. In addition, when upgrading the Genesys servers, the Genesys Cloud upgrade team will work with the customer to perform an upgrade of one server at a time, performing controlled switchovers between

the primary and backup system, and go through testing gates to verify with the customer that no impact is experienced.

*4.2.1.3.5 Vendor should provide notification of three (3) business days or more in advance of emergency maintenance. While the State understands emergency outages and/or unplanned maintenance windows occur, it is expected that these situations are kept to a minimum. Please describe your company's notification process for emergency maintenance and outages.*

Avtex fully understands the three-day notification requirement and will be coordinated between the Customer Account Manager CAM and support Escalation Manager.

See the answer for 4.2.1.3.4 above.

*4.2.1.3.6 If the Vendor's work requires them to be at a State site, the Vendor should provide Agency at least 72 hours' notice before arriving at the site and comply with State law and all Agency policies, including but not limited to background checks for contractors, vendors, and visitors. Please describe your approach and methodology in your solution/response.*

Avtex understands this 72-hour notification requirement.

*4.2.1.3.7 The Vendor's network operation support center should provide: all tiers of support, including end-user support, advanced technical expertise, be staffed with resources that are proficient in spoken and written English, maintain and take responsibility for trouble tickets reported by the State until resolved, and provide a tiered support escalation process. Please describe your network operation support center's structure, processes, and procedures for handling trouble tickets, resolving those tickets, and reporting back to the State's point of contacts.*

Understood, Avtex has quoted Managed Services to provide Tier 1 and MACD support. Once incident is triaged by West Virginia Avtex will work directly with the end user to resolve the issue.

The Genesys Network Operations Centers control and monitor all Genesys Cloud service 24/7/365. Genesys uses a distributed performance and availability monitoring solution that covers all aspects of the SaaS infrastructure. The system is capable of monitoring Genesys components as well as specific connectivity to client systems, including the MPLS network, circuits, and application servers, based on the specific deployment model. The monitoring system offers advanced alerting and visualization to allow us to obtain notification of any issues and immediately begin taking appropriate action.

4.2.1.3.8 *The Vendor's solution should include a documented support and escalation structure to address outages. The State prefers the severity of the issue/support problem to determine the average problem resolution response time, as outlined below:*

- *Severity Level 1 is defined as an urgent situation, where the customer's services are unavailable and the customer is unable to use/access the network. The Vendor should resolve Severity Level 1 problems as quickly as possible, which on average should not exceed two (2) business hours. If repair inside the 2-hour window is not feasible, then regular 1-hour updates are desired.*
- *Severity Level 2 is defined as significant outages and/or repeated failures resulting in limited effective use by the customer. The service may operate but is severely restricted (i.e. slow response, intermittent but repeated inaccessibility, etc.). The Vendor should resolve Severity Level 2 problems as quickly as possible, which on average should not exceed four (4) business hours. If repair inside the 4-hour window is not feasible, then regular 2-hour updates are desired.*
- *Severity Level 3 is defined as a minor problem that exists with the service, but most of the functions are still usable, and some circumvention may be required to provide service. The Vendor should resolve Severity Level 3 problems as quickly as possible, which on average should not exceed ten (10) business hours. If repair inside the 10-hour window is not feasible, then updates are desired at the start of the next business day and every day thereafter until repairs are complete.*

*Please describe your company's severity level structure, as well as your documented procedures for handling outages, including escalation processes, notification methods, and resolution times.*

**Avtex defines system emergencies as major system hardware, software, or application outages that impact your company's ability to receive or make calls and perform other critical system or application functions.**

#### **Major Problems Defined**

- Unscheduled total system outage and failure to reboot for any reason.
- Inability to access the system through 25% or more of all ports.
- Loss of system integration.
- Continuous system restarts or failovers.
- Loss of dial tone on more than 25% of system.

Avtex will ask our clients to categorize the severity of their issue and will respond accordingly. While our goal is to provide the best client experience possible, we do ask our clients to use the severity coding appropriately. For Emergency and High incidents Avtex requires a call into the queue as stated in the following table:

Priority	Business hours	Non-Business hours and Holidays	Hours of Activity
<b>Emergency</b> <i>Requires live call into queue</i>	Initial Contact: Immediate Follow-up: Constant	Contact: 30 min Follow-up: Hourly Escalation: 4 Hours	24 x 7
<b>High</b> <i>Live call into queue</i>	Initial Contact: Immediate Follow-up Service Level: Daily	Contact: 10:00 AM Central next business day Follow-up Service Level: Daily	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>High</b> <i>OnPoint or E-Mail</i>	Initial Contact: 4 Hours Follow-up Service Level: Daily	Contact: 10:00 AM Central next business day Follow-up Service Level: Daily	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Medium</b> <i>All interaction types</i>	Initial Contact: 4 Hours Follow-up Service Level: 3 business Days	Contact: 10:00 AM Central next business day Follow-up Service Level: 3 business Days	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Low</b> <i>All interaction types</i>	Initial Contact: 4 Hours Follow-up Service Level: 5 Business Days	Contact: 10:00 AM Central next business day Follow-up Service Level: 5 Business Days	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Move, Add, Change</b> <i>All interaction types</i>	Requests will be completed within 2 business days after receipt of the request	Changes will be scheduled during Avtex business hours and will be completed within 2 business days after receipt of the request	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays

Figure 3: Service Level Objectives

Genesys Cloud incidents will be categorized and handled according to an assigned severity level. The assigned severity level for a problem may be mutually determined by both parties during the problem resolution process but Genesys Care shall have final authority as to the actual designation. Genesys Care uses commercially reasonable efforts to respond to each Support incident within the applicable response time and reach resolution of code red and high impact issues within the timeframes described in the table below.

Priority Level	Initial Response	Mean Time to Restoration (MTTR)
Code Red	15 minutes (by Phone)	15 minutes
High	15 minutes (by Phone)	72 hours
Medium	24 hours (by Web)	N/A
Low	2 business days (by Web)	N/A

- Code Red:** Genesys Cloud’s operational ability to receive, route and deliver Customer purchased interaction services is ‘down,’ severely degraded, or major components of the service are not operational, and work cannot reasonably continue for greater than 10% of minimum monthly agent commitment as identified in the Order Form (see column entitled “Minimum Monthly Commitment for Users/Item”). Interaction services that are ‘down,’ severely degraded, or major components due to customer managed equipment and/or applications (email server, web chat server, etc.) are excluded from ‘Hard Outage’ credits.

- **High:** Non-business critical features of the Genesys Cloud Services are impaired or non-functional.
- **Medium:** Non-disabling or cosmetic errors with little or no impact on the Genesys Cloud Services.
- **Low:** Requests for information on Genesys Cloud Services, Policies, Processes, or Procedures from Supplier by members of Customer's Business, Management, or technical staff teams. Genesys will make administrative moves, additions or changes (MACs) as follows, provided Customer cooperates with Genesys as reasonably required to meet the response time:
  - The MAC will be scheduled during posted business hours and will be completed within twenty-four (24) business hours after receipt of the request.
  - All requests must be made using the support website: [Genesys MySupport Portal Login](#)
  - Customer will pay the amounts stated in the Order Form for MACs.

Genesys Cloud Operations has a regional management team, comprised of a Regional Service Delivery Manager, Regional Support Manager, and Regional Technical Account Manager(s) who will be designated as the management contacts. If an escalation is requested by a customer, the management team can be contacted by phone or email. The Regional Support Manager serves as the second level escalation contact and will oversee the escalation until the incident is resolved and coordinate internal resources to participate in scheduled calls with the customer. The response time on the incidents are defined in the customer contracts based on incident priority.

*4.2.1.3.9 The State desires the ability to place initial service orders, any changes with an associated charge, or to disconnect services, electronically and receive confirmation of receipt and subsequent order detail. The State desires details including the following data elements:*

- *Telecommunications Change Request (TCR) Form Number*
- *Date order was received*
- *Customer Name*
- *Customer on-site address*
- *Projected due date*
- *Rate element identifier (circuit ID or other)*
- *Additional order details*

*Additionally, the State prefers the Vendor's solution has a web portal for Agencies to enter moves, add, and changes that do not contain billing elements. MACD changes should be resolved by the same or next business day. Please describe your company's ability to accept, process, and report on electronic order submissions, as well as any requirements from the State needed to implement such a program.*

#### **Avtex Change Order Process or Telecommunications Change Request (TCR)**

The change order process is in place to provide a method for tracking system software, hardware and custom application changes. We ask that you follow this procedure, so we can guarantee timely delivery of client requests.

Your CAM should be your first point of contact when requesting changes. CAM's are dedicated to specific accounts, so they understand your configuration and existing applications. By following the change order process, you can implement enhancements with ease.

The following steps outline the change order process:

- 1) Contact your CAM to discuss your proposed change. Depending on the magnitude of your request, a meeting may be scheduled with key personnel. A timeframe for delivery will also be determined.



- 2) Your CAM will document.
- 3) Once the project has been defined, the CAM will submit it to a Project Engineer for pricing.
- 4) The CAM will then complete a Change Order or formal proposal for work when appropriate, including pricing, and e-mail it to you for review and signature.
- 5) Once Avtex has received the signed change order, a project team will be assigned, and completion date assigned.
- 6) Upon completion, a final invoice will be generated.

As a reminder, this process should be followed when you want to create a new application, modify an existing application, or add hardware or licenses to your system. Payment terms will be defined in the Change Order or Proposal for work.

*4.2.1.3.10 The State maintains a Learning Management System (LMS) for training purposes. The State desires web-based training and training materials for all services offered under this contract. The State desires the Vendor to provide materials that can be uploaded into its LMS, initial Train the Trainer session(s), and documentation/reference materials that can be distributed to and used by end-users. The State intends to incorporate these materials into its LMS, as well. Additionally, the State desires training sessions, if requested by the Agency, and the Vendor should include a professional services rate for training that would be above and beyond the initial training included in the site deployment. The expects the Vendor's training materials to be updated as necessary. The training services for the hosted voice services should be included in the monthly per package cost. Please provide information regarding your training program.*

Avtex has proposed live train the trainer services to meet the needs of West Virginia.

At Avtex, we believe that every user should possess a detailed knowledge of the technology platforms at their disposal. With that in mind, we've created a wide range of training courses designed to educate employees, end users, administrators and management on the best ways to use the tools available to them.

Our training services offer a wide range of benefits, including:

- improved platform effectiveness
- Improved data gathering
- Customer satisfaction
- Reduced IT support costs
- Consistency across departments
- Improved employee satisfaction
- Improved productivity
- improved ROI on platforms

Avtex offers a catalog of structured training classes delivered in a variety of formats to meet customer needs. Customized training can also be provided at standard hourly rates.

While our private training courses (custom) focus on the customer's specific configuration, customized training sessions are available upon request at standard hourly rates. Avtex instructors conduct discovery sessions with our customers to determine the scope and effort of the customized training, including custom agendas, options for train-the-trainer and end-user documentation, etc.



Most training classes can be offered in either a Train-the-Trainer or End User format. Train-the-Trainer is the standard and most common method of delivery, in which the Customer selects representatives of each Role (e.g. Administrator, Supervisor, Agent) to receive training and Avtex-guided preparation so that they are prepared to deliver training to the remaining system users.

Avtex provides options for Public and Private Instructor Led Online training. Public courses are hosted on Avtex systems and explore general features, functionality and best practice. Private courses are hosted on customer's systems and account for your specific configuration.

Avtex has provided a list of specific training modules at the bottom of page 23 of Attachment SO-1 - Avtex - SoWV - Managed and Hosted Voice Services - Base Configuration SOW.

#### **eLearning -- Web-based training**

Avtex recommends that end users review our Just-in-Time training videos, available on our website at <http://help.genesys.com/justintime/index.html>. The Just-in-Time videos are easy to find, brief and to the point training videos.

Suggested course(s) for Administrators is contingent upon the Genesys solution selected by the customer. As standard practice, Genesys provides technical instructor led training for the following:

- Interaction Center Core Specialist Bootcamp (ICCS) or ICCS Curriculum
- Interaction Administrator Core Concepts
- Interaction Attendant Core Concepts
- Interaction Dialer Certified Engineer (IDCE)
- Interaction Optimizer Certified Administrator (IOCA)
- Interaction Center Handler Developer Training (IChD)
- Interaction Center iceLib Developer Training (ICID)
- Interaction Process Automation (IPA) Core Concepts

Avtex recommends first sending the administrator to attend a standard administration course with Education Services, followed by an administration course tailored for their environment from Professional Services Organization (PSO).

The company also provides onsite "readiness" training, from the Professional Services Organization (PSO) that places an emphasis on the customer's selected solution and its architecture. These trainings are tailored to suit the customer's requirements:

- Administration training
- Supervisory training
- Agent training
- Reports development training

For a complete listing and schedule of available Genesys courses please visit our Education Services listing located on our web site at <https://www.genesys.com/customer-experience/customer-success/genesys-university>.

**4.2.1.3.11** *The State desires an hourly rate for Hosted Contact Center Training Services in the instance the State desires training sessions beyond the training provided at initial implementation. The training at initial implementation should be built into the one-time costs for the Contact Center. These training services should include training for all contact center roles and should be provided at the State's request. Please describe your Contact Center training offerings and your solution's ability to meet this goal.*

Avtex has extended a fully loaded training rate of \$278 per hour. The project is based on a train the trainer model.

Additional courses are offered based upon the system components requested by the customer. A comprehensive list of Avtex training courses can be found here: <http://www.avtex.com/avtex-private-training/>

**4.2.2. Mandatory Project Requirements** -*The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.*

**4.2.2.1 Managed Voice Services**

**4.2.2.1.1** *The Vendor must provide a turnkey technical support solution that ensures the continued operations and MACD needs of the State's existing telephony infrastructure, as defined in Appendix A, through the migration period to a Hosted VoIP solution. Additionally, the Vendor must, at the State's discretion, migrate any site to the hosted solution.*

The Avtex solution support includes a Premier support package with Managed Services including Tier 1 and MACD. The Managed Services was based on an estimated 300 incidents over 18 months to start. Avtex and the State will meet after 3 months, 6 months and 9 months to 1) Evaluate hours consumed and determine if this agreement hours needs to be adjusted; 2) Should the quarterly Managed Services hours show a ten-percent (10%) increase or decrease the parties agree to review and discuss an increase or decrease in the terms. Please see Attachment 4.2.2.1.1-1 - Avtex - SoWV - Base Configuration Premier CSA and Attachment 4.2.2.1.1-2 Avtex - SoWV - Managed and Hosted Voice Services Agreement for details.

**4.2.2.2 Hosted Voice Services**

**4.2.2.2.1** *The Vendor must agree the State owns all data gathered under the scope of this contract and the Vendor must produce and/or return the data upon the State's request in an editable format.*

AVTEX agrees that all data gathered under the scope of work will be the property of the State and will provide this data to the State in an editable format.

Genesys has a privacy policy that defines the Company's role as a processor or custodian of customer data. The Customer is the owner of the data, and Genesys would access information from the Customer only for performance valuation purposes, in accordance with agreements.

Genesys can provide evidence that data retention practices for routine operations occur as agreed to via our SSAE16 SOC2 report. Genesys can provide confirmation of destruction of data in the event of contract termination.

**4.2.2.2.2** *Vendor's solution must provide support for local failover and/or survivability services, if requested by Agency, in the event the hosted service becomes inaccessible.*

The Genesys Cloud disaster recovery strategy uses an automatic failover site model. This provides almost instantaneous resumption for critical services. If a primary system fails, these sites automatically switch operations to their active standby database, server, or network.

**4.2.2.2.3** *Vendor's solution must provide local telephone numbers in West Virginia.*

Genesys Cloud can be deployed in one of two ways:

- Local Control VoIP Model: Customers keep their current telco trunks and basically have an on-premise system (gateways, proxy/media servers, and IP/phones) but with the Customer server running in the Genesys data center.
- Remote Control VoIP Model: Calls come into trunks in the Genesys data center and are routed using VoIP over an MPLS network to the customer's agents. The only new hardware needed on the customer premises is IP phones (although agents can use soft phones too).

**4.2.2.2.4** *Vendor's solution must support inbound Automatic Number Identification (ANI).*

Genesys Cloud supports ANI.

**4.2.2.2.5** *Vendor's solution must include inbound Caller ID, outbound custom telephone number, and outbound custom name display.*

Caller ID data is sent to the outside via the line configuration settings. When the line is configured, the administrator sets up the Caller ID value that will be passed to the public switched telephone network (PSTN). In this configuration, one could set this up to send a specific caller ID value for each remote location.

Inbound Caller ID sends from the carrier to the ingress gateway. This data then populates into the SIP invite message and sends to the application. Once the application has the Caller ID information, it can then implement its routing rules based on this data.

**4.2.2.2.6** *Vendor's solution must support Dialed Number Information Services (DNIS) on 800 # toll-free telephone services.*

If Genesys is providing the carrier service from Level3, then we can RespOrg the 800 numbers over to Level3 with proper documentation from the current responsible party.

If another carrier is being used, then it would be up to the customer to move the toll-free numbers to that carrier.

**4.2.2.2.7** *Vendor's solution must support rerouting of calls to an alternate site at the State's directive.*

Genesys Cloud supports the ability to reroute calls to an alternate site as defined in the call flow design. Calls can also be automatically rerouted via defined overflow rules.

**4.2.2.2.8 Vendor's solution must support 900/976 blocking.**

Administrators may block all calls to a specific number such as 900 numbers or specified area codes for all users or they may block specific options for specific users. An example would be the "available, forward" option where users can forward their extension to their cell phones or home office phones when they are not at their desk working.

**4.2.2.2.9 Vendor's solution must support xl 1 services (currently 211, 411, 511, 611, 811, 911).**

Genesys Cloud includes the ability to create a National Emergency Number Association (NENA) 20-010 compliant file listing the automatic number identification (ANI) and automatic location information (ALI) data. Customers may submit file to the e911 public safety answering point (PSAP) provider to update the service provider's ALI database.

Genesys Cloud can integrate via application programming interface (API) with other applications to automate the PSAP ALI database updates.

In addition, to enable North American customers to comply with emergency service number (E911) regulations implemented in some states and areas, Genesys Cloud has recently released a new mechanism for E911 functionality. The E911 feature sends the Media Access Control (MAC) and IP address of a managed station that dials 911 through a Genesys Cloud client application to a third-party E911 service provider. The E911 service provider can associate those addresses to a previously provided Automatic Location Information (ALI) record and forward it to the correct Public Safety Answering Point (PSAP) to answer.

**4.2.2.2.10 Vendor's solution must include Direct Inward Dial (DID) feature and service.**

Genesys Cloud supports DID numbers. Administrators may assign individual DIDs to agents and workgroups to route to them directly.

**4.2.2.2.11 Vendor's solution must support Operator services.**

Interaction Attendant configures the auto attendant system built into Genesys Cloud. An auto attendant automatically answers a call. It prompts the caller to make menu choices and routes the call according to that caller's choice. A graphical application, Interaction Attendant allows the customer to determine how calls are handled in the organization. Using various call handling "trees" administrators establish routing for different situations, such as normal business hours, after hours, weekends, and holidays). For example, you can determine as in the screen shot below, that when the caller presses "3" the caller will be asked if they want hardware support or software support. Interaction Attendant allows administrators to manage call flows without having to customize handlers, adapting your system to the way you do business.

**4.2.2.2.12 Vendor's solution must support local number portability.**

Local number portability is a function of the current telco owning the number. If this is supported by the current vendor, Genesys supports the portability.

**4.2.2.2.13 Vendor's solution must provide unlimited free local and long-distance calling.**

See Attachment A - Genesys Pricing Addendum.

**4.2.2.2.14** *Vendor's hosting center(s) must be located within the continental United States.*

Genesys Cloud has data centers located in the United States, Canada, United Kingdom, Germany, Japan, and Australia. Genesys uses these data centers as co-location facilities but takes full responsibility for managing all components within these data center facilities.

This project will be supported out of dual geo-redundant data centers located in the USA, using mirrored, active/standby servers.

**4.2.2.2.15** *Vendor must provide Train the Trainer sessions for Hosted Voice Services implementations.*

Prior to "going live" with our solution, the individual(s) responsible for managing Genesys Cloud are required to take the Genesys Cloud Operational Readiness Education (C.O.R.E.).

C.O.R.E. is a self-paced curriculum focusing on the administration and operation of the Genesys Cloud solution. The C.O.R.E. courses include administering the Genesys Cloud solution with Interaction Administrator, implementing call flows with Interaction Attendant, and understanding the responsibilities of supporting the Genesys Cloud solution. After completion of the curriculum, a closed-book certification exam is provided to allow participants to earn the Genesys Cloud Certified Professional (CCP) designation. The Genesys Cloud C.O.R.E. Curriculum is available via the Customer's MyCloud account and consists of video content, a training manual, a self-assessment, and access to labs.

There is no cost to complete the C.O.R.E. curriculum. The curriculum or individual courses can be taken in whole or in part by as many individuals as you desire. The CCP certification exam involves an associated cost per person.

Additionally, PS typically offers "readiness" training as part of the implementation process. Customers can work with PS for any additional training needs they have.

**4.2.2.2.16** *The State recognizes the need for the inclusion of certain fees and charges mandated by the federal government or Public Service Commission, including but not limited to, Universal Service Fund Fees and 911 Fees. As such, the Vendor must include the latest published version of such fees with its cost response. The State will allow for quarterly Change Orders to care for changes in these fees.*

Genesys complies and adheres to the Federal Communications Commission's quarterly update to the Universal Service Fund Fee. The latest published version of these fees can be found on this link: <https://www.fcc.gov/general/contribution-factor-quarterly-filings-universal-service-fund-usf-management-support>

Avtex understands the need to allow governmental charges to be modified using the TCR process.

**4.2.2.3** *Hosted Contact Center Services*  
*Vendor's Contact Center solution must support:*

**4.2.2.3.1** *Automatic Call Distributor (ACD)*

Genesys Cloud provides the ability to queue and distribute various types of interactions coming in from the outside world. Our inherent ACD has revolutionized the call center industry by increasing the



efficiency of call center agents. Genesys builds on the basic concepts of automatic call distribution and skills-based routing to include sophisticated multimedia queuing.

#### **4.2.2.3.2 Computer telephony integration (CTI)**

Genesys Cloud provides IVR, ACD, skills-based routing, CTI, multimedia contact strategies, callback, reporting, WFO, speech services, monitoring and recording. In addition, Genesys Cloud also offers call blending with our predictive, power, preview, and manual-only dialing services. All these features are available to support and manage the at-home worker as effectively as they support and manage the in-office worker.

#### **4.2.2.3.3 Call control**

Genesys Cloud supports the following telephony features:

- Busy Override
- Call Back
- Call Forward Internal
- Call Forward External
- Call Forward all
- Call Forward on Busy
- Call Forward on no Answer
- Call Hold
- Call Park
- Call Pickup / Call Pickup Group
- Call Status Per Line)
- Call Transfer
- Blind transfer (or supervised transfer)
- Call Waiting
- Calling Line Identification/ Caller ID
- Calling Party Name display
- Circular Hunt/ Hunting group
- Class of restrictions
- Company directory accessible via phone
- Conference (6 way)
- Direct Inward Dial (DID)
- Direct Outward Dial (DOD)
- Distinctive Ring
- Display Call history
- Do Not Disturb
- DTMF
- Emergency service
- Extension Mobility/Roaming Support
- Last Number Redial
- Malicious Call ID and Trace
- Message Waiting Indication
- Multiple Calls per Line Appearance
- Multiple Line Appearances Per Phone (DID)
- Music-On-Hold



- On-hook Dialing
- On-hook answerback
- Privacy Release
- Speed dial
- Switch loop attendant console

**4.2.2.3.4 E.164**

Genesys Cloud supports RFC 3824 for using E.164 numbers with SIP.

**4.2.2.3.5 Interactive voice response (IVR)**

Genesys Cloud features integrated IVR functionality. As part of this offering, the product comes equipped with Microsoft text-to-speech. Integration with third-party IVR applications is also possible.

**4.2.2.3.6 Voice Recording**

Interaction Recorder, inherent to Genesys Cloud, records phone calls, ACD emails, faxes, and web chats. Interaction Recorder can also record the screens of local participants.

Interaction Recorder starts the recording process based on an initiation policy, instructing the interaction Media Server to record the interaction if it is a call. When Interaction Media Server is instructed to record a call, it compresses the recording file, and if the initiation policy has the action to encrypt the recording, the media server encrypts the file.

**4.2.2.3.7 High Availability with load balancing and built-in redundancy**

Genesys provides Cloud customers with a service level agreement that guarantees an uptime of 99.99%. This is done by providing customers with a primary application server housed within the Genesys data center facility and an active backup application server housed within a secondary data center to provide geographic enhanced availability.

The Primary Server processes all interactions. The Active Backup Server is a mirror image of the Active Primary Server and monitors the Active Primary Server. When the Active Backup Server detects a service issue with the Active Primary Server it will initiate an Automatic Switchover and take over as the Active Primary Server. As well, this configuration allows Genesys to perform maintenance on a server without impacting the service we provide to our customers. Maintenance can occur on one server while the mirror image continues processing interactions. The process is then repeated on the secondary server.

*4.2.2.3.8 Vendor must provide Train the Trainer sessions, encompassing all Hosted Contact Center roles -Administrator, Supervisor, and Agents. In the Genesys Cloud environment, proficiency is easily gained and the administrative requirements are minimized because most administration is handled through a graphical user interface (GUI). Many more administrative functions are included as part of the Genesys Cloud service. Agents and supervisors will receive training either directly from PS or indirectly through the "train the trainer" (TtT) program.*

In the TtT program, PS will train the trainers who will in turn train the agents/supervisors. Typical agent and supervisor sessions are 2 hours long (each).

Administrators and developers should be trained by Genesys' Education Services in the products of their focus. PS will then provide oversight, guidance, and training during the project to ensure the customer's designated personnel are prepared to administer and develop in the customer's environment.

- **System Administrator:** Genesys recommends the Genesys Cloud Operational Readiness Education (C.O.R.E.) curriculum. It is self-paced and focuses on the administration and operation of the Genesys Cloud solution. The C.O.R.E. courses include administering the Genesys Cloud solution, implementing call flows with Interaction Attendant, and understanding the responsibilities of supporting the Genesys Cloud solution. After completion of the curriculum, a closed book certification exam is provided to allow participants to earn the Genesys Cloud Certified Professional (CCP) designation. Please note that there is an additional charge for the certification exam. The Genesys Cloud C.O.R.E. Curriculum is available via the Customer's MyCloud account and consists of video content, a training manual, a self-assessment, and access to labs.
- **System Developers:** Genesys recommends the Interaction Center Handler Developer training as well as Interaction Center IceLib Developer courses. The Handler Developer course is offered in classroom and virtual-based formats. The IceLib training is currently offered as a classroom-based course.

#### 4.2.2.4 Security

4.2.2.4.1 *The proposed solution must adhere to the security and privacy baseline standards in accordance to the high-security and standard-security use-case requirements.*

Our information security program is a risk-based program using the framework of ISO 27001. A formal risk assessment including both quantitative and qualitative methods is performed, management evaluates the risks based on company and customer requirements, and formal controls are established to address the risks. Our architecture is multi-faceted and follows the framework of ISO 27002 guidelines, SOC 2 (SSAE18) Trusted Security Principles, PCI-DSS and various other privacy and regulatory compliance requirements.

We manage our security through a management governance function that drives policy and risk management. We employ a well-trained and knowledgeable security team that encompasses all environments. We have defined asset handling requirements based on clear classifications of assets in our environment. We maintain strong controls around our personnel and third-parties to ensure their integrity and awareness of security responsibilities. We have implemented strong network, systems, database and application controls that include network access controls, configuration standards, authentication standards and user access controls to ensure the security of our environment is protected. We maintain strong operational controls to operate, monitor the environment, detect vulnerabilities and weaknesses, and respond to events and incidents. We operate a rigorous change control process to provide integrity, stability, and awareness in our environment. Our software development lifecycle not only includes strong controls around our development process, product security requirements and testing, but also a feedback loop from our operational groups and environment. Throughout the lifecycle of our program we maintain a continuous feedback loop of data that informs us of the status of our controls, our efforts and the results we see. This feedback loop includes both internal and external audits to ensure our program aligns with our objectives.

4.2.2.4.2 *Must adhere to the State of West Virginia's Cyber Security & Privacy policies, procedures, and standards; these can be viewed at the following link: <http://technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx>*

Our information security program is a risk-based program using the framework of ISO 27001. A formal risk assessment including both quantitative and qualitative methods is performed, management evaluates the risks based on company and customer requirements, and formal controls are established to address the risks. Our architecture is multi-faceted and follows the framework of ISO 27002

guidelines, SOC 2 (SSAE18) Trusted Security Principles, PCI-DSS and various other privacy and regulatory compliance requirements.

We manage our security through a management governance function that drives policy and risk management. We employ a well-trained and knowledgeable security team that encompasses all environments. We have defined asset handling requirements based on clear classifications of assets in our environment. We maintain strong controls around our personnel and third-parties to ensure their integrity and awareness of security responsibilities. We have implemented strong network, systems, database and application controls that include network access controls, configuration standards, authentication standards and user access controls to ensure the security of our environment is protected. We maintain strong operational controls to operate, monitor the environment, detect vulnerabilities and weaknesses, and respond to events and incidents. We operate a rigorous change control process to provide integrity, stability, and awareness in our environment. Our software development lifecycle not only includes strong controls around our development process, product security requirements and testing, but also a feedback loop from our operational groups and environment. Throughout the lifecycle of our program we maintain a continuous feedback loop of data that informs us of the status of our controls, our efforts and the results we see. This feedback loop includes both internal and external audits to ensure our program aligns with our objectives.

Genesys will work with West Virginia's security teams to confirm compliance with West Virginia's Cyber Security & Privacy policies, procedures, and standards and address any exceptions.

**4.2.2.4.3** *Must adhere to all applicable security and privacy standards and provide compliance for components and network segments that are subject to the following:*

Avtex has reviewed the requirements and has completed a Type I: SOC 2 examination covering the Security and Availability Trust Services Principles related to Avtex's hosting and managed services. Linford & Co LLP CPA Firm: (See Attachment 4.2.2.4.3 - Avtex - State of West Virginia - SOC 2 Letter), 8310 Valley Hwy Ste 202 Englewood, CO 80112 Health Insurance Portability and Accountability Act (HIPAA) requirements as outlined in Attachment 4.2.2.4.3 - Business Associate Addendum (BAA).

The Genesys Cloud complies with this standard.

• *Federal Information Security Management Act (FISMA), National Institute of Standards Technology's Special Publication (NIST SP) 800-53, NIST SP 800-17 which serve as the baseline;*

Genesys does not support these standards. We may comply with certain portions of them, but as a whole, we do not.

• *Family Education Rights and Privacy Act (FERPA) requirements;*

Genesys does not support these standards.

• *Criminal Justice Information System (CHS) requirements;*

Genesys does not support these standards.

• *Payment Card Industry Data Security Standards (PCI-DSS) requirements;*

The Genesys Cloud complies with this standard.

- *Federal tax Information (FTI) and Internal Revenue Service publication 1075 (IRS 1075) requirements;*

The Genesys Cloud partially complies with this standard.

- *Centers for Medicare & Medicaid (CMS) Services Information Security Policy requirements.*

Genesys does not support these standards.

- *Ensure network boundary and access control protection such as dual session boundary controllers and firewalls.*

The Genesys Cloud complies with this standard.

- *Data-at-rest and data-in-transit encryption.*

The Genesys Cloud complies with this standard.

- *Role-based access control for all applications which process and/or store sensitive data, to ensure need-to-know policies are enforceable.*

The Genesys Cloud complies with this standard.

*4.2.2.4.4 Vendor must draft a cyber risk management plan outlining the process, by which, cyber risk management activities are conducted to identify, assess, communicate, and manage shared cyber risk. The Vendor must provide this prior to the first implementation on the Vendor's hosted solution.*

Avtex and Genesys will work with West Virginia's security teams to confirm compliance with West Virginia's Cyber Security & Privacy policies, procedures, and standards and address any exceptions.

*4.2.2.4.5 Vendor must draft an incident management plan aligned with NIST SP 800-61rev2, whereas both the State and Vendor must mutually approve. The plan must include the outlined scope, responsibility matrix, communications plan, procedures, and deliverables associated with cyber security incident response. In addition, the plan must outline incident reporting requirements, semiannual security reports, and cyber threat intelligence sharing. The Vendor must provide this prior to the first implementation on the Vendor's hosted solution.*

Avtex and Genesys will comply with this requirement.

*4.2.2.4.6 The Vendor must adhere to personnel security requirements for background checks in accordance with state law. The vendor is liable for all costs associated with ensuring staff meets all requirements.*

Avtex and Genesys will comply with this requirement.

*4.2.2.4.7 Vendor must agree to drafting an audit management plan designed to assist the state with conducting internal and external compliance audits when the vendor-supplied solution is within the audit scope. At minimum, the plan must include:*

- *How the vendor will provide a NIST 800-53 security controls report, outlining organizational responsibilities (State, Vendor, or Shared), per each applicable control for each major application/information system within the audit scope.*

Avtex and Genesys will comply with this requirement.

- *Plan of Action & Milestone documentation for non-compliant security & privacy controls when the vendor holds primary or shared control responsibility.*

Avtex and Genesys will comply with this requirement but only third-party audit reports will be shared externally.

*The Vendor must provide this prior to the first implementation on the Vendor's hosted solution.*

Genesys will comply to this requirement and will provide a copy of ISO27001/SOC2/PCI audit reports. Avtex will comply and provide the SOC2 report.

#### 4.2.2.5 Service and Support

*4.2.2.5.1 Vendor must provide a network operation support center(s) for all tiers of support, including end-user support, that is available 24x7x365 and is accessible via a toll-free number.*

Understood, Avtex has quoted Premier support and Managed Services to provide Tier 1 and MACD support. Once incident is triaged by West Virginia Avtex will work directly with the end user to resolve the issue. All tiers of support are available through a toll-free number, 1-800-323-3639.

Please see page 3 of the Avtex - State of West Virginia Support Handbook for details on contacting Avtex support.

Support for your service can be accessed two ways, either by phone or via our online support portal. We always prefer to hear from you via phone for the quickest resolution of your support incidents. For your convenience, we also offer the ability to report your issues via an online issue ticketing system. A skilled engineer from our Support team will contact you by phone as a follow-up to any ticket opened using the online ticketing system. This allows the engineer to obtain any additional information needed to resolve the issue as quickly as possible.

Personnel designated by your management team are provided Support access credentials to our support which includes an iVR pin code and a username/password for our online issue tracking system. Typically, customers designate IT, telecom, contact center supervisors, and select business users as resources to access support.

Please find the appropriate number in the table below to open a Support Incident via the phone. While Standard Support is available only during regional business hours, Priority and Emergency Support are always available.

Location	Support Type	Phone Number	Regional Business Hours
North America	Customer Support (Genesys Cloud, Managed Services, Premises)	1-866-353-6402 (1-317-715-8600)	M-F, 7am-9pm EST *Holidays excluded
	Collector (Latitude)	1-866-396-2599 (1-904-680-7100)	8am-7pm EST *Holidays excluded
	Decisions	1-866-329-6962	M-F, 9am-5pm EST *Holidays excluded
Latin America: Portuguese	Customer Support	+55 11 3882 0338	M-F, 9am-6pm BRST *Holidays excluded
Latin America: Spanish	Customer Support	Colombia: +57 (1) 744-7022 US: +1 317-957-1485	M-F, 7am-6pm COT/CST



Location	Support Type	Phone Number	Regional Business Hours
EMEA: Germany Netherlands Saudi Arabia South Africa United Kingdom	Genesys Cloud Support Customer Support Managed Services,	+49 6995 1066 112  +31 2065 00 001 +966 1125 029 98 +27 8774 009 11 +44 1276 457 222	M-F, 8am-5pm GMT/WET *Holidays excluded
APAC:  Australia Japan Malasia New Zealand	Customer Support  Customer Support Customer Support Customer Support	1 800 503 304 +61 2891 848 88 +813-5989-1302 +60 3277 63 300 + 650 800 2520 20	M-F, 8:30am-5:30pm AEST *Holidays excluded

**Support during Non-Business Hours**

Emergency support calls may be answered by a Genesys Support Engineer working in another part of the world. Every Support Engineer, regardless of physical location, is fully prepared to handle your request. We recommend Customers contact Support in their geographic area first.

Global Support provides coverage for emergency situations 24 hours a day, 7 days a week, including holidays. All other issues during non-business hours should be submitted online. A charge will be incurred for non-emergency issues that are called in as emergencies during non-business hours.

Situations are only considered emergencies when they involve live applications running in a production environment. Issues pertaining to non-production applications will not be considered emergencies and support on the types of issues will occur within normal business hours.

*4.2.2.5.2 The successful Vendor must assign an experienced and skilled Project Manager who will provide a high-level project management plan including key components such as a project charter, issue tracking, statements of work (SOW), work breakdown structures (WBS), implementation schedules, etc. in accordance with the Project Management Body of Knowledge (PMBOK) or other industry standard project management methodology stated in West Virginia State Code (§5A-6-4b). The link can be found at: <http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=05a&art=6#06>. The project management plan must be submitted to and approved by the WVOT Project Management Office (PMO) prior to engaging the first agency for VoIP services implementation.*

Avtex will deploy the proposed technology with its Standard Project Implementation Methodology which uses the Project Management Institutes standards. Avtex will provide all requested project documentation prior to engaging the first agency.

In addition, Avtex has an Iterative Project Implementation and a Small Project Consulting Process. Each of the methodologies are applied as needed. Please see Attachment 4.2.2.5.2 - Avtex Project Process Overview 2018 for further details.

**4.2.2.5.3** *The successful Vendor's Project Manager must track and report (via written status reports) the following: schedule, scope, budget, issues, risks, specified performance indicators, and other metrics determined appropriate throughout the project and each site implementation.*

As a part of the standard documentation offering the following Assessment, Plans and Reports are included:

- Business Assessment
- Application Assessment
- Reporting Assessment
- Solution Design Document and Project Plan
- Project timeline
- Change management plan
- Communication plan
- Project acceptance criteria
- Risk Assessment
- Assist with Test Plan creation
- Test with Client sponsors
- Training plan
- Weekly status reports
- Transition plan
- Quality Assessment Review

These documents are created and provided as deliverables during the following types of meetings are typical within the Genesys project implementation:

- **Project Kick-off** – this occurs at the start of the project and includes the Project Team Members from both Avtex and the Client.
- **Design Meetings** – these are scheduled shortly after the Project Kick-off. A typical project consists of two – three design meetings over the space of one to two weeks. Those meetings are attended by the Avtex Project Manager and appropriate Technical Resource(s) and the client Project Manager/Lead, Contact Center Manager, and appropriate Technical Resources.
- **Status Meetings** – these are scheduled weekly, generally once the design is completed. These would include the Avtex Project Team and the key Client Project Team Members.
- **Transition to Support Meeting** – after the system is successfully in production the Avtex Project Manager, Avtex Support Manager and the Telephony and Contact Center System Administrator meet to transition support from the Project Team to the Avtex 24 x 7 Technical Assistance Center team.

**4.2.2.5.4** *Vendor must work with the WVOT using the established Telecommunications Change Request (TCR) (Attachment\_C) procedures for ordering and implementing these telecommunications services.*

Avtex will use its standard Project Change Management Process as a framework to adhere to the established TCR.

#### **Project Change Management Process**

Changes to the project Statement of Work will be negotiated separately through a client approved Project Change Management process. In the event either party desires to change this project, the following procedures shall apply:

- The party requesting the change will deliver a "Project Change Request," verbally, via email or a formal "Change Order" to the other party. The Project Change Request will describe the nature of the change, the reason for the change, and the effect the change will have on the Statement of Work, which may include changes to the Deliverables, Project fees and charges, and/or the schedule.
- A Project Change Request may be initiated either by Avtex or by client for any changes to the Statement of Work. The Project Manager of the requesting party will review the proposed change with his / her counterpart. The parties will evaluate the Project Change Request and negotiate in good faith the changes to the Services and the additional charges, if any, required to implement the Project Change Request. If both parties agree to implement the Project Change Request, the appropriate authorized representatives of the parties will sign a Project Change Order, indicating the acceptance of the changes by the parties.
- Upon execution of the Project Change Order, said Project Change Order will be incorporated into, and made a part of, this Statement of Work.
- No party is under any obligation to proceed with the Project Change Order until such time as the Project Change Order has been agreed upon by both parties
- Whenever there is a conflict between the terms and conditions set forth in a fully executed Project Change Order and those set forth in the original Statement of Work, or previous fully executed Project Change Order, the terms and conditions of the most recent fully executed Project Change Order shall prevail.

*4.2.2.5.5 Vendor billing errors must be credited back to the State from the effective date of the error. The State reserves the right to withhold payment until credit is received.*

Understood.

*4.2.2.5.6 For auditing, billing, and support purposes, the State requires any service with an associated rate to be identified on its monthly bill. As such, the State must be provided, at a minimum, the following:*

- *Billing Month*
- *Billed Entity Name*
- *Customer Name/Account (if different from billed entity)*
- *Service Location*
- *Service Period*
- *Itemized Cost for Individual Billing Components*
- *Itemized Call Detail*
- *Itemized Cost for Any One-Time or Non-Recurring Charges*
- *Itemized Cost for Any Surcharges and Total Cost*

*The cost identified in the bill must match the contract rates for the specified services. The Vendor must provide the State's monthly bill in an editable format such as Excel and/or csv.*

Understood.

*4.2.2.5.7 The Vendor must invoice on a consistent monthly billing cycle across all services. Services installed or disconnected for a partial month must be prorated based on the date the service is activated/accepted or disconnected. The Vendor must not bill the State of services until the services have been activated and accepted as functional. The Vendor shall not bill the State for services after the disconnect due date listed on the submitted TCR.*

Understood

4.2.2.5.8 *The Vendor must provide and update a weekly status report and/or order log for submitted TCRs.*

Understood.

4.2.2.5.9 *If, as part of its proposal, the Vendor submits appendices or other supplemental materials, the Vendor must denote specifically in those materials where the relevant information is located.*

Comply.

4.2.2.5.10 *The State expects full, complete, and timely cooperation in disentangling the relationship in the event that the Agreement expires or terminates for any reason. In the event of expiration or termination, the State expects that the Vendor shall, among other things: return all State data and documentation to the State, including but not limited to configuration information; transfer ownership of all leased equipment at no cost to the State (other than the payments already received by the Vendor under the Agreement); and, allow the State or the replacement provider(s) continued access to all billing, ordering, and trouble ticketing systems, and processes that have been employed in servicing the State, in accordance with methods and procedures to be agreed upon and established in the Agreement. Please acknowledge your acceptance of this.*

Comply.

**4.3. Qualifications and Experience:** *Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives were and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.*

**4.3.1. Qualification and Experience Information:** *Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.*

4.3.1.1. *Vendor should provide three (3) examples demonstrating at least three (3) years of experience in providing a Hosted VoIP solution of a similar size and scope - 15,000 users across 200 sites with one example being a public entity. Vendor should provide a summarization of each project including goals and objectives, total number of phones deployed per site, length of time deployment took, if still in service, and reference for each example.*

**Customer: The State of Indiana**

A Genesys customer for nearly 10 Years. They started out with a single agency BMV follow by FSSA/DFR and all the remaining agencies have migrated onto the Genesys solution over the past several years. The State of Indiana has standardized on Genesys as their Contact Center Platform and currently support over 6,000 agents across 20 plus agencies. These agencies include; BMV, FSSA/DFR, DWD, DOR, DCS – Hotline, DCS – Kidline, and 15 other smaller agencies. The State of Indiana utilizes the Genesys platform for routing voice and other digital channels across the agencies. Prior to standardizing on the Genesys, the state was challenged with:

- manage the various platforms
- keep a consistent support team in place.

- Since standardizing, the State of Indiana Office of Technology Team has improved
- Large reduction in the volume of trouble tickets while improving their SLA's to their agencies
- Increased Savings

Justin Davis from the State of Indiana recently spoke as a Subject Matter Expert on Modernizing the Contact Center for government agencies. He is an excellent reference for an agency or State that is forward looking and trying to understand how to leverage technology to drive real benefits for the Citizens of their State.

**Customer: Microsoft**

Microsoft has been a customer since 2014. Detail of customer experience below.

**Challenges**

- Complex IVR Migration from a legacy IVR solution
- Over 13 IVR applications / Over 800 Call Flow Blocks
- Over 14,000 Contact Center Agents
- Over 5,000 peak IVR ports
- Over 2.5 Million calls a month
- 141 Countries and 38 languages
- Integration to Legacy Cisco Call Center

**Solution**

- Migrated contact center agents from Cisco premise solution to Genesys BEC.
- Upon completion, Genesys BEC served as a consolidated IVR and Contact Center solution for Microsoft supporting over 14,000 concurrent agent seats.
- Designed the most complex IVR using speech natural language understanding.
- Detailed call records provide valuable IVR interaction details for troubleshooting, tuning, and business reporting
- The backend technology, Elastic Search, allows user to quickly search through the records, and provides build-in support of data aggregation to meet the needs for business reporting.

**Customer: The Ohio State University**

OSU has been a customer for more than 5 years.

They have between 4,500-6,000 users that are also running Skype For Business. The plan in the next year is to move toward the 10-12K lines on Skype for Business. They moved to Skype for Business and Polycom for a nimble and scalable voice platform to migrate users off POTS phone lines.

**Customer: West Virginia, The Secretary of State's Office**

Customer is live and running the entire Microsoft telephony stack. They are leveraging about 75 users today.



*4.3.1.2. Vendor should provide at least one (1) example demonstrating at least three (3) years of experience in providing single/multiple Hosted Call Center solutions of a similar size and scope - 500 users across 20 sites. Vendor should provide a summarization the project including goals and objectives, total number of agents per site, length of time deployment took, if still in service, and reference for the example.*

**Customer: Red Hat, Inc.**

As a leading global provider of open source software solutions, Red Hat operates from 80 offices and 30 countries and has more than 8,000 employees. Critical to the company's success is world-class customer service and IT support that is consistent across the globe. Red Hat has established a truly global service department of 500 contact center associates that's built on the Genesys Customer Experience Platform—a reliable, unified system deployed completely in the cloud. In partnership with Genesys, Red Hat has successfully laid the foundation for future phases, such as a universal queue of omnichannel customer interactions, that will enhance operational visibility and functionality

Challenges:

- Lack of true business continuity (BC) and HA
- Siloed, disconnected regional contact centers
- Unsupported rapid growth

By working with Genesys as a trusted partner, Red Hat has transformed their global CX. In the first three months after the Salesforce integration, Red Hat routed 15% of all calls to the last-assigned engineer and cut handling time by 10%. "By offering this solution in partnership with Genesys, we've really exceeded the goals and aspirations of our internal customers. Genesys makes us a better supplier to them, but more importantly, it makes them better solution providers to our customers," said Congdon (Red Hat CIO).

Results:

- Unmatched redundancy ensures BC
- Can take calls in minutes in case of an outage
- Improved workflow management and customer experience
- 10% reduction in handling time

Genesys can provide full customer success story, if requested. Above are highlights from the customer success story.

*4.3.1.3 The State desires an Account Team (including Account Support Representative, Technical Support Representative, Solution Implementation Support Representative, Contract Manager, Billing Support Representative, Security/Compliance Specialist, and Project Manager) for the winning solution and life of the contract. Vendor should describe in detail the responsibilities of key roles and staff's experience in working in these roles.*

Avtex has a long history with the Genesys solution. Avtex has been a Genesys partner for 21 years with many awards and accolades. We currently support 600 Genesys implementations. We have 63 Genesys engineers with on average 7.6 years of experience with the platform. Avtex boasts 508 total years of experience with the proposed platform.

The following are the common roles for a new contact center implementation. Sometimes a single person can play multiple roles depending on skill sets and experience. For additional work break down

of the project team roles see "Project Implementation on page 19 of Attachment SO-1 - Avtex - SoWV - Managed and Hosted Voice Services - Base Configuration SOW. The client project team is also very import. Those roles are also included below:

#### **Avtex Project Team**

- **Project Manager** – this resource is the main point of contact for the client project team throughout the project. The project manager is responsible for all standard project management tasks and communications during the implementation.
- **Contact Center Field Engineer** – this resource is responsible for any software installation that may be required if local devices are included in the architected solution and the configuration of the application based on the agreed upon design documentation that results from the design workshops.
- **Contact Center Developer** - this resource is responsible for configuration of systems that require special coding and any custom solution development, reporting, etc. that was included in the solution and agreed upon design.
- **Business Analyst** – this resource is responsible for meeting with your team to complete the design for the solution that you have purchased. This will include discussions around call flows, custom IVR requirements, users, workgroups, etc. The business analyst will work with the client team to capture all necessary design decisions in configuration playbooks, call flows and other design documentation.
- **Training Consultant** – this resource is responsible for work with the client on the training plan and delivering the train-the-trainer courses included in the project. Often the training consultant also leads the UAT Kick-off event.
- **QA Analyst / Tester** - this resource is responsible for conducting additional testing once the Engineers and/or Developers are done with their configuration and development prior to handing the solution off to the client for User Acceptance Testing.
- **WFM Consultant** – the WFM Consultant will work with your team to understand the client's WFM needs and apply those needs to the best use of the WFM application.

#### **Avtex Support Team**

- **Client Account Manager** - Your CAM is a valuable point of contact within Avtex. CAM's are assigned to specific accounts, so they can become knowledgeable about your business and how our technologies have been implemented within your company. Through gaining an understanding of your systems configuration, including applications, your CAM will be able to discuss your business needs and make recommendations that ensure you are maximizing your investment.
- **Escalation Manager** - The role of the Avtex Escalation Managers is to ensure support incidents are brought to resolution in a timely manner and prioritize issues internally within Avtex as well as with vendors should an escalation be warranted.
- **Technical Assistance Center Support Team** – the project team will officially transition the customer over to the Avtex Technical Assistance Center Support Team at the end of the implementation. This team will become the main point of contact for the client once the implementation is completed.

#### **Client Project Team**

- **Executive Sponsor** – this resource is generally an executive level resource not involved in the day to day of the project but has a vested interest in the overall success of the project and often is the person responsible for financially authorizing the project. This resource may be asked to participate in an escalation if different business units within the project may not agree on the business goals or other competing business priorities need to be evaluated against the project.

- **Project Sponsor** – this resource may not be involved in the day to day of the project but is responsible successful outcome of the project. This person would be the escalation contact within the client organization for issues or questions the client Project Manager/Lead cannot address or may not have the authority to address for some reason. The project sponsor is primarily responsible for ensuring that the project delivers the agreed upon business benefits.
- **Project Manager/Lead** – this resource is the single point of contact for the Avtex Project Manager and is responsible for organizing and managing assigned tasks within the client team. The client Project Manager / Lead is responsible for ensuring that the client assigned project tasks are completed, client-side resources needed are available and ensuring any client-side constraints and concerns are brought to the Avtex Project Manager in a timely manner.
- **IT Manager/Lead** – this resource would be responsible for ensuring any client IT requirements are met. They may delegate those tasks to others on their team but are ultimately responsible for their completion.
- **Telephony System Administrator** – this is the resource that will be responsible for the day to day management and administration of the Genesys Cloud solution once implemented. They may or may not be responsible for the current system. They are likely the person responsible for working with the Carrier.
- **Contact Center Manager** – this resource is responsible for the business. If the project includes Contact Centers from various business units each should be represented. This resource would be critical for design and testing. The project may include others from this person's organization, i.e. Supervisor, Agent, etc., but the ultimate responsibility and decisions for the system functionality falls on them.
- **Contact Center System Users** – these resources are generally required during the customer User Acceptance Testing period as testers to execute the required business test cases. The number of testers will depend on the number of test cases and their complexity.
- **Business User** – this resource generally is involved in the customer User Acceptance Testing to ensure the business only phone users have the full required functionality.
- **Trainer** – this resource(s) will be responsible for building the client End User Training documentation and training sessions and training your agents and supervisors prior to cutover. The trainer would participate in the Train-the-Trainer sessions and can begin building training once that is completed and UAT has begun so they have access to the configured system.

*4.3.1.4 Vendor should describe its experience and process in conducting cyber risk management ensuring shared risk is identified, assessed, communicated, and managed.*

The Genesys Cloud is deployed for multiple secure customers. These include customers that need support for PCI, HIPPA, and other standards. The Genesys team works with customer's security teams to identify and address security needs and concerns. See response to Question 4.3.1.3.

*4.3.1.5 Vendor should describe its experience and process for conducting NIST SP 800-53 security assessment and authorization control families' activities, designed to ensure each vendor-provided solution implementation adheres to security and privacy requirements before being placed into production.*

The Genesys Cloud product is certified for DoD deployments by the Joint Interoperability Testing Command (JITC), which follows a rigorous testing process based on NIST 800-53 and may help customers to achieve or maintain FISMA compliance.

*4.3.1.6 Vendor should list all government or standards organization security certifications it currently holds that apply specifically to the vendor's proposal, as well as those in process at time of response. Specifically include HIPAA, CMS, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.*

Genesys Cloud is an SSAE 16 SOC2, Type II compliant cloud service. Genesys Cloud achieved SSAE16, SOC 2, Type II certification in July 2013 and received current attestation in 2018. In addition, we have built and assessed a dedicated cloud environment, within our US data centers, that has been attested for PCI DSS compliance by an independent Qualified Security Assessor (QSA).

Genesys Cloud has been independently audited in accordance with SSAE 16 standards. This audit and report are designed to attest that design and operative effectiveness of security controls that the Genesys has implemented are in accordance to the defined Trust Principles of Security, Availability, Processing Integrity, and Confidentiality.

The Genesys Cloud product is certified for DoD deployments by the JITC, which follows a rigorous testing process based on NIST 800-53 and may help customers to achieve or maintain FISMA compliance.

*4.3.1.7 Vendor should provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRAMP), and certifications relating to cybersecurity and privacy controls.*

Genesys Cloud is an SSAE 16 SOC2, Type II compliant cloud service. Genesys Cloud achieved SSAE16, SOC 2, Type II certification in July 2013 and received current attestation in 2018. In addition, we have built and assessed a dedicated cloud environment, within our US data centers, that has been attested for PCI DSS compliance by an independent Qualified Security Assessor (QSA).

Genesys Cloud has been independently audited in accordance with SSAE 16 standards. This audit and report are designed to attest that design and operative effectiveness of security controls that the Genesys has implemented are in accordance to the defined Trust Principles of Security, Availability, Processing Integrity, and Confidentiality.

Genesys Cloud performs regular external vulnerability scans on the environment. The scans are reviewed on a bi-weekly basis by the security and operations teams. The Genesys Cloud annual SSAE 16 SOC2 attestation report was reviewed and any issues identified and have either been remediated or are in the process of remediation.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Genesys Cloud environment is not FedRAMP compliant, but Genesys Cloud Operations achieved SSAE-16 SOC 2, Type II certification. FedRAMP certification is being pursued, with the target of completion in 2019 Q3.

*4.3.1.8 Vendor should describe its experience and capabilities in supporting their customers concerning compliance audits when the vendor-supplied solution is within the scope of audit.*

The Genesys Cloud is deployed for multiple secure customers. These include customers that need support for PCI, HIPPA, and other standards. The Genesys team works with customers security teams to identify and address security needs and concerns.

*4.3.1.9 Vendor should describe its experience and provide an overview of their incident management process and cyber threat intelligence sharing process for incidents associated with the vendor provided solution.*

Genesys has implemented a Security Incident and Event Monitoring solution (SIEM) that collects information from various sources and is monitored by the NOC and security engineering team. The incident response program is based on industry best practices. The goal of the incident management program is to minimize the adverse impact of incidents resulting from issues within the Genesys environment and to prevent the recurrence of incidents related to those issues. It is designed to identify, contain, and eradicate the root cause of incidents through investigation and analysis. Upon identification of the root cause, the Security Incident Response Team (SIRT) works to eradicate the issue and implements corrective and preventive actions with the appropriate team members to resolve the underlying problem, thus reducing the likelihood of recurrence. These might include changes to internal processes, procedures, and/or infrastructure.

SIRT is a cross disciplinary team. The program is overseen by Information Security but involves subject matter experts from across the organization, and supplemental experts are available to assist where necessary.

**4.4. Oral Presentations:** *The Agency will require oral presentations of all Vendors participating in the RFP process. The date of the presentations will be determined at a later time and all vendors will be notified in advance. During oral presentations, Vendors may not alter or add to their submitted proposal, but only clarify information. A description of the materials and information to be presented is provided below:*

*Materials and Information Requested at Oral Presentation:*

*4.4.1. Summary of solution, including product and support offerings, ability to deliver the solution in the specified timeframes, and experience in providing managed and hosted voice solutions.*

*4.4.2. The State will ask clarifying questions regarding the Vendor's submitted technical response.*

*4.4.3. Contact Center Presentation to see a live demonstration of Vendor's offering.*

Read and understood.



## **SECTION 5: VENDOR PROPOSAL**

**5.1. Economy of Preparation:** *Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.*

**5.2. Incurring Cost:** *Neither the State nor any of its employees or officers shall be held liable for any expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.*

**5.3. Proposal Format:** *Vendors should provide responses in the format listed below:*

**5.3.1. Two-Part Submission:** *Vendors must submit proposals in two received submitted in two distinct parts: technical and cost. Technical proposals must not contain any cost information relating to the project. Cost proposal must contain all cost information and must be sealed in a separate envelope from the technical proposal to facilitate a secondary cost proposal opening.*

**5.3.2. Title Page:** *State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature and date.*

**5.3.3. Table of Contents:** *Clearly identify the material by section and page number.*

**5.3.4. Response Reference:** *Vendor's response should clearly reference how the information provided applies to the RFP request. For example, listing the RFP number and restating the RFP request as a header in the proposal would be considered a clear reference.*

**5.3.5. Proposal Submission:** *All proposals must be submitted to the Purchasing Division prior to the date and time stipulated in the RFP as the opening date. All submissions must be in accordance with the provisions listed in Section 2: Instructions to Bidders Submitting Bids.*


Read and understood.

## ATTACHMENTS

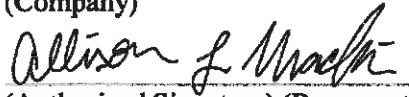
### Signature Pages

Please find the attachments beginning on the following page.

**DESIGNATED CONTACT:** Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

  
Government Account Representative  
\_\_\_\_\_  
(Name, Title)  
Zachary Kutyn, Government Account Representative  
\_\_\_\_\_  
(Printed Name and Title)  
1860 Michael Faraday Drive, Suite 100, Reston, VA 20190  
\_\_\_\_\_  
(Address)  
(703) 921-4059 / (703) 871-8505  
\_\_\_\_\_  
(Phone Number) / (Fax Number)  
Zachary.Kutyn@carahsoft.com  
\_\_\_\_\_  
(email address)

**CERTIFICATION AND SIGNATURE:** By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Carahsoft Technology Corporation  
\_\_\_\_\_  
(Company)  
 Team Lead  
\_\_\_\_\_  
(Authorized Signature) (Representative Name, Title)

Allison Mackin, Team Lead  
\_\_\_\_\_  
(Printed Name and Title of Authorized Representative)

11/26/2018  
\_\_\_\_\_  
(Date)

(703) 889-9819 / (703) 871-8505  
\_\_\_\_\_  
(Phone Number) (Fax Number)

Proposal 1: Step 1 –  $\$1,000,000 / \$1,000,000 = \text{Cost Score Percentage of } 1 \text{ (100\%)}$   
Step 2 –  $1 \times 30 = \text{Total Cost Score of } 30$

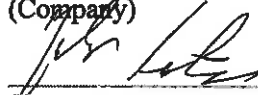
Proposal 2: Step 1 –  $\$1,000,000 / \$1,100,000 = \text{Cost Score Percentage of } 0.909091 \text{ (90.9091\%)}$   
Step 2 –  $0.909091 \times 30 = \text{Total Cost Score of } 27.27273$

**6.8. Availability of Information:** Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Carahsoft Technology Corporation

(Company)



Zachary Kutyn, Government Account Representative

(Representative Name, Title)

(703) 921-4059 / (703) 871-8505

(Contact Phone/Fax Number)

11/26/2018

(Date)

## Addendum Acknowledgement Form

Please find the attachment on the following page.



**ADDENDUM ACKNOWLEDGEMENT FORM**  
**SOLICITATION NO.: CRFP 0212 SWC190000001**

**Instructions:** Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

**Acknowledgment:** I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

**Addendum Numbers Received:**


(Check the box next to each addendum received)

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6  |
| <input checked="" type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7  |
| <input checked="" type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8  |
| <input checked="" type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9  |
| <input checked="" type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Carahsoft Technology Corporation

Company



Authorized Signature

11/26/2018

Date

**NOTE:** This addendum acknowledgement should be submitted with the bid to expedite document processing.

## **Purchasing Affidavit**

Please find the attachment on the following page.

STATE OF WEST VIRGINIA  
Purchasing Division

# PURCHASING AFFIDAVIT

**CONSTRUCTION CONTRACTS:** Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

**ALL CONTRACTS:** Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

**EXCEPTION:** The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

**DEFINITIONS:**

**"Debt"** means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

**"Employer default"** means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

**"Related party"** means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceeds five percent of the total contract amount.

**AFFIRMATION:** By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (W. Va. Code §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

**WITNESS THE FOLLOWING SIGNATURE:**

Vendor's Name: Carahsoft Technology Corporation

Authorized Signature: *[Signature]* Date: 11/26/2018

State of Virginia

County of Fairfax, to-wit:

Taken, subscribed, and sworn to before me this 26 day of Nov, 2018.

My Commission expires 12/31/19, 20  .

AFFIX SEAL HERE



NOTARY PUBLIC *[Signature]*

## **Attachment 4.2.1.1.1.1-7 - Avtex - State of West Virginia Support Handbook**

Please find the attachment beginning on the following page.



# Support Handbook



PureConnect  
Cloud



**A.V.TE.X:** (noun) - The **AdVantage** that **TEchnology** has when applied to **cX** strategy



**Strategy**- Avtex offers comprehensive CX consulting services including customer journey mapping, technology review and process planning to help you create a strategy for successful interactions.

**Implementation**- From planning to cross platform integrations, Avtex guides your business through the implementation process to optimize your CX ecosystem for today and into the future.

**Innovation**- Through creative utilization of your current technology, exploration of new platforms or development of a custom application, Avtex helps you keep pace with ever-evolving customer expectations.

**Management**- Avtex offers full-service application, license, hosting, and platform management services to keep your ecosystem performing at optimal levels.

## Vision

Fueling Exceptional Customer Experiences

## Mission

Using our technical know-how to enable our clients to deliver an exceptional experience to their customers

## North Star

Everything we do, everyday adds fuel to exceptional experiences



### Excellence

We help our customers be the best as we strive to be the best. We create a great experience for our customers so they can do the same for theirs.



### Innovation

We push the boundaries of technology for our customers. With the Avtex 360 approach, there is a perfect solution for your next project.



### Integrity

We're honest with our clients and provide the best service. We do whatever it takes to make your project a success so you can provide the ultimate experience for your customers.



### Passion

We love our customers and the work that we do! We take pride in the work we do and providing the best possible customer experience.

# Table of Contents

<b>General Support</b> .....	<b>3</b>
<b>1.1: Contacting Support</b> .....	<b>3</b>
Regular Business Hours:.....	3
After Hours and Holidays.....	5
<b>1.2: Opening a CTN – What to Expect</b> .....	<b>6</b>
<b>1.3: Service Level Objectives</b> .....	<b>9</b>
<b>1.4: Escalation</b> .....	<b>10</b>
<b>1.5: Evaluate the Support We Provide</b> .....	<b>11</b>
<b>1.6: Client OnPoint Portal</b> .....	<b>13</b>
<b>1.7: The Role of the Client Account Manager (CAM)</b> .....	<b>15</b>
<b>1.9: Change Order Process and Enhancement Requests</b> .....	<b>15</b>
<b>1.10: Remote Access Requirements</b> .....	<b>16</b>
<b>1.11: Training Offerings</b> .....	<b>17</b>
<b>1.12: Reporting</b> .....	<b>17</b>
<b>1.13: UX Services</b> .....	<b>18</b>
<b>1.14: CX Services</b> .....	<b>19</b>
<b>1.15: Business Intelligence</b> .....	<b>20</b>
<b>PureConnect Cloud Solutions</b> .....	<b>21</b>
<b>2.1: Services Provided with a Warranty or Support Agreement</b> .....	<b>21</b>
<b>2.2: Managed Services Offerings</b> .....	<b>23</b>
Move, Add, Change, Delete (MACD) .....	23
Tier One Troubleshooting.....	24
Support Database Integration .....	24
Proactive Monitoring and Alerting .....	24
Microsoft OS Patching .....	24
Staffing options .....	25
Avtex Voice Performance Readiness & Optimization (AVPRO).....	25
Avtex Quick Voice Assessment (QVA) .....	27
Voice Readiness Assessment (VRA).....	29
Network Consulting Services.....	33
Disaster Recovery as a Service (DRaaS).....	34
<b>2.3: Enhancement Requests</b> .....	<b>35</b>
<b>2.4: Security</b> .....	<b>35</b>
User Passcode Security.....	36
Setting Default Passcode Policy.....	36
<b>2.5: Repair Process for Avtex Provided Telephones and Headsets</b> .....	<b>37</b>
<b>Conclusion</b> .....	<b>37</b>

# General Support

## 1.1: Contacting Support

Avtex records all calls into our support center and logs all interactions in our client database and service application. At your discretion, you may request a service summary of work performed on your system. Requests for service on your system must come from a designated site contact. Information explaining how you can review your service history online can be found in [Section 1.6 Client OnPoint Portal](#).

Requests received by individuals from your company who are not listed as valid contacts in our database may be delayed as we attempt to reach a preauthorized contact for permission to proceed. For these reasons, we ask that you notify your Avtex CAM (Client Account Manager) of any changes to the list of employees within your company who are authorized to call and request assistance.

### Regular Business Hours:

The Support organization is staffed Monday - Friday from 7:00 a.m. to 7:00 p.m. Central (excluding holidays). During the regular business day, there are several ways you can contact Avtex to obtain support. All requests should be directed to support, rather than to a specific Avtex employee. You can reach support by dialing:

- 1-952-831-0888 or 1-800-323-3639
- Then speak "Support" or choose Option 1 for Support.
- You will be asked to speak or enter your Account or CTN number
- If you do not know your Account or CTN number, please speak "I do not know"

If you are calling due to a system **Emergency** or severe system-affecting problem, you should say "Support" or select **Option 1**. Additionally, you can say "**Down**" at any time at which time your call will receive priority routing and will be transferred to live assistance.

If you are contacting Avtex to report a problem or open a service request that is not an emergency, you may submit your request in one of the following ways:

1. If you would like to review and discuss your service request with a representative you may speak or select **Option 2**, after your initial product selection and you will be routed to the next available representative.
2. After your initial selection, speak or press 3 to leave a voice mail message. A client ticket number (CTN) will be generated and the first available team member will be assigned to the ticket. You will then be contacted by a Support Representative and given the CTN number for your reference. (All voice mail messages will be queued, along with email messages, and processed in the order in which they are received.)
3. E-Mail requests for support should be sent to [TAC@Avtex.com](mailto:TAC@Avtex.com)

All emails will be queued, along with voice mail messages and processed in the order they are received.

Please do not send an email to a specific employee's email address. Sending a message to a specific employee's email box does not guarantee that it will be acknowledged or acted on in a timely manner.

4. You may open a request for assistance via the web at <https://onpoint.avtex.com>

When opening a new incident, you will be asked to categorize the severity.

- **Emergency** *(Requires a live call into support)*
- **High**
- **Medium** *(Default if not specified)*
- **Low**
- **MACD** *(Move, Add, Change or Delete)*

If at any time you feel the priority of your issues needs to change, simply ask and we will respond accordingly.

Following these procedures will ensure that your service request is properly documented and addressed in a timely manner.



**For After Hours Emergency**

**1-952-831-0888 or 1-800-323-3639**

**Press 1 for Emergency Support**

## After Hours and Holidays

If your system is down, or you are experiencing other major problems that require immediate assistance, dial 952-831-0888 or 800-323-3639, follow the menu prompts and speak "Support" or select Option 1 for After Hours Emergency Support.

Your call will be routed to the Avtex answering service. When your call is answered you will be asked for the following information:

- Your name
- Your company name
- Your telephone number
- A brief description of the problem you are reporting
- Business impact

The representative will place you on hold while a designated Avtex resource is contacted; next you will be placed in conference with the Avtex resource. If you choose not to hold, you may leave your contact information with the answering service and an Avtex resource will call you back within 30 minutes.

When you call Avtex for after-hours support and must leave a number where you may be contacted live.

Avtex defines system emergencies as major system hardware, software, or application outages that impact your company's ability to receive or make calls and perform other critical system or application functions.

### Major Problems Defined

- Unscheduled total system outage and failure to reboot for any reason.
- Inability to access the system through 25% or more of all ports.
- Loss of system integration.
- Continual system restarts or failovers.
- Loss of dial tone on more than 25% of system.

Avtex will ask our clients to categorize the severity of their issue and will respond accordingly. While our goal is to provide the best client experience possible, we do ask our clients to use the severity coding appropriately.



## 1.2: Opening a CTN – What to Expect

As stated earlier in [Section 1.1: Contacting Avtex](#), a service request can be opened with Avtex via live call, email, or online. Live queue interactions are answered between 7:00 a.m. and 7:00 p.m. Central, Monday – Friday (excluding holidays). However, you may leave a message, 24 hours a day.

If you are experiencing a system emergency or service-impacting issue during business hours, please call our Support Organization. In addition to calling us, an email with pertinent information can be sent, however, please do not use an email as the primary mode to report emergency situations. E-mail and voice mail queues are only monitored during business hours. The only way to be guaranteed priority routing is by calling and selecting the menu option for a system down emergency.

The following steps are taken for each service request the team receives:

- Team member opens a Client Ticket Number, (CTN), entering the request and contact information.
- Team member provides CTN information to Responsible (client) Contact.
- Team member performs system diagnostics and processes the request. Team member updates the resolution portion of the CTN.

When opening a new incident, you will be asked to categorize the severity.

- **Emergency** (*Requires a live call into support*)
- **High**
- **Medium** (*Default if not specified*)
- **Low**
- **MACD** (*Move, Add, Change or Delete*)

The priority level is based on the impact the reported problem has on the system. As stated earlier, system down calls are given **Emergency** priority and will immediately be routed to a representative and a CTN will be opened. If you are calling to report a “system down” or “system affecting problem”, as identified by the criteria in [Section 1.1: Contacting Avtex](#)

A team member will immediately attempt to connect to the system, and/or work with you until the problem has been resolved. If the root cause of the problem has not been identified after conducting the required system triage, or if a path has not been outlined to achieve problem resolution, the CTN will be escalated as outlined in [Section 1.3: Service Response](#) and [1.4: Escalation](#)

Note: A CTN that is opened and assigned an **Emergency** or **High** priority automatically triggers email notification to Avtex Support Management, the Account Executive and the CAM on record for your company.

As a reminder, non-urgent interactions will be queued for the next available team member. Once your interaction is answered, our team member will open a ticket and review the service request with you. Calls that are answered live during the business day that do not meet the system emergency criteria will be addressed in

the order that they are received, along with email and online requests. Response times for non-emergency service requests are outlined in [Section 1.1: Contacting Avtex](#) of this handbook.

### Information you will be requested to provide when opening a CTN

In general, the following pieces of information must be provided, or questions must be answered as part of our initial triage procedures. This information helps to facilitate the successful resolution of your request. Having as much of this information as possible at the time you open your request will help eliminate potential delays in troubleshooting and CTN resolution.

- Date and time of occurrence.
- Who is affected?
- Users, Locations, etc...
- Is more than one user experiencing the same issue?
- Can the problem be reproduced?
- Have you verified that there are no network problems which could be contributing to the issue?
- When was the first reported occurrence of the problem?
- Are screen shots available?
- Are log files available?
- Call ID if applicable.
- Is there already an active Avtex CTN open for this issue?

If at any time you feel the priority of your issues needs to change, simply ask and we will respond accordingly.

- Anytime a CTN is Opened, Updated or Resolved the assigned Responsible Contact will receive an email notification (shown Below). Please click on the CTN number hyperlink to be routed to the Avtex OnPoint portal and provide your updates directly into the CTN notes

- Sample email

Dear Customer Name,

Your service request is currently being worked on by the Avtex Support team. You can view the full history of the ticket, check updates, or add an update by following this link

699303

**Title:** Title of Incident Here

**CTN:** 699303

**Status:** In Progress

**Priority:** Medium

**Total Time:** 15 minutes

**Issue Description:** Sample Incident.

Updates:

- **Date:** 7/24/2017 2:13PM  
**Time:** 0.25  
**Cost Category:** AVTE DESKTOP - SUPPORT-COVERED  
**Work Performed On:** 7/24/2017  
**Work done by:** Test Engineer  
**Opened CTN and placed in Queue**

## 1.3: Service Level Objectives

Our goal to respond to all service requests within the timeframes outlined below.

Priority	Business hours	Non-Business hours and Holidays	Hours of Activity
<b>Emergency</b> <i>Requires live call into queue</i>	Initial Contact: Immediate Follow-up: Constant	Contact: 30 min Follow-up: Hourly Escalation: 4 Hours	24 x 7
<b>High</b> <i>Live call into queue</i>	Initial Contact: Immediate Follow-up Service Level: Daily	Contact: 10:00 AM Central next business day Follow-up Service Level: Daily	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>High</b> <i>OnPoint or E-Mail</i>	Initial Contact: 4 Hours Follow-up Service Level: Daily	Contact: 10:00 AM Central next business day Follow-up Service Level: Daily	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Medium</b> <i>All interaction types</i>	Initial Contact: 4 Hours Follow-up Service Level: 3 business Days	Contact: 10:00 AM Central next business day Follow-up Service Level: 3 business Days	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Low</b> <i>All interaction types</i>	Initial Contact: 4 Hours Follow-up Service Level: 5 Business Days	Contact: 10:00 AM Central next business day Follow-up Service Level: 5 Business Days	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Move, Add, Change</b> <i>All interaction types</i>	Requests will be completed within 2 business days after receipt of the request	Changes will be scheduled during Avtex business hours and will be completed within 2 business days after receipt of the request	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays

### CTN Updates

The below table defines the “Warning” and “Past Due” alerting in place to ensure CTN’s are being updated in a timely manner.

Updates to engineer Time Tracking, the CTN “Notes” filed and or notes added via the OnPoint client portal will reset the timer on a CTN.

Warning and Past Due emails are sent to the CTN “Owner” and Avtex Support Management

Contact Center Support		
Priority	Warning email (Business Hours)	Past Due email (Business Hours)
Emergency		2
High	8	12
Medium	24	36
Low	48	60
MACD	12	24
Notes		





## 1.5: Evaluate the Support We Provide

The email sent to you confirming that a CTN has been closed will also include a survey.

Sample of e-mail you should receive when closing a CTN:

Dear Customer,

To help us better serve you, please click on the link below to take our brief survey. We value your opinion about our service and how effectively we resolved your support issue.

[Please click here to take the survey.](#)

Thank you!

Support Management

*Relevant information/history:*

CTN Number:

Issue Description:

Please call our support number with any questions at (952) 831-0888.

Thank you for choosing Avtex!

By clicking on the link in the email, you can complete a quick 6 question survey to evaluate our performance on the service request.

We thank you for your business and sincerely want to improve our services in every aspect of our interaction with our customers. Please take a few moments to provide honest feedback regarding our processes and people so that we may provide you with even greater levels of service in future projects.

**Name:** Jon Walker  
**Company:** Avtex  
**Date:** 03-January, 1:53 PM  
**Case Number:** 651810

1 = Strongly disagree  
 5 = Strongly agree

- |  |                         |                         |                         |                         |                         |                           |
|--|-------------------------|-------------------------|-------------------------|-------------------------|-------------------------|---------------------------|
| 1. The Avtex engineer(s) that I worked with were knowledgeable.                | <input type="radio"/> 1 | <input type="radio"/> 2 | <input type="radio"/> 3 | <input type="radio"/> 4 | <input type="radio"/> 5 | <input type="radio"/> n/a |
| 2. The engineer(s) asked appropriate, precise questions to diagnose the issue. | <input type="radio"/> 1 | <input type="radio"/> 2 | <input type="radio"/> 3 | <input type="radio"/> 4 | <input type="radio"/> 5 | <input type="radio"/> n/a |
| 3. Avtex made it easy for me to handle my issue.                               | <input type="radio"/> 1 | <input type="radio"/> 2 | <input type="radio"/> 3 | <input type="radio"/> 4 | <input type="radio"/> 5 | <input type="radio"/> n/a |
| 4. I received timely status updates on my service request.                     | <input type="radio"/> 1 | <input type="radio"/> 2 | <input type="radio"/> 3 | <input type="radio"/> 4 | <input type="radio"/> 5 | <input type="radio"/> n/a |
| 5. I am satisfied with the resolution of my issue.*                            | <input type="radio"/> 1 | <input type="radio"/> 2 | <input type="radio"/> 3 | <input type="radio"/> 4 | <input type="radio"/> 5 | <input type="radio"/> n/a |
| 6. I believe my issue was resolved in a timely manner.*                        | <input type="radio"/> 1 | <input type="radio"/> 2 | <input type="radio"/> 3 | <input type="radio"/> 4 | <input type="radio"/> 5 | <input type="radio"/> n/a |

Comments...

Thank you!

[Submit Results](#)

\* If your issue is not fully resolved because it was passed to another entity, please check "n/a" for this question.

Survey data is reviewed regularly and used to help us evaluate staffing, training, coaching needs, quality assurance and more. We value your feedback and encourage you to participate in the survey for each CTN. You will always have a chance to provide immediate feedback on how we are doing!

In addition to reviewing survey data, random recordings of all support interactions are reviewed monthly for quality assurance and mentoring.

## 1.6: Client OnPoint Portal

It is the goal to provide regular and timely updates on all open cases. In addition to the updates Avtex provides, Avtex provides clients with access to its Client Support Portal. The Avtex Client Support Portal is a convenient way for clients to review and update their active cases and more.

The Avtex Client Support Portal is located at <https://onpoint.avtex.com>. It can also be accessed from the main Avtex website [www.avtex.com](http://www.avtex.com) by clicking Support

The Avtex Client Support Portal provides clients with the following features:

### Account

- Register for an Avtex Client Support Portal account.  
Note: First time users will need to register an account to access Avtex Client Support portal services and resources.

### Review CTN's

- Review active, resolved and/or cancelled CTN's
- Create new CTN's
- Monitor CTN status and updates
- Add updates or attachments to existing CTN's
- Export CTN histories

## Projects

- Review active projects
- Review documentation, status updates and other information on current projects

## Avtex Team

- Contact information for your Avtex Team



# Avtex

3500 American Blvd W Bloomington, MN 55431 // P: (952) 646-0800

Account Code: AVTE001

[My Support Requests](#) [Projects](#) [Avtex Team](#) [Contact](#)

## Active Projects

Project	Description	Last Modified Date
Avtex UniPoint		1/20/2014 11:35:43 AM
Open Air Initial Deployment	Open Air Initial Deployment	1/21/2014 6:50:21 AM

[My Support Requests](#) [Projects](#) [Avtex Team](#) [Contact](#)

## Open Support Tickets

[Export](#)

Search by Keyword

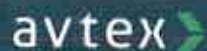
Active

-Any-

Last Month

[Search](#)

CTN	Title	Ref #	Location	Opened By	Priority	Subject	Status	Created	Updated
604436	Missing Emails		Avtex - Bloomington MN	Laurel Hess	Medium	Managed Services	Active	1/23/2014 9:59 AM	1/23/2014 9:59 AM
604424	Avtex Misc		Avtex - Bloomington MN	Mitch Suzmore	Medium	interactive intelligence	Active	1/23/2014 6:10 AM	1/23/2014 6:22 AM



## 1.7: The Role of the Client Account Manager (CAM)

Your Client Account Manager (CAM) is a valuable point of contact within Avtex. CAM's are assigned to specific accounts, so they can become knowledgeable about your business and how our technologies have been implemented within your company. Through gaining an understanding of your systems configuration, including applications, your CAM will be able to discuss your business needs and make recommendations that ensure you are maximizing your investment.

CAMs are also responsible for conducting Business Review meetings with you. During this meeting, the CAM will provide a summary of the service on your system, a status update on projects in flight, and allow you to discuss any upcoming business initiatives that could affect your environment. Knowing about your company initiatives allows Avtex to be proactive in coordinating enhancements or changes to your environment. Our goal is to be a partner not just a vendor.

Your CAM can also act as an escalation point within Avtex. If you have any type of issue and you are unsure of whom to contact, your CAM will ensure that the correct parties are engaged.

Your CAM will also coordinate your annual Client Support Agreement (CSA), which covers software and hardware maintenance for your system(s). Prior to the expiration of the existing agreement (or warranty period), a renewal notice will be sent to you. Your CAM will work with you to get the agreement signed and avoid a disruption in service.

Overall the CAM is responsible for maintaining and enhancing the client relationship.

## 1.9: Change Order Process and Enhancement Requests

### The Change Order Process

The change order process is in place to provide a method for tracking system software, hardware and custom application changes. We ask that you follow this procedure, so we can guarantee timely delivery of client requests.

Your CAM should be your first point of contact when requesting changes. CAM's are dedicated to specific accounts, so they understand your configuration and existing applications. By following the change order process, you can implement enhancements with ease.

The following steps outline the change order process:

1. Contact your CAM to discuss your proposed change. Depending on the magnitude of your request, a meeting may be scheduled with key personnel. A timeframe for delivery will also be determined.
2. Your CAM will document.
3. Once the project has been defined, the CAM will submit it to a Project Engineer for pricing.
4. The CAM will then complete a Change Order or formal proposal for work when appropriate, including pricing, and e-mail it to you for review and signature.
5. Once Avtex has received the signed change order, a project team will be assigned, and completion date assigned.



6. Upon completion, a final invoice will be generated.

As a reminder, this process should be followed when you want to create a new application, modify an existing application, or add hardware or licenses to your system. Payment terms will be defined in the Change Order or Proposal for work.

## 1.10: Remote Access Requirements

Note: This section only applies to Premise based devices supporting a “Local Control” model

i.e. Edge Devices, Gateway's, SIP Proxy where applicable

Avtex requires remote access for support on your system(s). If remote access is restricted, Avtex cannot guarantee service response times.

### Kaseya – Preferred Access Method

*NOTE: Kaseya or client provided remote access will be used for Premised based servers and devices. Terminal Services Remote Access – TSRA will be used for access to PureConnect Cloud based servers and devices*

Kaseya is a self-hosted application that will allow Avtex to efficiently access your organization. Kaseya equips our staff with a comprehensive set of tools including: session recording and complete system control or client collaboration. Remote control sessions speed up the process of diagnosing and fixing problems and allow Avtex to remotely maintain attended or unattended computers and servers. Kaseya applies the highest levels of security throughout the entire support process. Strong passwords along with SSL and 256-bit AES encryption protect your systems from login to logout. All information is encrypted before it is transferred.

In addition to the ease and security of the product, Kaseya keeps detailed information about the who, what and when of a session. An access-detailed, text-based account of every action that occurred during the remote-control session is available to Avtex management.

### Other Access options

- LogMeIn
- Join.me
- NT Utilities

## 1.11: Training Offerings

At Avtex, we believe that education is critical to the success of our clients. We understand that as time goes on, your company may experience growth, turnover, or simply decide it's time to become more hands on. To help keep or bring your staff up to speed, Avtex offers a comprehensive education curriculum. Details can be found on the Avtex web site at <http://www.avtex.com/training/>

- Private and Public Training Options
  - Private Onsite or Online Instructure Led
  - Public Online Instructor Led
    - For registration and use of support covered training hours please contact [TrainingRegistration@Avtex.com](mailto:TrainingRegistration@Avtex.com)
- Training Courses on PureConnect and PureCloud Solutions
- Private Train-the-Trainer or End User Audience Options
- Private Custom Build Option
- 30+ Private Training Courses and 25+ Public Training Courses Offered
- 8 Hours of Training included in PureConnect and PureCloud Premier and PureConnect Cloud Enhanced Support Plans

For additional information and assistance please contact your CAM.

## 1.12: Reporting

Many of our Managed Services Clients elect to receive monthly reports to monitor the state of their environment. These reports can help clients identify certain technologies in their environment that may need to be improved or re-evaluated. These reports can also be used to help understand the volume of service requests their company is making, time to resolution, etc. Areas that are typically monitored and reported to clients include but are not limited to:

- Server uptime and disk health
- Number of service requests opened and closed
- Average time for resolution
- Types of service requests made (password resets, account unlocks, etc.)

Again, these are just a small sample of the reporting Avtex can provide, if there are certain performance indicators you would like to track and receive reports on, please contact your CAM to request your reports.

## 1.13: UX Services

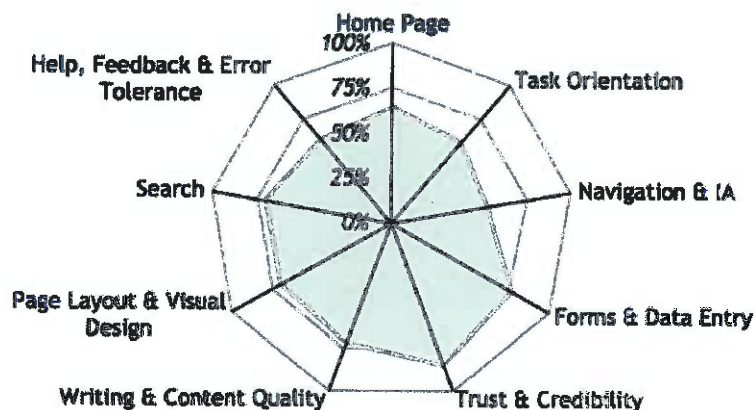
A User Experience (UX) Assessment is an **objective** analysis of a website, mobile application, business application or intranet designed to provide **actionable** feedback. It is an evaluation of **current state** with a report outlining practical **future state** solutions.

- Heuristic Evaluation – Score Card
- Detailed Findings Report
- Presentation of Results

Criteria	Score
The site avoids unnecessary registration and distracting information	1
Excessive use of scripts, applets, movies, audio files, graphics and images has been avoided	1
The site avoids unnecessary registration	0
The critical path (e.g. purchase, subscription) is clear, with no distractions on route	0
Information is presented in a simple, natural and logical order	0
The number of screens required per task has been minimised	-1

Comments
The site does not present unnecessary registration tools however it does label links to sensitive content as "Members Only" which implies users is required and creates a barrier. The process could be streamlined through content and explanation of the membership types up front. This would eliminate a step in the process.
I think there are opportunities to reduce the number of required steps and screens on many processes. However, it is understandable that some structures may be in place to accommodate

- Rapid Turn Around
- Assessment of any site, application or mobile app
- Complete findings report with recommendations
- Six-month follow-up scoring to measure progress



## 1.14: CX Services



### Customer Experience Strategy

**What is it?** Customer experience (CX) is defined by interactions between a customer and an organization throughout their business relationship. An interaction can include awareness, discovery, cultivation, advocacy, purchases and service. Customer experience is a primary driver behind overall customer management and the reason why it's important is because a customer who has a positive experience with a business is more likely to become a repeat and loyal customer. True customer experience leaders treat every customer interaction as a precious and finite resource. We help companies refine marketing, sales, channel management and service approaches to better serve targeted customer segments, maximize sales, improve loyalty and minimize costs

### Customer Experience Analysis

**What is it?** Customer experience analysis is the work on understanding the current customer experience in detail. Although this work will include journey mapping, it is much more than journey mapping. Customer and staff interviews along with ethnographic observations are important to fully document the customer experience. Experiences are not only rational steps in a process, but the experience is also defined by the customer's emotions, goals, objectives and pain points. The analysis decomposes the customer experience into the various individual interactions that make up the entirety of the experience. This is accomplished so the organization can focus on the interactions that need the most attention and re-imagining

### Customer Experience Research

**What is it?** Customers are not only influenced by experiences that your competitors provide but also by experiences that may have nothing to do with the specific industry you are in. Economic, competitive and regulatory trends all may affect what customers expect for their experience with an organization. This service area does primary and secondary research to uncover influences that should be taken into consideration when developing the future state customer experience.

## Customer Experience Innovation

**What is it?** Intentional customer experience innovation is one of the keys to successfully creating differentiation in the market place through customer experience. However, innovation is harder to do than most people think. Avtex provides a framework and tools set to help our customers apply the best thinking and concepts to defining and creating new experiences that can differentiate themselves in the market. Using tools from Design Thinking methods to unique ideation techniques we can help our clients lead the way with customer experiences that are truly delightful to the customer.

## Customer Experience Design

**What is it?** Once an organization understands the kind of experiences their customers are seeking it is important to design the experiences into the various touch points and interactions. This design work includes the creation of the future state journey map as well as making organizational design decisions to support the ongoing execution of the new experiences. The design work begins to pivot towards an internal perspective and may include typical process mapping to imbed the experiences into the organizations current processes. If the experience includes a digital experience then user experience, (UX) and digital design are often needed.

## Customer Experience Improvement

**What is it?** Too many times organizations fail to prioritize and implement the capabilities to support the new customer experience journey map. Lack of fundamental program and project management competencies, competing priorities and the void of a project plan all contribute to the gap between design and execution. Avtex comes along side our client to make sure that the appropriate level of planning is done to realize the improvements in the customer experience.

If you are interested in a CX Consulting engagement, please contact your CAM

## 1.15: Business Intelligence

The Avtex BI Team handles almost anything as it relates to turning data into information. The BI Team handles;

- Data Migration/Integration between applications, servers and other solutions
- Designs and Develops Data Warehouses built on Microsoft technologies
- Leverages Power BI and SQL Reporting Services to create rich, interactive dashboards and content
- Develop rich machine learning models to help drive predictive analytics
- Offers strategic consulting around BI to help clients create an analytics roadmap



# PureConnect Cloud Solutions

## 2.1: Services Provided with a Warranty or Support Agreement

Features	Description
Access to Avtex Technical Service	24x7
Response Time for Critical Issues	Business Hours: Live Call Non-Business Hours: 30 minutes via Answering Service
Response Time for Non-critical issues submitted by phone, email or OnPoint Portal	Included (Acknowledgement by 10:00 AM Central next business day)
Access to Avtex OnPoint Portal	Included
Avtex Labor to apply Genesys Base Software Releases and Patches	Coordinate installation, assist with troubleshooting and facilitate issue resolution
Labor to design and implement new features and or functionality	Contact Client Account Manager for quote
User Experience (UX) Consulting	Two Assessments including Score Card, Reporting, 6-month follow-up
Customer Experience (CX) Consulting	Building the Foundation for Exceptional CX Virtual Workshop
Avtex VRA (Voice Readiness Assessment)	10% Discount off List Rates
Avtex AVPRO Proactive Voice Network Monitoring Alerts to Avtex Support	\$350/site/month
Discounted PSO Rates	10% Discount off List Rate
Solution Optimization Consulting	50% Discount off List Rates
Development support for Avtex applications	Required and Included
Remote training 8 hours per year	Contact Client Account Manager for quote
Remote Move, Add, Change, Delete (MACD)	Included - 2 hours per month (Business hours only)
Labor Rate Notes	7:00 AM – 7:00 PM Central - Standard Rate Non-Business hours 30-minute Minimum
Travel Expenses	Not included

**The following services are NOT included in an Avtex Warranty or CSA:**

- Labor or material required to restore the system due to an act or event occurring external to the equipment which causes, either directly or indirectly, a failure or malfunction in the equipment. This includes without limitation: failures or malfunctions of Telco circuits, cable, or other equipment connecting the equipment to the telecommunications system; or abnormal power fluctuations which adversely affect the equipment.
- Administration services over and above the 2 hours per month included in the CSA
- Additions too, changes or relocation or system hardware.
- Neglect, misuse, tampering, accident or abuse, including use of the system for purposes other than which designed.
- Wiring, repair, alteration, modifications or improper installation by anyone other than Avtex, its subcontractors or affiliates without Avtex prior written consent.
- Accidents, disaster including water, wind, fire, lightning and earthquake unusual electrical shock; transportation; acts of God or public enemy.
- Vandalism; burglary; theft; lost or stolen parts; and or equipment other than equipment under warranty of Support Agreement from Avtex, including damages caused by equipment or lines of the host telephone system, host computer or LAN.
- Opening service tickets or maintaining ownership of service request with third party vendors.
- Replacing or troubleshooting network components.
- Forwarding or un-forwarding of telephone lines.
- Troubleshooting individual PC workstations.
- Running or moving new/existing cable.
- Applications created by parties other than Avtex. Time and materials, best effort basis.

## 2.2: Managed Services Offerings

### Move, Add, Change, Delete (MACD)

*NOTE: For services included in your selected support plan, please refer to the table in [Section 2.1: Services Provided with a Warranty or Support Agreement](#).*

Moves, Additions, Changes or Deletes (MACD's) are classified as administrative moves, additions or changes. MACD's are billed at the Avtex current or client contracted labor rate.

Avtex will make administrative MACD's as follows:

Changes will be scheduled during Avtex posted business hours and will be completed within 2 business days after receipt of the request, provided client cooperation with Avtex as reasonably required to meet the response time. All MACD requests should be made by calling into support at 800-323-3639 or via <https://onpoint.avtex.com/default.aspx>

MACD's are classified as small administrative Moves, Adds, Changes and Deletes from the PureConnect / Genesys solution, including but not limited to:

- Users
- Stations / Managed Phones
- Client Templates
- Workgroups
- Roles
- Status Messages
- Dial Plan
- Phone Numbers (DID Table)
- Password Policies
- Schedules
- Reports
- Wrap-up codes
- ACD Skills
- Interaction Recorder - Categories, rules, policies
- Interaction Dialer - Call lists, campaign creation
- Interaction Optimizer

Client requested changes beyond the scope of MACD requests above will require scoping by Avtex. These requests will be treated as small projects, requiring either a change order or a scope of work, and will be invoiced at the Avtex current or client contracted labor rates.

## Tier One Troubleshooting

This option provides relief for the client's PureConnect staff. ABC Company's end users continue to process requests and or issues through client's internal processes. When the need arises to contact Avtex support for assistance, the client's designated contact(s) will open a CTN with Avtex. From this point forward Avtex will work directly with the end user(s) to resolve the issue.

The Tier I specialist will gather the client's information and determine the client's issue(s) by analyzing the symptoms and figuring out the underlying problem. This includes troubleshooting methods such as:

- Verifying physical layer issues
- Resolving username and password problems
- Uninstalling/reinstalling basic software applications
- Verification of proper hardware, software and applications set up
- Assistance with navigating around application menus

Personnel at this level have a basic to general understanding of all Avtex supported hardware and applications.

## Support Database Integration

- Email or API
- Benefits
  - Each organization working in known environment
  - Reporting & Statistics
- Synchronization
  - Create, Update and Resolution
  - Status changes
  - Priority
  - Owner(s)

Please contact your Client Account Manager (CAM) to schedule a discussion

## Proactive Monitoring and Alerting

- Performed and provided by Genesys as part of the PureConnect Cloud

## Microsoft OS Patching

- Performed and provided by Genesys as part of the PureConnect Cloud

## Staffing options

This option provides relief for the client's PureConnect staff. Avtex has solutions to provide

- Dedicated on-site
- Dedicated Remote
- Pooled Remote
- The Avtex support organization is staffed to assist with your needs - (All times are Central)
  - 7:00 AM – 7:00 PM Monday thru Friday – Full Support, Maintenance & Managed Services
  - 7:00 PM – 12:00 AM Monday thru Friday – Emergency Support & Scheduled Events
  - 12:00 AM – 7:00 AM – Emergency Support

## Avtex Voice Performance Readiness & Optimization (AVPRO)

With proactive monitoring from AVPRO, issues impeding network performance are identified quickly to ensure troubleshooting efforts are focused on the right area. Key metrics associated to critical VoIP performance and network health are closely monitored and alerted on when pre-determined thresholds are reached.

### Monitoring Overview

The Avtex AVPRO solution will give the organization the following:

- Customized network health reports will be automatically emailed on a weekly basis that outline status and potential issues
- Quarterly report including observations and recommendations to remediate.
- Continuous unidirectional monitoring across entire network infrastructure; triggering alerts when predefined metric thresholds are reached
  - Bidirectional monitoring requires an appliance at the remote site(s).
  - A maximum of 15 Paths may be monitored with one appliance. Additional Paths will require a second appliance.

### Monthly RTP voice assessments

- Voice assessments are performed, simulating up to 99 concurrent unidirectional calls, leveraging synthetic RTP traffic, over each remote path
  - Bidirectional voice tests can be performed, simulating up to 100 concurrent calls, leveraging real RTP traffic, to remote locations with that have an onsite appliance

### End-to-end QoS safety checks

- Validate proper traffic is marked at layer 3 (DSCP)
- Ensure marked traffic is honored across entire path

### Traffic Analysis

- Application aware network analyzer
- View top-talkers for specific data and voice categories

- Network performance auditing
- Identify bandwidth hogs prioritized; dropping any fair-queue data

### Circuit/path monitoring:

With the appliance installed, Avtex will be able to create unidirectional paths, which traverse local or WAN links. This will help determine where congestion is occurring. Data is gathered to determine the following metrics:

- Total and utilized capacity
- Data loss
- Voice loss
- Latency
- Data Jitter
- Voice Jitter
- ICMP response time
- MOS

Continuous monitoring is performed for each path that is created using ICMP and UDP packets which can simulate different types of traffic. If a threshold is reached for any of the metrics measured, diagnostics are automatically run on the path to determine where the issue may be occurring.

Client will also be able to monitor the type of traffic traversing WAN circuits. With a port mirror configured and connected to the appliance, Avtex will be able to break down traffic on your network. The function works similar to NetFlow, which can identify traffic at the application level. This data can be categorized into different groups (i.e. "streaming media", or "social networking"). The information is then graphed, which will help identify and visualize the amount of bandwidth that each class is using.

### Deliverables

Avtex will supply ABC Company with reports and alerts pertaining to circuit utilization, service quality, data performance, voice performance, and voice testing results. Reports can be provided hourly, daily, weekly and monthly. Additionally, 4-6 hours per quarter will be devoted to reviewing diagnostics reports, voice assessments, and network concerns, with an Avtex Network Engineer.

### Appliances

After completion of the 12-month term, if the client has not renewed AVPRO service for an additional 12-month term, the client will be required to return all Avtex provided hardware within 10 business days. If an extension is needed, Avtex approval will be required. Violation of this agreement will result in a charge of \$600/month per appliance with no included services.

### Out of Scope Items

- Redesign of the network - this can be provided under a separate agreement.
- Response to alerts generated by AVPRO
- Troubleshoot network related issues - this can be provided under a separate agreement
- Network device configuration - this can be provided under a separate agreement
- Network equipment, software, cabling, or services to upgrade the network



## Client Device Installation and Configuration Requirements

- Provide a resource that has appropriate access to the network equipment for review and documentation. Outbound access on TCP 25, 443, 5721 and 80 are required. Please advise if a web proxy is used and if static IP addresses need to be assigned to the appliances.
- Ensure the following ports and protocols are allowed along the entire network path which is to be monitored:
  - ICMP echo
  - ICMP echo reply
  - ICMP TTL expired
  - ICMP destination unreachable - port unreachable
  - ICMP destination unreachable - fragmentation needed and DF set
  - UDP ports 45056 through 49151 - default port range used by UDP traceroute and AppView Voice Tests
  - UDP port 3239 - default port opened at the target appliance for testing on dual-ended paths
- Identify switch port to be used for AVPRO appliance management interface
- Identify switch port to be used for FlowView (if requested)
  - Configure SPAN port for monitor interface
- Install AppNeta M35 at client location. Connect management and monitor port to interfaces previously identified
- Configure devices to be monitored in AVPRO
- Clear counters on all interfaces that are to be monitored

## Avtex Quick Voice Assessment (QVA)

The purpose of the QVA is a light weight/quick evaluation to attempt to identify network issues that impede voice performance and validate if issues are network related. The methodical process we follow ensures valuable time and resources are not spent troubleshooting areas where problems do not exist, allowing us to focus effort on the right area or technology. During the assessment, key metrics associated to critical VoIP performance and network health are evaluated.

The Avtex Voice Health process is as follows:

- **Quick Voice Assessment (QVA) - Optional** – This solution is used to isolate where VoIP quality issue exist in the network, or other parts of the infrastructure. This rapid assessment can be used to determine if a full VRA is needed or if resources should be focused on other areas.
- **Voice Readiness Assessment (VRA)** – A methodical in-depth evaluation to determine the true root cause of voice quality issues. This can be done with or without the QVA prior. The output of the VRA is a detailed report that provides recommendations and remediation steps, including a quote from Avtex to assist or perform the work. Avtex VRA can also be used to validate network performance and capabilities prior to VoIP systems being placed into production. Any fees charged for the QVA will be credited towards the VRA.
- **Remediation Services** – Avtex can provide a full range of remediation services, from basic assistance for your networking team to a complete remediation solution of all issues identified in the VRA
- **Avtex Voice Performance Readiness & Optimization (AVPRO)** – An Avtex solution that provides you access to the tools used in a VRA, along with Avtex Sr. Network resources, to be proactive in monitoring

your company's VoIP networks. AVPRO helps pinpoint where network performance issues are occurring, saving you countless hours of wasted time.

### Monitoring overview

The Avtex QVA solution will give the organization the following:

#### RTP voice tests

- Voice tests are performed, simulating up to 100 concurrent bi-directional calls, leveraging real RTP traffic
- Ability to load up WAN circuit with benign TCP/UDP traffic during tests to validate proper traffic is prioritized; dropping any fair-queue data
- Analytics performed against completed voice tests

#### Circuit/path monitoring

With the appliance installed, Avtex will be able to create paths, which traverse local or WAN links. This will help us determine where congestion is occurring, down to the device and interface. Data is gathered to determine the following metrics:

- Total and utilized capacity
- Data loss
- Voice loss
- Latency
- Data Jitter
- Voice Jitter
- ICMP response time
- MOS

### Avtex Professional Services

#### Senior Network Engineer

- Remote kick-off meeting:
  - Discuss the required steps to deploy appliance used in the QVA
- General network review using the client provided diagrams
  - Determine expected voice paths and the devices that will be involved in monitoring and testing.
  - Review potential traffic congestion points
- WAN utilization review
- Voice LAN and WAN Path Validation
- Examine the path of VoIP traffic from end to end. The statistics are produced for Mean Opinion Score, Jitter, Latency, and packet loss
- Confirm QoS markings are honored end to end and all ports are set to full duplex
- Review current and expected traffic patterns and the estimated load it will place on the network

#### Deliverables

At the end of the one-week engagement, Avtex will supply the client with basic reports pertaining to circuit utilization, service quality, data performance, voice performance, and voice testing results and

recommendations on next steps. No troubleshooting or in-depth analysis is provided as a part of this engagement.

### Out of Scope Items

- Troubleshooting or remediation of any network related issues - this can be provided under a separate agreement
- Redesign of the network. This can be provided under a separate agreement.
- Network device configuration - this can be provided under a separate agreement
- Network equipment, software, cabling, or services to upgrade the network

### Client Device Installation and Configuration Requirements

- Provide a resource that has appropriate access to the network equipment for review and documentation. Outbound access on TCP 25, 443, 5721 and 80 are required. Please advise if a web proxy is used and if static IP addresses need to be assigned to the appliances.
- Ensure the following ports and protocols are allowed along the entire network path which is to be monitored:
  - ICMP echo
  - ICMP echo reply
  - ICMP TTL expired
  - ICMP destination unreachable - port unreachable
  - ICMP destination unreachable - fragmentation needed and DF set
  - UDP ports 45056 through 49151 - default port range used by UDP traceroute and AppView Voice Tests
  - UDP port 3239 - default port opened at the target appliance for testing on dual-ended paths
- Provide SNMP community string from client for all devices to be monitored
- Identify switch port to be used for QVA appliance management interface
- Install AppNeta M30 at client location. Connect management and monitor port to interfaces previously identified
- Install and configure single QVA appliance
- Clear counters on all interfaces that are to be monitored

### Voice Readiness Assessment (VRA)

Avtex will perform a remote Voice Readiness Assessment focusing on contact center readiness. The purpose of the assessment is to document the network and to determine if it is performing as required to support the needs of VoIP technologies. A successful VRA will provide confidence that the voice network will support the expected call volumes with high voice quality. This assessment is required for any part of ABC Company network for which voice traffic (SIP/RTP) will flow over.

#### Assessment Process

Avtex will deploy 3rd party network monitoring appliances that will reside at the client's location. The testing of the network will be performed during peak and non-peak times between various VoIP end-points. The ABC Company network team is responsible for ensuring the network is prepared for the assessment prior to the start of the Voice Readiness Assessment.

The voice assessments will determine if specific network paths will be able to handle a predetermined amount of VOIP traffic. Voice loss, MOS, latency, voice jitter, RTT and QoS markings will be measured at every hop across the path. Up to 100 concurrent calls can be generated for the assessment, which will then give a readiness score. Along with the call generator, Avtex will also be able to generate standard data traffic on the path to verify which traffic is being preferred and if QoS is being utilized. This will also help with tuning any QoS policies.

**The Voice Readiness Assessment will also validate that:**

- Full Duplex is enabled on all voice network devices
- Latency in one direction is less than 150ms (for both SIP & RTP)
- Jitter is less than 30 milliseconds
- Mean Opinion Score (MOS value) for the G.711 audio codec is 4.1 or greater and for the G.729 audio codec is 3.9 or greater
- RTP packets include the proper markings for service priority queuing following the DSCP model
- Network segments do not exceed a packet loss rate of one per cent (1%)
- Network bandwidth is sufficient to allow for approximately 84kb/s per call using the G.711 audio codec and 21kb/s per call using the G.729 audio codec
- VLAN settings are set in accordance with the QoS for the PureConnect Platform and Microsoft whitepapers

### Monitoring overview

#### Circuit/path monitoring:

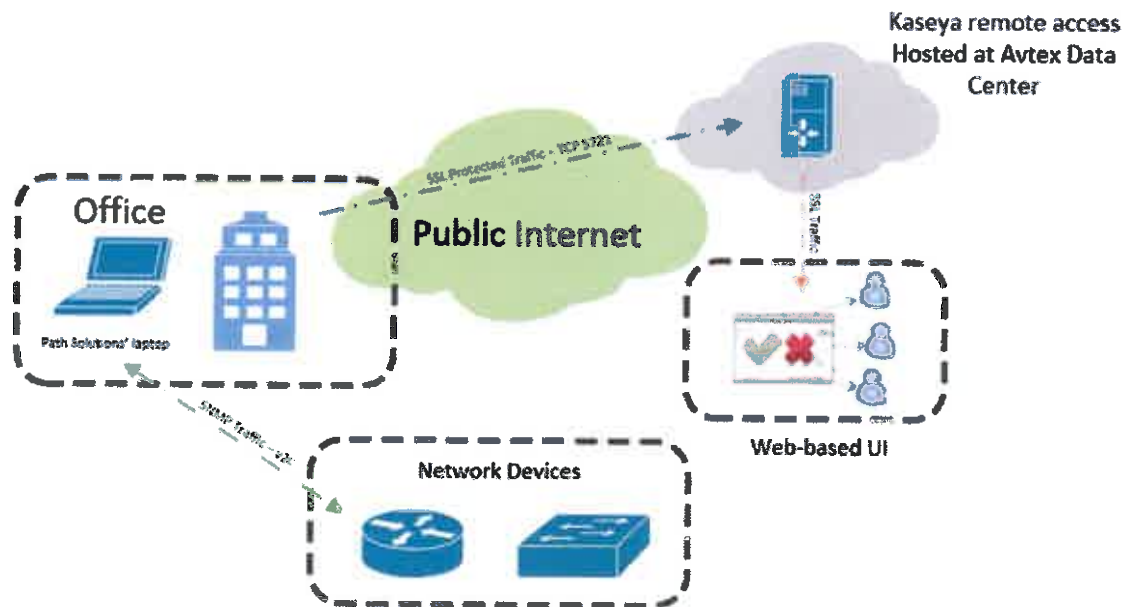
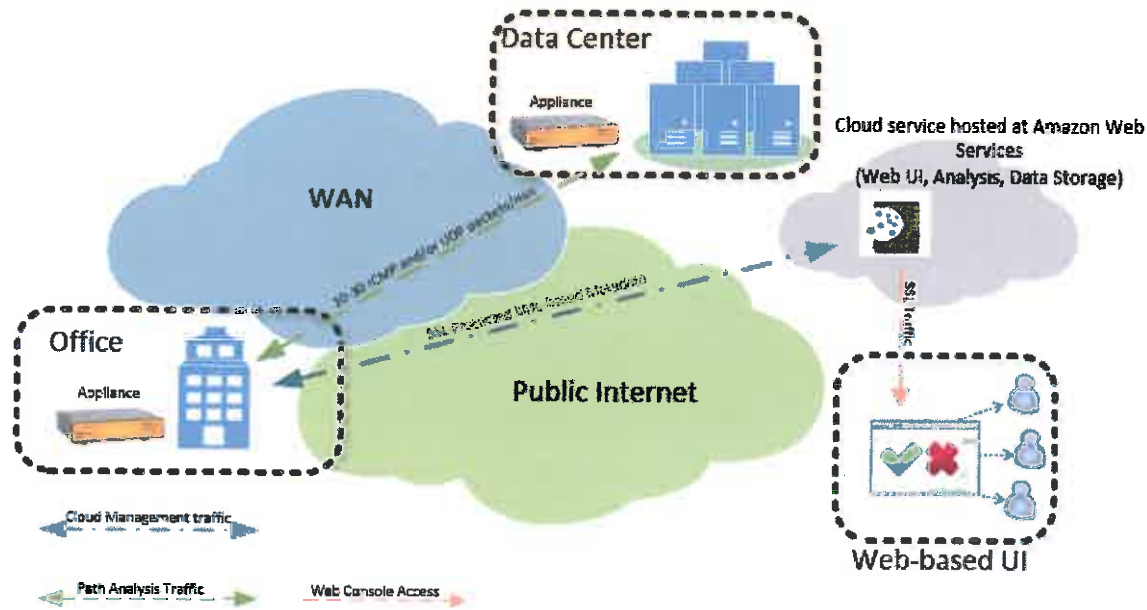
With the appliance installed, Avtex will be able to create paths, which traverse local or WAN links. This will help us determine where congestion is occurring, down to the device and interface. Data is gathered to determine the following metrics:

- Total and utilized capacity
- Data loss
- Voice loss
- Latency
- Data Jitter
- Voice Jitter
- ICMP response time
- MOS

Continuous monitoring is performed for each path that is created using ICMP and UDP packets which can simulate different types of traffic. If a threshold is reached for any of the metrics measured, diagnostics are automatically run on the path to determine where the issue may be occurring.

If necessary, Avtex may monitor the type of traffic traversing WAN circuits. With a port mirror configured and connected to the appliance, Avtex will be able to break down traffic on your network. The function works similar to NetFlow, which can identify data down to which protocol is used. This data can be categorized into different groups (i.e. "streaming media", or "social networking"). The information is then graphed, which will help identify and visualize the amount of bandwidth that each class is using.

## Appliance and Laptop Communication:



## Avtex Professional Services

### Senior Network Engineer

- Remote assessment kick-off meeting:
  - Discuss the required steps of the assessment
  - Discuss ABC Company requirements for the assessment
  - Discuss ABC Company concerns regarding the network in detail
- Review the current network design
- General network review using ABC Company provided diagrams
  - Determine expected voice paths and the devices that will be involved in the assessment



- Review potential traffic congestion points
- QoS Configuration Deployment Review
- Configure paths in AppNeta
- Configure Voice Assessment in AppNeta
- Configure FlowView in AppNeta
- Configure devices to be monitored in PathSolutionsWAN utilization review
- Voice Device Inventory Discovery: This test will identify all devices on the network that are suitable for voice testing.
- Voice LAN and WAN Path Validation
- Examine the path of VoIP traffic from end to end. The statistics are produced for Mean Opinion Score, Jitter, Latency, and packet loss
- Confirm QoS markings are honored end to end and all ports are set to full duplex
- Review current and expected traffic patterns and the estimated load it will place on the network

#### Project Manager

- Schedule and host Internal kickoff call
- Schedule and host External kickoff call
- Provide documentation on VoIP network requirements and assessment pre-requisites
- Schedule and host ongoing status meetings (minimum weekly is typical)
- Track project status and loop in current SMEs as appropriate
- Orchestrate shipping logistics of network devices
- Create and work off project plan
- Manage change, risks, hours, communications, and budget
- Drive and track any project escalations to resolution

#### Deliverables

Avtex will supply ABC Company with reports pertaining to circuit utilization, service quality, data performance, voice performance, and voice testing results. Reports can be provided hourly, daily, weekly and monthly.

#### Appliances

This assessment includes a maximum time of two weeks per-site to perform from the date the appliances are received by the client. After completion of the VRA, the client will be required to return all Avtex provided hardware within 10 business days. If an extension is needed, Avtex approval will be required. Violation of this agreement will result in a charge of \$600/month per device with no included services.

#### Out of Scope Items

- Redesign of the network - this can be provided under a separate agreement
- Troubleshoot network related issues - this can be provided under a separate agreement
- Network device configuration - this can be provided under a separate agreement
- Network equipment, software, cabling, or services to upgrade the network



## Client Device Installation and Configuration Requirements

- Provide a resource that has appropriate access to the network equipment for the purpose of review and documentation. Outbound access on TCP 443, 5721 and 80 are required. Please advise if a web proxy is used.
- Ensure the following ports and protocols are allowed along the entire network path which is to be monitored:
  - ICMP echo
  - ICMP echo reply
  - ICMP TTL expired
  - ICMP destination unreachable - port unreachable
  - ICMP destination unreachable - fragmentation needed and DF set
  - UDP ports 45056 through 49151 - default port range used by UDP traceroute and AppView Voice Tests
  - UDP port 3239 - default port opened at the target appliance for testing on dual-ended paths
- Provide SNMP community string from client for all devices to be monitored
- Identify switch port to be used for AppNeta and PathSolutions management interface
- Identify switch port to be used for FlowView (if requested)
  - Configure SPAN port for monitor interface
  - Alternatively, the AppNeta device can sit in-line
- Install AppNeta M30 at client location. Connect management and monitor port to interfaces previously identified
  - If static IP addresses are required, the client will need to provide the IP address, subnet mask, gateway, DNS servers, NTP server, and web proxy.
- Install PathSolutions laptop at client location. Connect management port to interface previously identified
  - Optional: Client may provide a VM with Kaseya agent for Avtex to access and install/run polling tools instead of using a laptop.
  - Minimum Requirements for VM are:
    - For networks with less than 5,000 total interfaces:
    - Pentium 800Mhz Processor or faster (Virtual server is fine)
    - 1 GB of free disk space
    - 1 GB of RAM for the service (2 GB RAM for the server)
    - 100 MBPS Network Interface Card
    - Windows 2008, Windows 2012 (32bit or 64bit)
- Clear counters on all interfaces that are to be monitored

## Network Consulting Services

Assist with both client projects and remediation work

- Data Center re-locations
- Core network design and replacement

- WAN migration planning
- Data and voice traffic engineering
- QoS policy design and implementation
- Network problem? We can help!

Please contact your Client Account Manager (CAM) to schedule a discussion

### Disaster Recovery as a Service (DRaaS)

- Assessment
- Migration
- Constant Health monitoring and Frequent Failover testing
- Low Cost / High Value Solution with MRR

Please contact your Client Account Manager (CAM) to schedule a discussion

## 2.3: Enhancement Requests

An Enhancement Request is defined as any **NEW** feature or functionality of the Genesys Product that is not:

1. included in the product as standard functionality.
2. Functionality or features which cannot be added via Avtex customization.
3. Functionality or a feature not available.

The Genesys products are very feature-rich products that offer many options and customization choices. Occasionally, there may be features and functions that you may desire to meet your environment or needs. Genesys encourages and offers the opportunity for clients and partners to submit Enhancement Requests for such desired features and/or functions. Enhancement Requests bring user feedback and suggestions directly to the manufacturer, which in turn result in better products presented to the industry.

The typical Enhancement Request procedure works as follows:

1. A client defines the request they want to present and communicates the need to their Avtex CAM.
2. The request is forwarded internally at Avtex to a Project Engineer for evaluation.
3. The Avtex Project Engineer determines if the request can be fulfilled by either a standard function in the system, customization by an Avtex Developer or in a hotfix or Service Update (SU).
4. If it is determined that none of the above are possible, the Project Engineer returns the request to the CAM.
5. The CAM will email the Enhancement Request to Genesys' Enhancement Request team.
6. The CAM will receive an email confirmation that the Enhancement Request was received.
7. The Genesys Product Marketing and Development teams will review the request and keep your CAM informed with respect to its disposition.
8. Once Genesys' review has been completed, a status will be assigned to the Enhancement Request. The statuses are as follows:
  - o Declined
  - o Proposed
  - o Approved

Your Avtex CAM will relay to you (the requesting client) the information decided upon. If the Enhancement Request has been approved, an anticipated timeframe will be provided as soon as it is known.

## 2.4: Security

Security should be the priority on any system within your organization. It is your responsibility to implement and enforce your corporate security policy, which in turn will help ensure and protect your system and investment. The following are some guidelines we recommend:

### User Passcode Security

The default passcode should be “secure” meaning it should not have sequential or repetitive digits. This is the passcode used to access mailboxes for the first time.

- Require all users to change security upon first time access.
- Implement options for passcode aging and complexity.

### Setting Default Passcode Policy

(Your screens may look different depending on product and or version)

#### Manage Organization

The screenshot shows the 'Password Requirements' settings page. It features a navigation bar with 'Organization Details', 'Settings', and 'Password Requirements'. The main content area lists several password requirements, each with a dropdown menu and a 'Reset' icon:

Requirement	Value	Action
Minimum Length	8	Reset
Minimum Letters	0	Reset
Minimum Lower Case Letters	1	Reset
Minimum Upper Case Letters	1	Reset
Minimum Numerals	1	Reset
Minimum Special Characters	1	Reset
Password Expiration	<input type="checkbox"/>	Reset
Minimum Age	<input type="checkbox"/>	Reset

### Other Security Recommendations

- User accounts that are no longer in use should be removed immediately
- Perform audits of user accounts to verify that only active users remain in the system
- Restrict dialing privileges to only those that are necessary

## 2.5: Repair Process for Avtex Provided Telephones and Headsets

All device repair and or replacement will be referred to the manufacture of purchase

If Avtex assistance is requested all time will be invoiced at the current T&M labor rate.

# Conclusion

You have made a significant investment in your communication system and all of us at Avtex are committed to its success. Throughout the solution implementation, and through our ongoing support of your environment, we take great pride in the work that we do. As with any partnership, we welcome your ideas and suggestions on ways that we can continue to improve our service offerings.

Thank you for your business and your partnership with Avtex!

## **Attachment 4.2.1.1.1.4 - Presidio Service Transition Management v2**

Please find the attachment beginning on the following page.



## Presidio Service Transition Management

Service Transition Management is a phased process in which Presidio implements Managed Services. It includes uploading information into the Monitoring Framework, including the Service Management System and configuration of the DCA. This consists of all steps required to activate and onboard Managed Services.

### Kickoff Meeting

Presidio assigns a Project Manager (PM) to act as a single point-of-contact during the Service Transition Management phase. The external Kickoff Meeting indicates the initiation of the kickoff phase and is typically conducted via web or voice conferencing. The Kickoff Phase, as well as all remaining phases within Service Transition Management, is typically facilitated by the PM in collaboration with a Presidio Engineer.

This Service Transition Management phase includes the following activities:

- Coordinating, scheduling, and executing the Kickoff Meeting.
- Reviewing deliverables included in this Managed Service Contract.
- Reviewing services purchased, as indicated on the Client Purchase Order (PO).
- Aligning Presidio and Client on all major activities, risks, and milestones during Service Transition Management phase.
- Reviewing and scheduling a timeline for completing the Runbook and covered equipment list (CEL).

### Runbook

Reviewing the Runbook components and key information is critical to success for Service Transition Management. Contained in the Runbook is the CEL, which identifies Managed and Monitored CIs. The PM develops a Project Plan for subsequent steps with distribution to project contacts. The required information must be uploaded into the Monitoring Framework. The Client is responsible for providing the information included in the Runbook, which is provided as part of Service Transition process.

### Presidio Monitoring Framework

The DCA is configured to monitor Managed CIs per the CEL included in the contract. During the network discovery process, the PM communicates any discrepancies between identified CIs and requested Managed CIs in the CEL. Additional documentation specifying addressing, ports, and protocols is provided and reviewed with Client during kickoff.

Requested additions beyond the Managed CIs defined in the PO are subject to incremental service fees and additional Service Transition Management intervals. The PM communicates with sales personnel to add any additional items via an Addendum.

Implementing the Monitoring Framework includes the following:

- Preparing, configuring, and testing DCA.
- Shipping DCA to the designated Client premise.
- Remotely assisting Client with DCA installation; on-site installation support is available at client request.

- Establishing SSL over HTTP connectivity between Presidio and the Client premises.
- Configuring Presidio internal systems in preparation for service delivery.

Presidio inputs managed and monitored-only CI information into Monitoring Framework and the Service Management system. Service, support and escalation processes are also configured in the Service Management system during the Transition phase with input and agreement from the Client. This completes the implementation of the Monitoring Framework.

### **Managed Device Preparation**

The Monitoring Service element is dependent upon:

1. Network connectivity to Managed CIs.
2. Configuration of SNMP.
3. Trap Receiver destination IP address.
4. Provision of login and enable passwords.

A required device-specific configuration is supplied to Client, including community strings and host destination addresses.

### **Setup and Modeling of the Application**

Setup and modeling of the application is 100% Presidio's responsibility and includes the installation software components of the Monitoring Framework. Managed device information from the collection stage is loaded, and each individual device is configured for required monitoring statistics/reporting. Presidio and the Client resolve any network connectivity, firewall, or routing issues between CIs and DCA.

### **Remote Training Session**

The PM will schedule remote training sessions as necessary. These sessions are conducted via WebEx provided by Presidio.

The objectives of the training session are reviews of:

- Services to be delivered.
- Service documentation.
- Presidio and Client responsibilities during the service delivery process.
- Processes for obtaining service.
- Service escalation process.
- Client Portal overview.

### **Start of Service (SOS)**

The SOS milestone begins the Service Term, and is contingent on the timely completion of all activities as identified in the Runbook project schedule. Presidio works with the Client to meet the Start Date milestone and validate that the Service Transition Management phase is complete before Managed Services commences. Notification/Escalation and Event Management does not occur until a detailed operations handover has been performed, all required documentation and procedures are put in place. At the agreed-upon start date, the PM and the Client execute a Certificate of Acceptance, concluding the Service Transition Management phase, and the Service Delivery phase commences.

## CLIENT RESPONSIBILITIES

### Install Monitoring Framework

Client shall provide the following with respect to the installation of the DCA:

- Provide appropriate secure rack-mount location for the DCA with suitable environmental conditions.
- Install the DCA and network connectivity per Presidio-supplied guidelines or allow Presidio to access appropriate location to deploy the DCA.
- Provide communications facilities and services including internet and network configuration. Communication facilities and services must be maintained for the duration of the service term.
- Provide a resource to support the installation of the DCA. These activities include:
  - Installing the DCA in a suitable equipment rack and connecting to network.
  - Power connection to Uninterruptible Power System (UPS) or other facility with continuous uninterrupted power.
  - Power-up.
  - Notification to Presidio that installation is complete.
  - Provide suitable commercial power, and recommends UPS or other acceptable power back-up facilities providing a minimum of 1kVA dedicated to each appliance.

### Training

The Client shall provide training coordination support, including identifying trainees and trainee contact information.

### Transition Management

To ensure Presidio's ability to provide services for Managed CIs, Presidio requires the Client to:

- Assign a Project Manager or equivalent to represent the Client during the Service Transition Management phase.
- Assign a Technical Lead or equivalent to assist Presidio with establishing the network access required for Managed Services.
- The Client Project Manager and Technical Lead must attend the Project Kickoff Meeting and training sessions.

### Runbook

Utilizing the required information provided by the client, Presidio will complete the Runbook, which provides the key information critical to success for the Service Transition Management phase. The Runbook provides information, such as:

- Detailed CI inventory information.
- Definition of Client-specific support policies including:
  - Points of contact and profile data
  - Change management procedures

- Notification policy
- Escalation policy
- Manufacturer maintenance and support contract information and contract number (e.g., Cisco SMARTnet).
- Provide as-built documentation including detailed design, network implementation plan(s), site survey(s), and bill of materials (if available).

### **Service Connectivity and Network Access**

The Client is required to provide Read and Write management access to Managed CIs as defined by the Runbook. Access must be implemented in a timely manner in accordance to the Runbook. This includes SNMP, syslog, and other defined protocols as necessary to support services.

The Client will maintain manufacturer maintenance and support contracts covering hardware and/or software as may be applicable on all Managed CIs for the duration of the Managed Services contract. Client must provide support contract details, LOA and all other Client documentation and authorization required to facilitate incident resolution.

If the Client elects not to maintain such coverage, Presidio provides reasonable business effort only and may not have access to necessary manufacturer resources, such as support and software updates to facilitate repair.

In cases of special support arrangements; e.g., Client stocking their own spares (self-insuring), Client acquiring manufacturer support on a Time and Materials (T&M) basis, or instances of no manufacturer maintenance and support, the Client must provide a sparing strategy for replacement of devices, and the replacement and recovery of device functionality is the sole responsibility of the Client.

### **Communication and Change Management**

Presidio has a co-management approach to Managed Services, allowing the Client and other Client-approved vendors to retain access to Managed CIs. Because multiple parties can make changes to the environment, Presidio requires anyone with access to the Client's environment to follow a consistent and documented Change Management process. This process is reviewed and agreed-upon prior to completion of the Service Transition Management phase.

The Client will:

- Notify Presidio in advance if scheduled or unscheduled maintenance of Client's Managed and Monitored-Only CIs will impact the:
  - DCA monitoring of Managed CIs.
  - Proper operation or network connectivity of Managed CIs.
  - Maintain responsibility for informing Presidio of Client employee status changes.
  - Provide and maintain a list of Client employees authorized to request changes.
  - Provide and maintain an escalation path within the Client's employee base.

## **Attachment 4.2.2.1.1-1 - Avtex - SoWV - Base Configuration Premier CSA**

Please find the attachment beginning on the following page.

This Customer Support Agreement ("Agreement") is entered into as of January 1, 2018 ("Effective Date") between **Avtex Solutions, LLC** ("Avtex") a corporation organized under the laws of Minnesota, with principal offices located at **3500 American Blvd. West, Suite 300, Bloomington, Minnesota 55431** and **State of West Virginia** ("Customer") with principal offices located at **2019 Washington Street East #50130, Charleston, West Virginia 25305-0130**.

Avtex agrees to provide the services described in Section 2 of this Agreement, for the System that is incorporated herein by reference ("System") for the term of this Agreement.

**1. TERM AND AMOUNT:**

The term of the Agreement will be one year from the Effective Date commencing on the day of ordering software licenses. Term of Agreement will not commence until both parties have executed this Agreement and Customer will have paid Avtex the amount plus tax annually. Termination by Customer will immediately require payment of the balance for the remaining term. This Agreement will be renewed automatically for successive one-year term at the current Avtex rate unless either party gives the other party written notice of termination, which termination will be effective only on the expiration of the current Term. Annual adjustments for incremental purchases of product and services along with manufacturer price adjustments will apply. Payment for successive one-year terms will be annually in advance. The Customer may give Avtex written notice of termination of this Agreement sixty (60) days prior to the Effective Date of a renewal Term. Avtex will give the Customer at least sixty (60) days' notice if Avtex chooses not to offer a renewal Term.

- Annual Costs (reoccurring):
  - Base Configuration Statement of Work: \$ 748,024
    - Managed Services agreement uplifts to Tier 1 and MACD estimated 16 hours per month

**2. CUSTOMER SUPPORT SERVICES:**

a. **Software Maintenance.** This agreement entitles the Customer to all PureConnect patches for 4.0 and 201x when they become generally available by Genesys. Avtex will provide 24 x 7 maintenance on the base PureConnect System Software. Maintenance specifically refers to patches for 4.0 and 201x. Customer is responsible for performing configuration back-ups on the System. In the event that Avtex must restore the System and the backed-up configuration is not accurate, Customer agrees to pay all labor required at then current Avtex labor rates. Reference Exhibit A for software covered.

b. **Application Maintenance.** Avtex will provide support for applications installed as part of the original installation proposal or added through a request for application development and limited to applications developed by Avtex or its subcontractors. Reference Exhibit A for application maintenance.

c. **Software Upgrades.** This agreement entitles the Customer to all the base PureConnect software upgrades, referred to as "Release" or Rx, when they become generally available by Genesys. Labor for installation of Release i.e. R1, R2 software upgrade is included.

d. **Monitoring.** Avtex will provide proactive monitoring and alerting via Kaseya. Alerts will be sent to a customer designated e-mail address and Avtex Support for remediation.

e. **Moves, Adds, Change, Delete (MACD).** Avtex will provide two (2) hours per month (plus 16 Managed Services Agreement) remotely such services as are necessary and available with respect to the System to move, add, change, and delete the System during business hours, as defined in Section 4.d.

f. **Training.** Remote Avtex Training services of up to eight (8) hours per year are included.

**3. EXCLUDED/ADDITIONAL SERVICES:**

The following services are available at the Customer's request but are expressly excluded from this Agreement. The Customer agrees to pay additional charges for such services, along with services noted in Section 2 above, at then current Avtex rates. Additional equipment or features, ordered by the Customer, is subject to the prices prevailing at the time orders are placed.

a. **Repair of damage, replacement of parts or increase in service time caused by:**



- 1) Failure by the Customer to continually provide a suitable environment for the System(s), including but not limited to adequate space, electrical power, air conditioning, dust control, connectivity to telephone system, host computer system and LAN;
- 2) Failure by the Customer to follow the installation, operation and maintenance instructions provided by Avtex;
- 3) Neglect; misuse, tampering, accident or abuse, including use of the System for purposes other than which designed;
- 4) Wiring, repair, alteration, modifications or improper installation by anyone other than Avtex, its subcontractors or affiliates without Avtex prior written approval or supervision;
- 5) A corrosive atmosphere harmful to electronic circuits;
- 6) Damages caused by pests or domestic animals;
- 7) Accidents, disaster including water, wind, fire, lightning and earthquake; unusual electrical shock; transportation; acts of God or public enemy;
- 8) Vandalism, burglary; theft, lost or stolen parts; and/or
- 9) Equipment other than equipment under Warranty or Support Agreement from Avtex including damages caused by equipment or lines of the host telephone system, host computer or LAN.

b. **Hardware Maintenance.** On a billable basis, Avtex will provide such service and repairs as may be reasonably necessary to keep the System operating in good working order.

c. **Customer and/or Third-Party Software Application Maintenance.** Requests for support on applications developed and/or installed by the Customer or other 3<sup>rd</sup> party vendors is not included. Customer agrees to pay the labor required for such support, invoiced at then current Avtex labor rates.

d. Custom Software Application Upgrades created to meet the customer's specific needs, which exceed the publisher's usual and customary programming practices, may incur additional programming charges in the upgrade of the operating system software. Avtex will notify Customer of such Applications that may result in additional upgrade charges prior to their creation.

e. Any services required for reconfiguration of the PureConnect system as required to support the Customer's changing of their Central Office (CO). This includes, but not limited to, changes within the same CO, changing CO's and/or adding circuits.

f. **Phones.** For phones purchased through Avtex, Avtex recommends the Customer purchase spares, as Avtex does not provide break/fix support.

g. **Ancillary Servers & Non-Genesys Software.** Support for ancillary servers and software, excluding the main PureConnect server, are the responsibility of the Customer.

#### 4. SUPPORT COVERAGE:

a. **Response/Emergency.** During business hours, as defined in Section 4.d., Avtex provides priority routing to live assistance to respond to emergencies. During non-business hours, Avtex will respond to emergency calls (the inoperability of the System) within 30 minutes via Answering service after receiving notice thereof.

Inoperability is defined as:

- Unscheduled total system outage or failure to reboot
- Inability to access the system through 25% or more of all ports
- Loss of system integration
- Continual system restarts or failovers
- Loss of dial tone on more than 25% of system
- A custom software program developed by Avtex is not functioning.

b. **Response/ Non-Emergency.** Avtex will acknowledge non-critical issues by 10:00 a.m. Central the next business day after notice thereof.

c. **Availability.** Avtex will make service available to customer twenty-four (24) hours per day, seven (7) days per week, except holidays observed by either Avtex or Customer. Note: Non-emergency service requested during non-business hours will be invoiced at the non-business hour labor rate as defined in Section 5.

d. **Business Hours.** Support will be provided during business hours. Business hours will be understood to mean Monday through Friday, 7:00 a.m. to 7:00 p.m. Central, except any holidays observed by either Avtex or Customer.

e. **Non-Business Hours.** Non-business hour support will be provided for break-fix related issues. Non-break-fix issues will be addressed the following business day as outlined in Section 4.b., unless invoicing is approved by the customer.

f. **On-Site Support.** Any on-site coverage will be invoiced at then current Avtex rates.

#### 5. CURRENT BILLABLE SERVICE LABOR RATES:

Different types of services and their respective rates are available upon request. Support will be invoiced in 30-minute increments after exceeding the minimum.

Services provided during business hours, as defined in Section 4.d., will be billed at then current Avtex labor rates.

Services provided during non-business hours requires 30-min minimum billing at the non-business hour rate of \$185 per hour.

#### 6. OBLIGATIONS OF CUSTOMER

a. Customer will pay to Avtex, all charges, including applicable taxes set forth below:

- 1) For all services covered in Section 2, Customer will be obliged to pay the amount set forth in Section 1.
- 2) Charges for services provided as specified in Section 2.
- 3) The price for additional equipment and features ordered as specified in Section 3.

b. "Payment" - The amount set forth in Section 1 of this Agreement will be due and payable in advance of the commencement date. All other charges will be due and payable upon receipt of invoice.

c. To permit performance of services herein mentioned, Customer hereby grants Avtex access as necessary to the business premises of Customer.

d. Customer agrees to allow Avtex to use Customer's name for marketing purposes.

#### 7. DEFAULT:

a. If Customer is delinquent in payment of sums of money owing to Avtex, for equipment or services invoiced under the provision of this, or any other Agreement between Avtex and Customer. Avtex will have the right, after written notice, to cease performance of maintenance service hereunder until such time as such delinquencies are cured. Such suspension in service will not extend the term of this Agreement beyond the term herein provided.

b. In addition to all remedies available to Avtex at law or in equity, in the event of a default by Customer hereunder or under the terms of any other contract between Avtex and Customer. Avtex will be entitled to collect interest upon the sum then due and owing at the maximum rate of 18% per annum from the due date of the last payment until such default by Customer has been cured. It is expressly agreed and understood that in no event will the aggregate interest exceed the maximum rate of interest that can be charged under the applicable state law.

c. Should either party be obliged to institute legal action to enforce its rights hereunder, the prevailing party in such action will be entitled to recover reasonable attorneys' fees in the amount allowed by the court.

#### 8. ASSIGNMENT:

Avtex will have the right to assign the maintenance of the System to a vendor approved in writing by Customer; approval will not be unreasonably withheld.

#### 9. CUSTOMER TO PROVIDE:

Customer will, as specified by Avtex in writing, provide appropriate environmental conditions, necessary commercial power and facilities for the System, access to the premises, and if required by local law, conduit and or special fire-retardant cabling. Customer will pay all charges including, but not limited to charges for telephone trunk lines, PBX extensions and or PBX

equipment, host computer ports and data connection(s), Local Area Network (LAN) connection(s) required for the maintenance of the System.

**10. REPRESENTATION:**

Customer and Avtex each warrant and represent to the other that it has been duly authorized by all necessary corporate or other action to execute this Agreement and will not violate any provision of law or its Articles of Incorporation or Bylaws, or result in the breach of an Agreement to which it is a party.

**11. NOTICES:**

All notices required or permitted to be given under this Agreement may be given by either party to the other by depositing same in the United States Mail with first class postage prepaid or by facsimile. Until changed by written notice, such notices will be directed to Avtex at the address that appears at the beginning of the Agreement and to Customer at the Premises.

**12. LIMITATION OF LIABILITY:**

Notwithstanding same, should the System malfunction or cease to function for any reason, including telephone service interruption, defective parts or workmanship, negligence of Avtex, or any breach or alleged breach of this Agreement, Avtex's liability hereunder will be limited to general money damages in an amount not to exceed three (3) months maintenance service. Such limitation will be the full extent of Avtex's liability regardless of the form in which any legal or equitable action may be brought against Avtex, and the foregoing will constitute Customer's exclusive remedy.

UNDER NO CIRCUMSTANCES WILL AVTEX BE LIABLE FOR ANY LOST PROFITS OR FOR SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, OR COMMERCIAL LOSS, OR FOR INFRINGEMENT CLAIMS DUE TO USE OF SOFTWARE, EVEN IF AVTEX HAS BEEN ADVISED

Furthermore, no action, regardless of form, arising out of or under this Agreement may be brought by either party more than one (1) year after the first day that the cause of action has occurred, except for an action for nonpayment. Avtex hereby assigns to and passes through to Customer any Warranty provided to it by its equipment supplier(s), and Avtex will not be responsible for any defective parts or workmanship in new equipment provided hereunder. Rebuilt or reconditioned equipment may be provided upon notice to Customer, and Avtex will be responsible therefore to the extent of the terms of this Agreement, and same will not reduce to any extent the Warranty or the availability of maintenance provided hereunder.

**13. ENTIRE AGREEMENT:**

The provisions contained in the foregoing and attached System Itemization constitute the entire Agreement between Avtex and Customer and any alterations or modifications thereto must be in writing, reference this Agreement and be executed by both parties. If any provision(s) of this Agreement are held to be illegal, invalid or unenforceable, then such provision(s) will be deemed null and void, without invalidating the remaining provisions hereof.

**14. THIS AGREEMENT WILL NOT COVER:**

An act or event occurring external to the equipment, which causes, either directly or indirectly, a failure or malfunction in the equipment including without limitation, failures or malfunctions of the trunk or toll lines, cable or other equipment connecting the equipment to the telecommunications system, failure of the host telephone system or abnormal power fluctuations, which adversely affect the equipment.

**15. EMPLOYEES:**

Customer agrees not to hire directly or indirectly any employee(s) of Avtex from the date of this Agreement and for one (1) year thereafter without prior consent from the President of Avtex. Should Customer hire such an employee during this period, the Customer will pay, as liquidated damages and not as a penalty, the sum of Seventy-Five Thousand Dollars (\$75,000) for each employee hired.

IN WITNESS WHEREOF, Avtex and Client cause this Agreement to be executed by their duly authorized representatives on the dates specified below.

**Avtex Solutions, LLC ("Avtex")**

**State of West Virginia ("Customer")**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

**Exhibit A:**

**We based our pricing on the configuration provided to us below. Any additions or reductions to software, hardware and applications will affect the pricing, as well as, any manufacturer pricing adjustments.**

**Exhibit B: Premier Features**

- Includes Customer Journey Mapping and Innovation Workshop
- Includes Three User Experience Assessments Including Score Card, Reporting, and 6-month follow-up
- Includes installation, one (1) hour remote Avtex training and application support for one of the following Avtex products:
  - RoboReports – Scheduled report delivery
  - iSurvey – Post call survey
  - Avtex Clone – Server sync
- 10% Discount off List Rate for Avtex VRA (Voice Readiness Assessment)
- Special rate of \$421/site/month for Avtex AVPRO Proactive Voice Network Monitoring
- 10% Discount off List Rate for Disaster Recovery as a Service (DRaaS)
- 10% Discount off List Rate for Professional Services
- 50% Discount off List Rate for Solution Optimization Consulting

## **Attachment 4.2.2.1.1-2 Avtex - SoWV - Managed and Hosted Voice Services Agreement**

Please find the attachment beginning on the following page.





# Managed and Hosted Voice Services Agreement

**Prepared for:**

State of West Virginia

**Prepared by:**

**Matt Coy**

*Account Executive*

[mcoy@avtex.com](mailto:mcoy@avtex.com)

(847) 664-8887

**Mark Granquist**

*Solutions Consultant Team Lead*

November 9, 2018

**avtex**  the point of interaction

Avtex Solutions LLC  
3500 American Blvd West  
Suite 300  
Bloomington, MN

## Executive Summary

---

State of West Virginia recognizes the need for a PureConnect Cloud Contact Center solution by Genesys. To improve quality, reduce costs, strengthen controls, and remediate staffing issues, Avtex will provide the following support and services.

With the combination of your Premier Support Agreement and this Managed Services Agreement, Avtex will be delivering the following services:

- Moves, Add, Change, Delete (MACD)
- Tier One Troubleshooting
- Service Database Integration
- Mon- Fri; 7 AM - 7 PM Central, Full Support
- 24 x 7 Emergency Support
- Support for all customizations and integrations

Avtex is proposing remote pooled support staff focusing on the services defined above. In addition to the existing Premier support contract covering all levels of remote support, Avtex has a full team of individuals who can provide support on the PureConnect Cloud platform.

## Scope Overview

---

Avtex will provide support for State of West Virginia's PureConnect Cloud solution from Genesys, in accordance with Client's established policies and procedures, including:

### Support Services

Avtex will perform the following as part of Support Services:

- Follow Client standards and procedures for Security, Change Management, Stakeholder Communication, and System Availability Protection (maintenance windows)
- Determine the type of problem when assigned by the State of West Virginia Voice Services and own the ticket through resolution
- Perform any necessary troubleshooting or discovery work and engage the appropriate party to resolve the issue as needed
- Work directly with end users as required to resolve the issue
- Keep end users updated as needed
- Create Knowledgebase Documents ("KB's") for common, repeat issues reported by End Users and share with State of West Virginia Help Desk
- Manage to State of West Virginia Incident Management Service Levels
- Gather all necessary logs for investigation of issues
- Engage third party vendors including Genesys as needed for follow through to resolution
- Keep vendors and partners updated as needed
- Perform post installation verification

- Telco support
  - Troubleshooting and resolution of Tier One, End-user issues in coordination with client voice services and or telecom team
  - All changes will be reviewed and approved by State of West Virginia

## Reports/Meetings

- Avtex will provide State of West Virginia with at least monthly Support Statistics via your personalized Power BI view to review support statics ad-hoc
- Avtex will meet onsite with State of West Virginia quarterly to review Support Statistics
- Avtex and State of West Virginia will meet on a reoccurring scheduled cadence to review open incidents
- Avtex and State of West Virginia will meet after 3 months, 6 months and 9 months
  - Evaluate hours consumed and determine if this agreement hours needs to be adjusted
  - Should the quarterly Managed Services hours show a ten-percent (10%) increase or decrease the parties agree to review and discuss an increase or decrease in the terms

## Incident Transfer

- State of West Virginia will submit issues to Avtex as described below:
- All requests for support and services will be submitted to the State of West Virginia Voice Services
- State of West Virginia Voice Services will triage and troubleshoot
- Upon determining the incident is related to the PureConnect Cloud solution the incident will be assigned to Avtex for resolution
- State of West Virginia will provide Avtex access to their Client ticketing system and collaborate with the Avtex Application Development team to integrate between Avtex and State of West Virginia ticketing systems
- Both State of West Virginia and Avtex will need to participate in design, deployment, testing and ongoing support of systems for integration.

## Exclusions

- Avtex is NOT required to provide support for:
  - Server and Desktop hardware support
  - Microsoft OS configuration that is NOT related to Avtex and Genesys software
  - Telephones – Hardware Provisioning and Deployment
- Telco
  - Account relationship, Initial contact, case creation, and assistance with resolution of issues
  - Coordination and resolution of new or change related issues. All changes will be coordinated with Avtex

## Services Details

### Move, Add, Change & Delete (MACD)

State of West Virginia will identify designated technical employees to contact and work with Avtex's Technical Assistance Center (TAC).

Avtex will perform the following as part of Move, Add, Change or Delete. MACDs are classified as small administrative Moves, Adds, Changes and Deletes from the PureConnect Cloud / Genesys solution, including but not limited to:

- Users
- Stations / Managed Phones
- Client Templates
- Workgroups
- Roles
- Status Messages
- Dial Plan
- Phone Numbers (DID Table)
- Password Policies
- Schedules
- Reports
- Wrap-up codes
- ACD Skills
- Interaction Recorder - Categories, rules, policies
- Interaction Dialer - Call lists, campaign creation
- Interaction Optimizer

Client requested changes beyond the scope of MACD.requests above would require scoping by Avtex. These requests will be treated as small projects, requiring either a change order or a scope of work, and will be invoiced at the Avtex current or client contracted labor rates.


### Tier One Troubleshooting

State of West Virginia will identify designated technical employees to contact and work with Avtex's Technical Assistance Center (TAC) for troubleshooting.

This option provides relief for the client's PureConnect staff. State of West Virginia's end users continue to process requests and or issues through client's internal processes. When the need arises to contact Avtex support for assistance, the client's designated contact(s) will open a CTN with Avtex. From this point forward Avtex will work directly with the end user(s) to resolve the issue.

The Tier I specialist will gather the client's information and determine the client's issue(s) by analyzing the symptoms and figuring out the underlying problem. This includes troubleshooting methods such as:

- Verifying physical layer issues
- Resolving username and password problems

 **avtex** the point of interaction™

- Uninstalling/reinstalling basic software applications
- Verification of proper hardware, software and applications set up
- Assistance with navigating around application menus

Personnel at this level have a basic to general understanding of all Avtex supported hardware and applications.

## Transition to Support

When we engage a client for support of their environment we conduct a transition to support meeting to ensure we are covering all aspects of the support process with our clients. This meeting includes personnel from the Avtex team as well as the State of West Virginia team. As part of the meeting, we go over the support process to include opening, updating, and resolving CTNs as well as defining contacts for each company, appropriate monitoring sets, maintenance windows, remote access and other items.

This meeting allows both parties to “get on the same page” as well as ask questions and provide more details as to how we will work together in our partnership.

## Product and Services Quote

Included in Customer Service Agreement CSA cost illustrated in section 1 Term and Amount.

## Additional Information

**Effective Date:** January 1, 2019

**Agreement Length:** 12 months

## Support Services and Responsibilities

- English proficiency is required to contact Avtex TAC.
- Information Technology (IT) support services will be available Monday Through Friday (Avtex designated holidays excepted) during normal business hours
- To provide the most efficient level of service, Avtex will not take calls directly from end users but rather use the State of West Virginia service desk to funnel their support through to Avtex. The service desk should be able to determine if it is a PureConnect issue, an issue on their network, etc. Routing would be as follows:
  - Non-critical during business hours – call, email, open ticket via OnPoint (Avtex client portal)
  - Non-critical after business hours – call, email, open ticket via OnPoint (Avtex client portal). For non-critical requests opened outside normal business hour, Avtex will respond the next business day.
  - Business Critical issues regardless of time of day or location of end-user – call Avtex support directly
    - During business hours will be answered by a live support technician

- After-business hours will be handled by an answering service, who will contact Avtex on-call personnel to work on the incident.
- Support agreement incidents are prioritized by severity, and then by the order in which each incident is received. Critical equipment outages are treated with the highest priority. Avtex will make a good faith attempt to acknowledge every support Incident within two (2) hours from receipt of Service Request, during normal business hours

## Client Responsibilities

- Train Avtex Resources on Client's standards and procedures for Security, Change Management, Stakeholder Communication, and System Availability Protection (maintenance windows), and where those standards and procedures are stored and maintained.
- Provide Avtex Management the location of Client's standards and procedures and a list of client tool sets used to deliver Support and Managed Services.
- State of West Virginia will assign a Client Project Manager and Release Coordinator to manage end-user communications for Genesys software Release and Patch updates.

## Assumptions, Constraints, and Identified Risks

- Client will be responsible to have a suitable, serviceable broadband connection (defined as cable, DSL, partial to full T-1, or greater bandwidth) and agrees to provide the necessary cooperation to allow an engineer online via an acceptable and secure Internet connection to gain remote access to Client's system(s) or providing remote monitoring, support and troubleshooting
- If it is determined by Avtex and the client that an issue needs to be escalated to the manufacturer of the software or hardware being supported (e.g. Microsoft, Mediant, etc.) any fees associated with engaging the manufacturer will be the responsibility of the client.
- Client will provide Escalation lists and protocols, including contact names, contact methods, response policies and procedures, and definitions of critical events.
- Client agrees to provide necessary cooperation to assist Avtex in providing support via telephone or remote support tools **before** on-site service is requested
- Client will, to maintain security from threats via the Internet, have in place a hardware firewall protection device acceptable to Avtex
- No illegal, unlicensed or "bootlegged" software will be installed, supported or serviced by Avtex
- Avtex will invoice an hourly fee of at our current Avtex labor or negotiated rates for engineering time used to troubleshoot any non-PureConnect server, device or application. Additionally, Avtex will invoice current Avtex labor or negotiated rates for any engineering time used to troubleshoot or reconfigure the PureConnect instance and the infrastructure on which PureConnect resides. If State of West Virginia or any 3rd party modifies the PureConnect instance or infrastructure.
- All software installations, hardware replacements, upgrades or configuration changes must be performed by Avtex unless otherwise agreed in writing. Avtex will invoice Avtex standard rates during



normal business hours with a minimum of two hours for engineering time used to troubleshoot or reconfigure servers, desktop computers, laptop computers, notebook computers, routers, firewalls, managed switches, backup devices, network devices, or telephony systems that have been modified by anyone other than Avtex. Client is responsible for the cost of all hardware components, software, consumables and related costs for repair and/or replacement of equipment not covered under warranty

- Incidents that cannot be completed during normal business hours will be completed by Avtex during the next available normal business day time slot. If Client requests Avtex to continue to work after normal business hours, Client will pay for after-hour emergency services provided at the after-hours rate outlined in the Customer Support Agreement (CSA) with a two-hour minimum unless included within the Services listed above
- This support agreement includes support incidents but does not include enhancements on the various platforms. Such requests must be made through your Account Executive or Client Account Manager. These requests will require a separate statement of work.

### Warranty

Nothing herein to the contrary notwithstanding and except as expressly stated in this agreement Avtex does not make, and hereby disclaims all expressed or implied warranties, including, but not limited to, warranties of merchantability, fitness for purpose, non-infringement and title and any warranties arising from a course of dealing, usage or trade practices.

- Product warranties, if any, are provided by the respective manufacturer(s) or publisher(s) of the respective products and not by Avtex. Avtex's sole obligation is to act on behalf of Client to assist in the satisfaction of the manufacturer's or publisher's warranty;
- Avtex hereby warrants that any products or materials to be installed by Avtex's technicians will be installed in a good and workmanlike manner, consistent with generally prevailing and accepted industry standards for comparable services, and in compliance with the requirements of this agreement. Services will be performed or provided in compliance with all statutes, acts, ordinances, laws, rules, regulations, codes and standards.

### Escalation

If the Client is dissatisfied with Avtex's service under this agreement, please contact your Avtex Account Executive. An Avtex manager will review the concern, investigate, and reply within one business day. Some issues may require detailed investigation and more than one day for resolution.

### Fees and Payment Terms

This agreement is valid for 30 days. If Client has not accepted the agreement within a 30-day period, by virtue of authorized signature, then the agreement is no longer valid.

**Note: Any travel and applicable taxes are not included in this summary.**

**Fees**

**Annual Support Services Agreement**

Fees will be invoiced on an annual basis and are due upon receipt.

Professional Services outlined in the agreement will be 100% due upon signature unless other payment terms were agreed upon and written in this agreement.

This agreement will automatically be renewed unless written/email notice is provided by the Customer thirty (30) days prior to the end of the term.

**Payments**

Client will be responsible to pay all applicable shipping and sales and use taxes; however designated, incurred as a result of or otherwise in connection with this agreement or the Services. Any invoice not paid within 30 days after it is sent to Client will accrue interest at 1.5% per month or, if lower, the highest rate allowed by law.

**Billing Profile Information:**

Billing Address: \_\_\_\_\_

Billing Contact Name: \_\_\_\_\_

Contact Phone: \_\_\_\_\_

Contact Email: \_\_\_\_\_

**No change to current billing information**

**Acceptance**

This Agreement is made between **Avtex Solutions, LLC** ("Avtex"), and **State of West Virginia**, ("Client") pursuant to the terms of the Master Sales Agreement that Avtex and Client have executed.

In WITNESS WHEREOF, Avtex and Client cause this Agreement to be duly executed below.

**Avtex Solutions, LLC**

**State of West Virginia ("Client")**

Signature: \_\_\_\_\_

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_



## Appendix A - Priority Levels

“Priority Levels” are the severity designation assigned to a Problem or Incident (i.e., Emergency, High Priority, Medium Priority, or Low Priority). All Problems, Incidents and/or contacts with the Service Desk will be logged and assigned a level of priority considering these Severity Levels which are identified in the table as follows:

Severity Level	Description	Criteria for Severity Level (one or more may be present)
Emergency	Critical Business Impact	<ul style="list-style-type: none"> <li>• Total loss of critical application / system</li> <li>• One primary or all Facilities are impacted, and users are unable to perform their duties</li> <li>• Total loss of production service(s) to any part of Client’s business and no workaround, bypass or alternative is immediately available</li> <li>• Impacts one or more Service Levels, revenue streams or delivery schedules</li> <li>• An imminent outage that could turn into a total loss of production service(s) or could cause any of other Severity Level 1 criteria described above</li> </ul>
High Priority	High Business Impact	<ul style="list-style-type: none"> <li>• A key enterprise component, application, critical system or network is down, degraded or unusable</li> <li>• Major loss of production service(s) to any part of Client’s business that does have a work around</li> <li>• Processing is severely impacted or multiple Clients are impacted and no acceptable workaround, bypass or alternative exists</li> <li>• Potential critical impact on a Service delivery condition exists</li> </ul>
Medium Priority	Medium Business Impact	<ul style="list-style-type: none"> <li>• An enterprise component or procedure is down, unusable or difficult to use</li> <li>• Minor loss of an application(s) or production service(s) is degrading service but does not prevent the delivery of service to the Client</li> <li>• Impaired ability to deliver service affecting scattered users</li> <li>• Problems that would be considered Severity Level 1 or 2 that have a workaround, alternative or bypass</li> <li>• An acceptable workaround, alternative or bypass exists</li> </ul>
Low Priority	Low Business Impact or Question	<ul style="list-style-type: none"> <li>• Component or procedure that is not critical to the Client</li> <li>• Alternative is available, deferred maintenance is acceptable</li> <li>• An acceptable workaround, alternative or bypass exists</li> <li>• Minimal impact to business</li> <li>• No production systems, applications or environment is affected</li> <li>• How to questions</li> </ul>

## Appendix B - Service Level Guidelines

Priority	Business hours	Non-Business hours and Holidays	Hours of Activity
<b>Emergency</b> <i>Requires live call into queue</i>	Initial Contact: Immediate Follow-up: Constant	Contact: 30 min Follow-up: Hourly Escalation: 4 Hours	24 x 7
<b>High</b> <i>Live call into queue</i>	Initial Contact: Immediate Follow-up Service Level: Daily	Contact: 10:00 AM Central next business day Follow-up Service Level: Daily	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>High</b> <i>OnPoint or E-Mail</i>	Initial Contact: 4 Hours Follow-up Service Level: Daily	Contact: 10:00 AM Central next business day Follow-up Service Level: Daily	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Medium</b> <i>All interaction types</i>	Initial Contact: 4 Hours Follow-up Service Level: 3 business Days	Contact: 10:00 AM Central next business day Follow-up Service Level: 3 business Days	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Low</b> <i>All interaction types</i>	Initial Contact: 4 Hours Follow-up Service Level: 5 Business Days	Contact: 10:00 PM Central next business day Follow-up Service Level: 5 Business Days	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays
<b>Move, Add, Change, Delete</b> <i>All interaction types</i>	Requests will be completed within 2 business days after receipt of the request	Changes will be scheduled during Avtex business hours and will be completed within 2 business days after receipt of the request	7:00 AM-7:00 PM (Central) Monday thru Friday, excluding holidays

## **Attachment 4.2.2.4.3 - Avtex - State of West Virginia - SOC 2 Letter**

Please find the attachment on the following page.

April 18, 2018

Avtex Solutions, LLC  
3500 American Boulevard West  
Suite 300  
Minneapolis, MN 55431

Type II SOC 2 Completed  
April 1, 2017 - March 31, 2018

Avtex Solutions, LLC has completed a Type II SOC 2 examination covering the Security and Availability Trust Services Criteria related to Avtex's hosting and managed services. The report was for the period April 1, 2017 through March 31, 2018. The examination resulted in an unqualified opinion. The examination was performed by Linford & Company LLP, a Certified Public Accounting firm.

*linford & co llp*



## **Attachment 4.2.2.5.2 - Avtex Project Process Overview 2018**

Please find the attachment beginning on the following page.

# Avtex Project Process

## Overview



## Avtex Project Management Overview

The Avtex Project Management approach works hand in hand with the customer's project team. The Avtex Project Manager is the main point of contact on the Avtex Project Team once the project is initiated. Our project managers are trained in various industry standard project management processes, including Waterfall and Agile Scrum, and most carry project management credentials in those methodologies.

Our Project Manager will bring implementation knowledge and experience for deploying similar projects and help your project team understand and plan for the tasks they will need to complete to hit target timelines. A regular cadence of planning and status meetings will be scheduled with the core project team, and regular additional project communication will be provided through status and budget reporting and dedicated SharePoint project portals for collaboration.

When the customer Project Team includes a Project Manager or a Project Management Office, our Project Manager will team up with the customer's Project Manager to deliver the best possible solution for the customer. If the customer does not have a Project Manager, the Avtex Project manager will work closely with the customer's designated project lead.

Avtex has three basic project implementation methodologies and processes depending on the type of project:

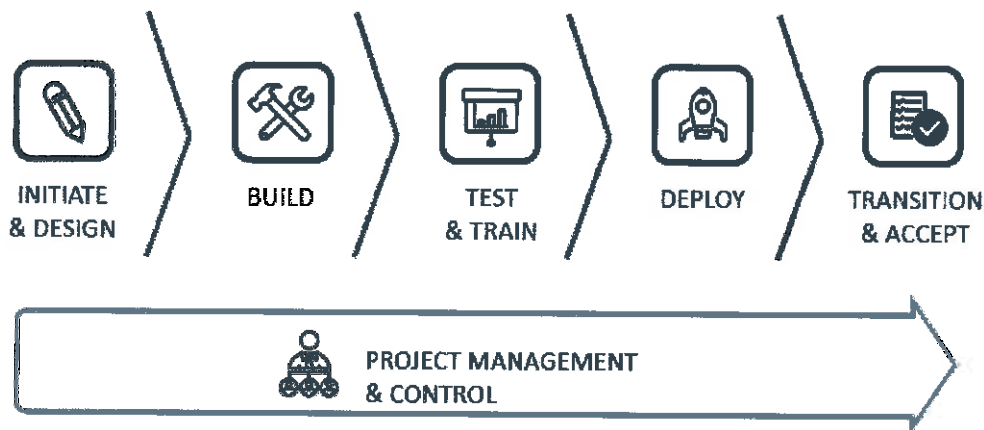
- Avtex Standard Project Implementation Methodology
- Avtex Iterative Project Implementation Methodology
- Avtex Consulting Project Methodology for Small Projects



## Avtex Standard Project Implementation Methodology

The Avtex Standard Project Process methodology follows a five (5) Phase process, with Project Management throughout the project.

This methodology is generally used for our implementation, upgrade and enhancement projects in the Contact Center, Unified Communications, SharePoint, Office 365 spaces, as well as smaller CRM Implementations and Enhancements and smaller Application Development projects.



### Initiate & Design

Avtex will assign the project team upon signature and the project team will work with the sales team to transition the project into delivery and kick-off the project with the client. Any design workshops, final design documentation required and infrastructure readiness will occur during this phase.

- Project Initiation & Planning Tasks
- Project Kick-off Meetings
- Software/Hardware Procurement
- CX Assessment Engagement, if applicable
- Design Workshops / Meetings
- Design Documentation
- Preliminary Test Plan
- Preliminary Training Plan
- Customer Hardware & Network Readiness, Installation / Build
- Voice Readiness Assessment (VRA), if applicable
- **Milestone: Design Approval**



## Build

Avtex engineers, developers, and application consultants will complete installation, configuration and custom development work included in the scope of the project. Base functionality and unit testing is completed by resources as part of their efforts during the solution build out.

- Installation, Configuration, Development, Unit Testing
- Final Test Plan
- Final Training Plan
- Customer Starts User Acceptance Testing (UAT) Scripts & Case Development
- **Milestone: Installation, Configuration and Development Completed**

## Test & Train

The test and train phase requires resources other than the original engineer, developer and or consultant to test the solution to verify it meets agreed upon designs, and most importantly requires the customer to test the solution and confirm the required functionality and business cases are tested to ensure it meets designs and business needs. Adjustments will be made based on test results if they did not meet the design requirements. Occasionally new requirements result from business test cases that may require change requests, which will be handled through the project change management process.

Avtex trainers will train your key resources, i.e. SMEs, Team Leads, Trainers, Administrators during this phase, most often prior to UAT to ensure your UAT testers are able to effectively complete test scripts. Customers' trainers will take the training and complete preparations for their end user training in the Deploy Phase.

- QA Testing
- Customer Completes UAT Test Script & Case Development
- Train the Trainer Sessions
- Customer Completes End User Training Plan
- UAT Kick-off
- Customer User Acceptance Testing (UAT)
- UAT Support & Adjustments
- **Milestone: UAT Acceptance**
- Customer Training Development
- Production Deployment/Cutover Plan
- **Milestone: Production Go/No Go Decision**



## Deploy

The Deploy Phase is putting the new solution into a production environment, or the final environment included in the solution and scope.

- Customer End User Training
- Deployment / Cutover
- Data and/or Configuration Migration
- First Day of Service
- Second Day of Service, if applicable
- **Milestone: Production Usage**

## Transition & Accept

The Transition & Acceptance phase handles transitioning the environment from the project team to the appropriate support organization, be that an Avtex Support team or the customer's support organization. Most projects include a short Post Implementation Support / Hyper Care period of about two weeks, unless otherwise agreed to, to handle post production questions and punch list items to ensure that smooth transition. This phase also includes any additional environment refreshes, switch-overs and any training that requires production data to complete.

- Post Implementation Support / Hyper Care
- Switch Over, if applicable
- Hand-off to Support
- Additional environment refresh, if applicable
- Post Cutover Training Requiring Production Data, i.e. Analyzer, WFM/Optimizer, etc.
- Project Closure Tasks
- **Milestone: Project Acceptance and Closure**

## Project Management and Control

Project Management encompasses the project and occurs from the beginning of the project until the project is accepted and closed.

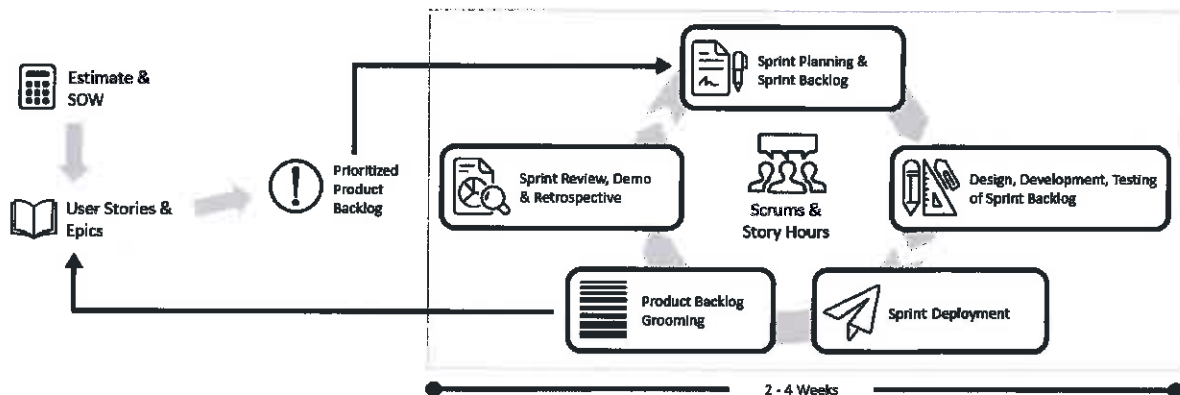
- Avtex Project Team Project Status and Planning Meetings
- Full Project Team Project Status and Planning Meetings
- Project Status Reporting & Communication
- Project Budget Management and Reporting
- Task Management and Reporting
- Issues & Risk Management and Reporting
- Resource Management and Reporting
- Schedule Management and Reporting
- Project Change Management
- Training and Test Planning Management



## Avtex Iterative Project Implementation Methodology

The Avtex Iterative Project Process methodology is time boxed, repetitive and collaborative approach based on the Agile Scrum methodology. It provides the product owner the ability to regularly assess and reassess the priority of the work that will get completed in a specified time box called a Sprint. This methodology allows the team to focus on the highest priority items and drive those to completion more rapidly.

This process is generally used at Avtex for larger Application Development projects, some large CRM Implementations with custom development and on-going product/solution enhancements.



Our Iterative Project process uses most of the standard Agile Scrum terminologies, assets, and meetings, with some adjustments to better adapt it to a consulting engagement.

- **Sprints:** A Sprint, the timebox for the current work, will generally be run two - four weeks in duration. Sprints, or iterations, for a specific project will all be of the same agreed upon duration.
- **Product/Project Backlog:** ordered list of desired features, outcomes, issues, etc. owned by the Product Owner.
- **Sprint Backlog:** committed project backlog items broken down into tasks and owned by the team.
- **Scrum Meetings:** a 15-minute daily time-boxed event for the Team to inspect, adapt and transparently synchronize on the Sprint Goal. Team members answer the following three questions:

- What did I accomplish yesterday?
- What will I accomplish today?
- Are there any roadblocks?

All members of the project team including the customer team are welcome to attend the daily scrum meeting but any discussion beyond the three questions from the developers will take place separately from the scrum meeting.

- **Sprint Review/Demo:** an inspect and adapt mechanism for the Product Owner to get feedback on the working product increments from stakeholders. Sprint Review will be



held at the end of each sprint prior to the next sprint planning activity. Any updates requested as a result of the sprint review will be captured in the Product Backlog and prioritized by the Product Owner.

- **Backlog Grooming:** Working session scheduled with product owner, key business stakeholders, scrum master as well as technical resources as required. The objective of this working session is to review the product backlog, adjust priority and identify user stories to be included in the next sprint.

In addition to Agile Scrum focused methodology, there will be regularly scheduled Project Sponsor status meetings to report progress, issues, opportunities and hours to the executive leadership. These meetings will include sponsors, product owner, project manager, scrum master but generally not the development team. All status reports as well as an ongoing issues list will be maintained on the project's Avtex OnPoint collaboration site.

For our Application Development projects in addition to the above standard scrum ceremonies and processes, we recommend adding a weekly Story Hour.

- **Story Hour:** Given the distributed nature of the team, a designated "Story Hour" may be scheduled once a week throughout the duration of the development effort. The purpose of Story Hour is to give the team the opportunity to review User Stories under development to clarify objectives and expected behavior of the system as a group. This ensures common understanding across the team. The Product Owner, Scrum Master, Team and invited SMEs are involved in the Story Hour.

## Avtex Consulting Project Process for Small Projects

A project that does not require engineering, development and/or deployment of any kind will be run as a single Consulting Phase. This type of engagement is used for Discovery, Assessments, WFM Consulting, Training Engagements, etc. CX Consulting projects also follow this process but have additional sub-phases to track specific scope milestones.

Some very small enhancement projects will be run using our Avtex Consulting Project Process as well, with a single phase and basic tasks to build out, test and deliver the agreed upon solution to the client in an as efficient manner as possible.

A Project Manager or Coordinator will be assigned to interface with the client and ensure proper scheduling and coordination and hand-off between resources and the client.

**Attachment SO-1 - Avtex - SoWV - Managed and Hosted Voice Services - Base Configuration SOW\_Redacted**

Please find the attachment beginning on the following page.



# Managed and Hosted Voice Services - Base Configuration

## Statement of Work

**Prepared for:**  
State of West Virginia

**Prepared by:**  
Matt Coy  
*Account Executive*  
mcoy@avtex.com  
(847) 664-8887

Mark Granquist  
*Solutions Consultant Team Lead*

November 7, 2018

avtex  the point of interaction

Avtex Solutions LLC.  
3500 American Blvd West  
Suite 300  
Bloomington, MN

# Table of Contents

---

<b>Executive Summary.....</b>	<b>3</b>
CX Experience Analysis .....	3
About Avtex .....	4
<b>Solution Overview.....</b>	<b>5</b>
Application Summary .....	5
Architecture Summary.....	6
Cloud Components.....	6
Premise-Based Components.....	7
Design Assumptions .....	7
Architecture Diagram .....	8
<b>Applications and Integrations .....</b>	<b>9</b>
Interaction Attendant / Inbound Call Routing .....	9
ACD Routing and Queue Management .....	9
Historical Reporting.....	10
Scheduled Reports.....	10
Customer Access to Reporting Data .....	10
Interaction Recorder with Quality Management.....	10
Interaction Dialer .....	11
Unified Messaging.....	12
Microsoft Skype for Business Integration.....	12
Voice Readiness Assessment Overview.....	13
Voice Readiness Assessment Services Overview .....	17
<b>Project Implementation .....</b>	<b>19</b>
Avtex Project Process .....	19
Project Management and Control.....	20
Avtex Professional Services .....	20
<b>Implementation Assumptions .....</b>	<b>25</b>
<b>Pricing.....</b>	<b>28</b>

## Executive Summary

West Virginia Office of Technology is seeking proposals from Vendors to establish an open-end, Statewide Contract for Managed Voice Services and Hosted Voice over Internet Protocol ("VoIP") Services, encompassing Unified Communications as a Service ("UCaaS"), and Hosted Contact Center Services.

It is the State's intent to establish a contract with a single Vendor to provide maintenance, management, and support for the State's current IP Telephony platforms while working to migrate those telephony services to a fully managed and hosted VoIP solution. Additionally, the Vendor will be expected to provide daily management and operational support for multiple Contact Centers while working to migrate those Contact Centers to its hosted solution.

Avtex is pleased to respond with a proposal for the PureConnect Cloud platform from Genesys to meet State of West Virginia's requirements for a contact center solution. This Statement of Work describes the solution design, hardware and software requirements, scope of services provided by Avtex, and State of West Virginia responsibilities. Once the project team is assigned, Avtex will work with State of West Virginia to create the Solution Design Document, which serves as the project blueprint and captures the detailed, customer-specific application requirements.

This Statement of Work includes pricing for Avtex Professional Services to design, build, and implement the solution. Genesys will provide the cloud-based infrastructure and systems, and Avtex will manage the project from kickoff through support-transition, working closely with the Genesys and State of West Virginia teams throughout the process.

### CX Experience Analysis

This project includes a CX Experience Analysis, intended to begin at the start of the project. During the implementation, the Avtex team will review each customer contact center interaction and define the functional and emotional needs of the interaction. This analysis will be used to help configure the PureConnect platform. The analysis will include:

- Definition of the various customer contact center interactions
- Workshop to define the emotional and functional needs of the customer for each interaction
- Definition of leading practices for those interactions
- Capability analysis of the PureConnect platform
- Integration and Configuration recommendations

**Note:** The Project Change Order process will be used to document and approve any new applications or integrations that may be identified in the CX Analysis, but not defined in this Statement of Work. This includes any potential licensing changes. The teams will then determine the estimated impact to the project budget and decide how and when to move forward with those enhancements.

Key differentiators of PureConnect Cloud include:

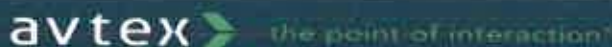




- **Experienced and Proven:** Genesys is an experienced and proven contact center and unified communications solutions provider, offering the PureConnect Cloud solution based on a single, all-in-one IP communications software suite with more than 6,000 customer deployments. PureConnect Cloud offers data isolation through a single-customer, multi-instance environment, with industry-certified security, giving customers an option to keep all voice traffic within the customer's network.
- **Breadth of Functionality:** Giving customers a higher return on their investment, Genesys delivers a cloud solution that provides the broadest inbound and outbound multichannel contact center and UC functionality, developed and delivered by a single vendor. This functionality includes IVR, multichannel routing and recording, screen-pop, outbound/blended dialing, quality monitoring, workforce management, desktop call control, desktop faxing, unified messaging, and presence management.
- **Flexibility:** Enabling customers to better adapt to changing business needs, PureConnect Cloud offers several deployment choices; the ability to migrate from the cloud to on-premises should business needs change; and a simplified method for adding new applications.
- **Reliability:** PureConnect Cloud offers guaranteed service levels with 99.999% application uptime. This includes geo-redundancy across Genesys global data centers and proactive monitoring as well as outstanding support from a 24/7 world class Network Operating Center (NOC).
- **Security:** PureConnect Cloud is the solution of choice for large mission-critical operations that demand ultimate security. Customers are isolated from one another via virtualization and segmented infrastructure within a larger cloud network. For added level of security, Genesys uniquely offers customers the option to keep all voice traffic and sensitive customer data within the customer's network.
- **Integration:** Many customers are highly invested in applications from 3rd parties like Oracle, Microsoft and Salesforce.com to name a few. Genesys has a dedicated team focused on developing, enhancing and maintaining a deep level of integration with these CRM and UC applications. This allows customers to leverage their investment in these best of breed applications within their contact centers.
- **Customization:** No two contact centers are the same. Even within the same business verticals, contact centers differentiate themselves and their services by customizing their contact center applications to service the business needs and those of their customers. PureConnect Cloud offers the greatest level of customization and integration in the cloud through comprehensive APIs and an experienced service team.
- **Deployments:** PureConnect in the cloud is a global offering collocated at top-tier data centers in North America, Canada, United Kingdom, Germany, Australia, Brazil and Japan. These data centers provide state of the art physical and logical protection of all interactions, and the Operations Team manages all components of the service located at these data centers.

## About Avtex

Avtex is an end-to-end CX technology deployment partner that provides professional services and solutions. Our customers receive unique CX technology deployment delivered with accuracy, consistency and vision specific to their organization to ensure an integrated customer experience for every point of interaction. We provide



professional services and strategic consulting encompassing a full 360 suite of solutions ranging from unified communications, contact centers, portals, custom applications, infrastructure and CRM.



Driven by technology know-how and passionate about customer experience, Avtex is uniquely qualified to help clients deliver exceptional experiences to their customers using technology.

## Solution Overview

### Application Summary

The proposed PureConnect Cloud solution will provide State of West Virginia with the following capabilities. The Project Scope section includes additional details.

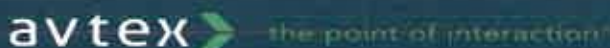
- Resident/Citizen Experience Consulting – CX Engagement
- Business User Client Access
- ⊗ Attendant/IVR less than 30 selections includes 6 queues under 3 routing criteria. Single data dip less than 3 self-service entry read back only add-on.
- ⊗ Dialer, 1 agent based basic scripting and 1 agentless campaign.
- Recording and Quality Management
- ⊗ Supervisor dashboard
- ⊗ Multi-channel ACD
- Skype server integration – Best effort based on PureConnect Cloud and Selected Skype Platform
- ⊗ Voice Readiness Assessment for 2 locations plus the Data Center
- ⊗ Development Environment
- Single cutover project

## Architecture Summary

- A geo-redundant design will be provided, leveraging Genesys data centers in Carmel, Indiana; and Denver, Colorado.
- Genesys will provision PureConnect Cloud systems in a PCI Zone to support State of West Virginia's requirements for PCI compliance.
- A "Remote Control Media" design is proposed. This is a full-cloud architecture in which a hosted PSTN connection is provided in the PureConnect Cloud data centers. The benefit to State of West Virginia is the lack of premise-based hardware and telephony infrastructure to purchase and maintain. A network connection and phone are all that an agent needs to begin using the platform.
- Genesys will provide SIP circuits in the PureConnect Cloud data centers for PSTN access.
- An MPLS connection is required between the State of West Virginia and Genesys networks. State of West Virginia will maintain their existing MPLS-carrier relationship and have their carrier bring MPLS circuits into the PureConnect Cloud data centers to connect the networks.
- Skype for Business
- End-User Voice Endpoints: AudioCodes, Polycom VVX and SIP Softphones
- Uncompressed G.711 RTP codec will be used for all call paths. If there are bandwidth constraints, licensing for G.729 compression may be added to the system.
- Telephony Port licenses are required for SIP circuits terminating in the Genesys data centers. A non-blocking architecture is based on an agreed-upon need for (910) Telephony Ports to support the required number of simultaneous contact center calls. State of West Virginia will commit to a minimum number of ports in their service contract with Genesys, however the architecture will scale to support periods of increased volume, with overage billed as applicable.
- Remote Content servers will be located in the Genesys data centers.
- The Interaction Dialer configuration will include two Central Campaign servers configured in a geo-redundant failover configuration.
- 911 Calls
  - Standard configuration is as follows: Each user/station location can be assigned an Outbound ANI that is sent to the carrier when a user dials 911. As long as the carrier can accept a call "from" the specified ANI, they will route the call to a Public Service Access Point (PSAP). The PSAP must have the correct corporate address on file for the ANI received in order to determine the *general* location of the caller. It is the customer's responsibility to provide ANI to Location mappings to the carrier.

## Cloud Components

The following components are planned for location in the Genesys data centers. State of West Virginia's PureConnect Cloud contract with Genesys must reflect this proposed design.



- PureConnect Production switchover pair: Geo-redundancy between primary and secondary data centers
- PSTN Connectivity – Circuits and SIP Gateways
- Media Server resources
- Dialer Campaign Server(s)
- Remote Content Server(s)
- Recording file storage
- SQL Server Reporting Database

## Premise-Based Components

- Phones

## Design Assumptions

- Final bandwidth estimates to be determined based on number of concurrent users/calls per location.
- G.711 is the default codec for voice through the PureConnect system.
- All voice devices or endpoints are SIP-compliant.
- The PureConnect Solution will leverage State of West Virginia's Active Directory Services for authentication.
- SIP carrier supports outbound Dialer applications and at least 10 call setups per second. The required rate may be greater. Support and maximum CPS must be confirmed prior to using a SIP trunk with Interaction Dialer. While it is possible that Dialer requirements may be met with less than 10cps depending on campaign types and objectives, it is critical to have full carrier support to avoid failed call attempts or service interruptions.

# Architecture Diagram

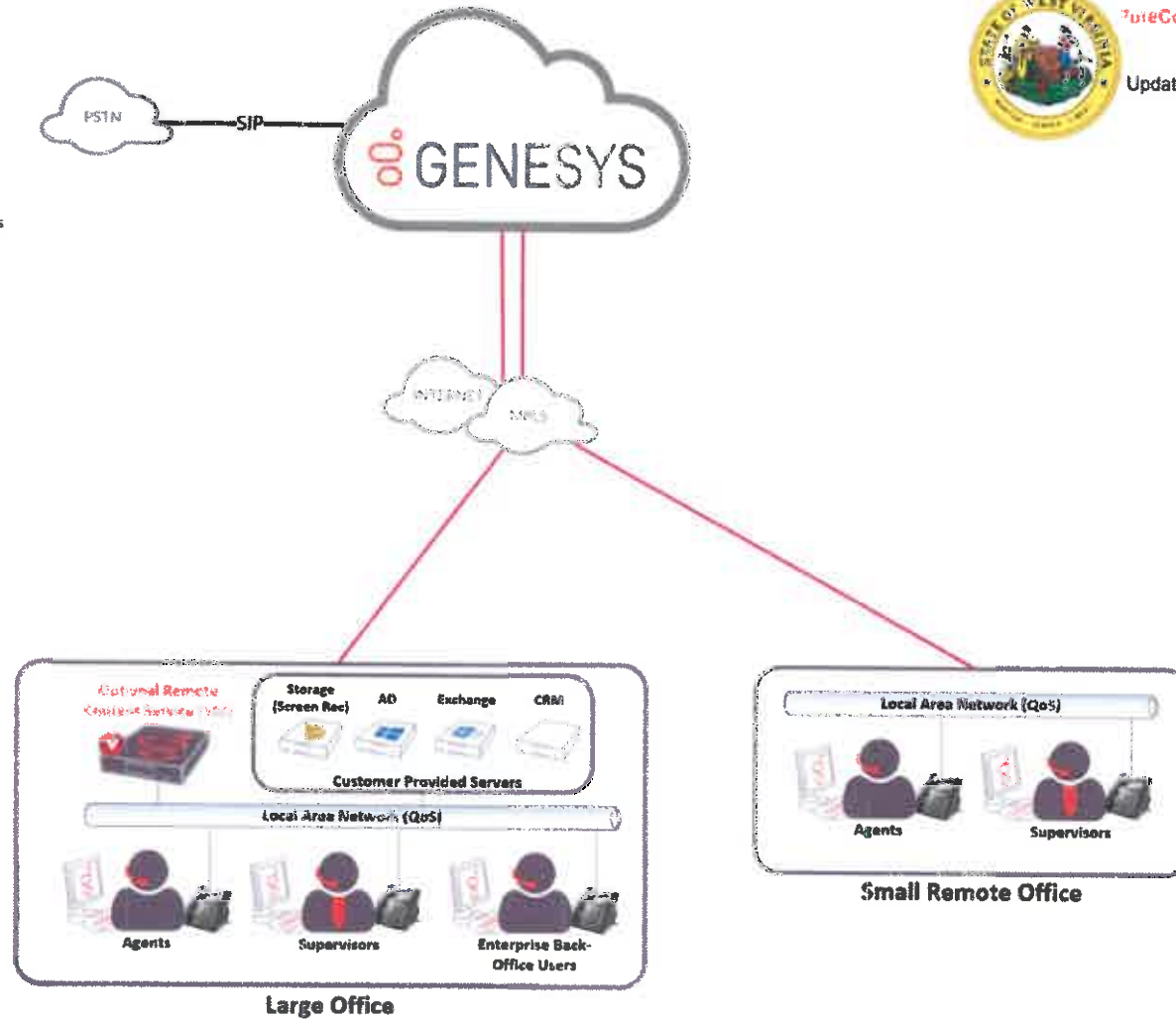


State of West Virginia  
 Hosted Voice Services  
 PureConnect Cloud RCM base

Last Update: 11/16/2018  
 Updated By: Mark C Granquist  
 Revision #1  
 Confidential and Proprietary

**Design Assumptions:**

- PureConnect Cloud provided SIP trunk carrier services will be provided.
- Access to PureConnect Cloud services is established via the customer provided Verizon MPLS connection. Some services (like the agent web-based interface) can be made accessible via the public internet.
- Customer responsible for LAN QoS and firewall
- Bandwidth calculations to be sized based on IP Endpoints utilized and codecs utilized
- RCS used to manage local screen recording storage and streaming



## Applications and Integrations

### Interaction Attendant / Inbound Call Routing

#### Scope Summary

Call flow/script requirements have not been identified. Avtex will work with State of West Virginia to design and document the configuration that will be created on the PureConnect system. Configuration will not begin until State of West Virginia has signed off on the final call flows.

### ACD Routing and Queue Management

The PureConnect automatic call distributor (ACD) is an integrated component of the platform. During the Design phase of the project, State of West Virginia's queue details, routing and queue management requirements will be determined.

#### Scope Summary

- The following ACD media types are included:
  - Call, Voice Callback, Email
- Skills Based Routing if needed - One or more skill requirements will be specified before an interaction is transferred to an ACD workgroup. Each agent will have an assigned Proficiency level for each applicable skill in Interaction Administrator, and this will influence the agent-selection process.
- Standard Voice Callback Requests
  - Callers will be given the option of requesting a callback rather than wait in queue. This may occur before entering a queue (based on look-ahead queue conditions) and/or after waiting in a queue for a period of time. The system will use either the ANI or allow the caller to enter a phone number.
  - The original call is replaced by a callback object that retains the same position in queue.
  - The callback is routed to the next available agent in a preview manner so that they can click to initiate the call.
  - Upon conclusion to the call attempt, the agent must disposition or close out the attempt as a Success or Failure for reporting purposes.
  - Standard callbacks do not support the concept of multiple attempts or retries other than the Retry Later button:
    - The Retry Later button appears only if your PureConnect administrator has enabled this feature. Click this button to remove the callback request from your queue and place it back on the workgroup queue in a "Snoozed" state. After an interval configured by your PureConnect administrator, the callback request is processed as a new interaction on the workgroup queue. The PureConnect administrator also configures the maximum number of times agents can retry a callback request.



- Use of Interaction Attendant for in-queue audio sequence and options such as leaving a voicemail or requesting a callback.
- Any callback requirements outside of the above functionality will require a Change Order.

## Historical Reporting

PureConnect includes a package of reports as a standard offering available to licensed users. Standard reports are provided for call information such as call detail and summary, trunk line information such as usage and call detail, user information such as user call reports and user activity (status) reports, queue reports such as shift activity, service level reporting, and queue analysis. Graphical reports, detail reports, and summary reports are available as standard offerings.

A Reporting Assessment will be performed to discuss State of West Virginia's requirements. Based on the results of the reporting assessment, Avtex will determine if a Change Order is needed for any customizations.

Please refer to the following document for a sample of all reports included with PureConnect:

[https://help.genesys.com/cic/mergedProjects/wh\\_tr/desktop/pdfs/sample\\_reports\\_for\\_interaction\\_reporter.pdf](https://help.genesys.com/cic/mergedProjects/wh_tr/desktop/pdfs/sample_reports_for_interaction_reporter.pdf)

## Scheduled Reports

Scheduled Reports allows PureConnect users to schedule IC Historical Reports to run on a daily, weekly, or monthly, basis, and it can distribute those reports to multiple locations. The reports can be generated in different formats, such as Adobe Acrobat® PDF and Excel 8.0. Reports can be automatically distributed through e-mail messages, saved to a file, or printed.

### Scope Summary

- The Scheduled Reports monitoring service requires a separate server for installation (i.e. not located on the main PureConnect server). If applicable, it can also be co-located with Interaction Web Portal / Marquee. Avtex will install (1) instance of the monitoring service.
- A single Scheduled Reports Monitoring Server can service multiple PureConnect "CIC" servers.

## Customer Access to Reporting Data

- Genesys will host the PureConnect SQL database in the PureConnect Cloud data center. The live production database is only accessible via the standard built-in system reports.
- Upon request, Genesys can provide a free nightly export of the full production historical database. Exports are provided in a standard SQL backup format only to a PureConnect Cloud-provided FTP server. Each nightly export is only available for 24 hours. Customers are responsible for the retrieval, import and management of this data once it is provided. Import of this SQL Server export requires that the customers' own SQL Server match or be newer than the PureConnect Cloud current production version.

## Interaction Recorder with Quality Management

Interaction Recorder is a fully-integrated, feature rich, rules-based recording and Quality Management add-on to the PureConnect platform.

## Scope Summary

- System will record calls and other applicable/licensed media types as per the number of Interaction Recorder Add-on licenses.
- PureConnect Cloud includes access to screen recording for users that are licensed with the Interaction Recorder Add-on.
- Supervisors licensed with the Quality Management Add-on will have access to the Quality Management interface to create scorecards and document agent performance while reviewing recordings.
- Encryption of recordings is an optional selection to meet State of West Virginia's security requirements.
- PureConnect Cloud includes a standard amount of cloud-based storage for recording files, and additional storage can be purchased if needed. State of West Virginia can optionally store files on local infrastructure if preferred.

## Interaction Dialer

Interaction Dialer is a pre-integrated, add-on application that resides on top of PureConnect. With the capabilities provided in PureConnect, including ACD and multimedia queuing, Interaction Dialer adds the ability to blend inbound and outbound interactions. Interaction Dialer leverages PureConnect for outbound and blended predictive dialing, and provides call scripting, multisite campaign management, intelligent campaign staging, compliance options, and more.

Interaction Dialer has two server components. The Outbound Dialer Server component is installed on the PureConnect "CIC" application servers. The Central Campaign Server (CCS) component is installed on a dedicated server, and manages the database integration.

## Scope Summary

- The Design process will determine State of West Virginia's detailed campaign and list-management requirements, outbound call flows, agent script configuration, and any integration requirements to be included in the Interaction Dialer implementation. This information will be included in the Solution Design Document and will serve as the blueprint for the configuration.
- The Professional Services estimate is based on configuration of up to (2) Outbound Campaigns.
- A standard template will be used for the agent interface, with buttons and Call List information added according to specific requirements gathered during the Solution Design Document process.
- Interaction Scripter is the standard Dialer client. Agents will log into Interaction Scripter to handle campaign calls. The Professional Services estimate is based on standard script configuration performed within the Interaction Administrator application. This standard interface provides configurable call control buttons, call disposition choices, and customer information pulled from the Dialer database (Contact List table). Any information located in the Dialer database can be displayed for the agent. An important distinction with the standard scripting interface is that it is not able to directly pull in or modify data from other sources. Doing so would require an alternative configuration.

- The proposed configuration does not include writing Dialer call disposition results back to the system of record. Additional scoping would be necessary to determine the method of integration and specific data requirements.
- Based on State of West Virginia requirements, the following campaigns will be configured:
  - 1 agent based campaign with Basic Scriptor
  - 1 agent-less campaign with read only information

## Unified Messaging

Unified Messaging is available to licensed users. This allows voicemail and fax messages to be delivered to the users' email inbox (utilizing State of West Virginia's mail server for storage), or optionally to a file server on the network. Messages can be retrieved via email client, IC Client, or phone.

Desktop Faxing is available to licensed users to allow them to send faxes from their desktop by printing documents to the Interaction Fax virtual printer.

## Microsoft Skype for Business Integration

Genesys has developed an integration between PureConnect and Microsoft Skype for Business that provides the following standard features:

- **Synchronized Presence** – Configurable status mapping between systems
- **Common Directory** - Only available when using the Interaction Desktop user client
- **Direct SIP connection** – Allows the use of a Skype for Business voice endpoint as the station device for PureConnect calls, and allows direct calls between the platforms.
- **Launch Microsoft Skype for Business Instant Message and Video via Interaction Desktop** - Only available when using the Interaction Desktop user client
- **Interaction Desktop with Embedded Skype for Business Client** - Only available when using the Interaction Desktop user client

### Important considerations for Presence Synchronization when using Skype for Business Enterprise Voice:

- There are some additional considerations in an environment that includes Enterprise Voice, as there will now be two systems with PBX functionality.
- By default, the only presence state that is synchronized in both directions is "Do Not Disturb." Other status mappings are configured as one direction from PureConnect to Skype. Other two-way mappings may be enabled, but this should be approached with caution for ACD users, just to ensure that events outside of the contact center system do not unexpectedly affect an agent's availability to receive ACD interactions.
- From an ACD standpoint, it is recommended that PureConnect be solely responsible for managing an agent's status. This is to avoid unintended or unexpected consequences that may occur in some situations.

- If an ACD user makes or receives a call directly in Skype for Business, then PureConnect will not be aware of the call and will still consider them to be available for an ACD call. This can be addressed in the following ways:
  - Outbound calls can be dialed via the PureConnect client so that PureConnect is aware of the call. Since the agent may still dial calls via the Skype for Business client, the Skype for Business voice routing can be configured to send outbound calls to PureConnect, which will already be configured as a PSTN gateway in Skype for Business as part of the integration. This would not be necessary for non-ACD users.
  - If any agents are able to receive directed inbound calls, these should be routed to PureConnect, not Skype for Business. The agent will still receive the call on their Skype for Business phone, and if it rolls to voicemail, PureConnect will perform a SIP transfer to Exchange UM.

### Scope Summary

- A Skype for Business Trusted Application Server must be added to the topology to support the PureConnect status integration application.
- One application server will be configured for the PureConnect Production environment.
- Agents will use Skype for Business voice endpoints as their PureConnect station device.
- PureConnect will use a SIP trunk for communication with Skype for Business. This will be used for station connections and calls that may be placed between users on each platform.

### Voice Readiness Assessment Overview

Avtex will perform a remote Voice Readiness Assessment. The purpose of the assessment is to document the network and to determine if it is performing as required to support the needs of VoIP technologies. A successful Voice Readiness Assessment will provide confidence that the voice network will support the expected call volumes with high voice quality. This assessment is required for any part of State of West Virginia network for which voice traffic (SIP/RTP) will flow over.

#### Assessment Process

Avtex will deploy 3rd party network monitoring appliances that will reside at the client's location. The testing of the network will be performed during peak and non-peak times between various VoIP end-points. The State of West Virginia network team is responsible for ensuring the network is prepared for the assessment prior to the start of the Voice Readiness Assessment.

The voice assessments will determine if specific network paths will be able to handle a predetermined amount of VOIP traffic. Voice loss, MOS, latency, voice jitter, RTT and QoS markings will be measured at every hop across the path. Up to 100 concurrent calls can be generated for the assessment, which will then give a readiness score. Along with the call generator, Avtex will also be able to generate standard data traffic on the path to verify which traffic is being preferred and if QoS is being utilized. This will also help with tuning any QoS policies.

**The Voice Readiness Assessment will also validate that:**

- ⊗ Full Duplex is enabled on all voice network devices

- Latency in one direction is less than 150ms (for both SIP & RTP)
- Jitter is less than 30 milliseconds
- Mean Opinion Score (MOS value) for the G.711 audio codec is 4.1 or greater and for the G.729 audio codec is 3.9 or greater
- RTP packets include the proper markings for service priority queuing following the DSCP model
- Network segments do not exceed a packet loss rate of one per cent (1%)
- Network bandwidth is sufficient to allow for approximately 84kb/s per call using the G.711 audio codec and 21kb/s per call using the G.729 audio codec
- VLAN settings are set in accordance with the QoS for the xIC Platform and Microsoft whitepapers

### **Monitoring overview**

#### **Circuit/path monitoring:**

With the appliance installed, Avtex will be able to create paths, which traverse local or WAN links. This will help us determine where congestion is occurring, down to the device and interface. Data is gathered to determine the following metrics:

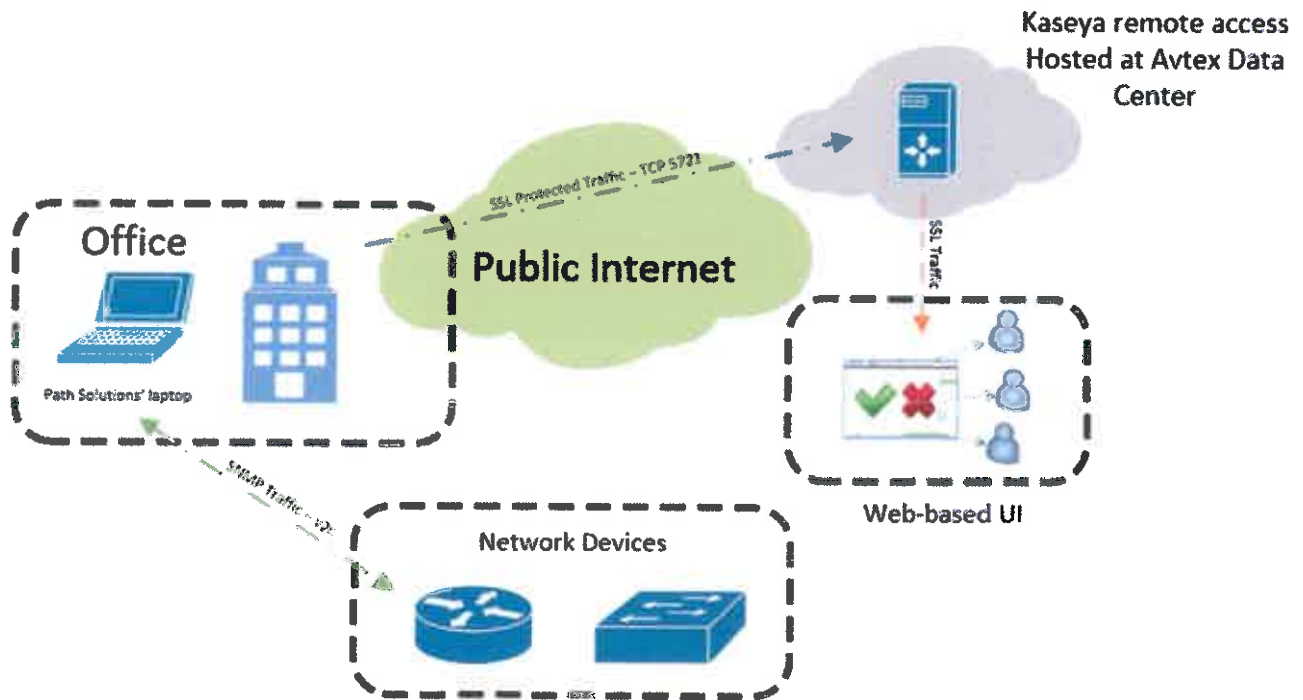
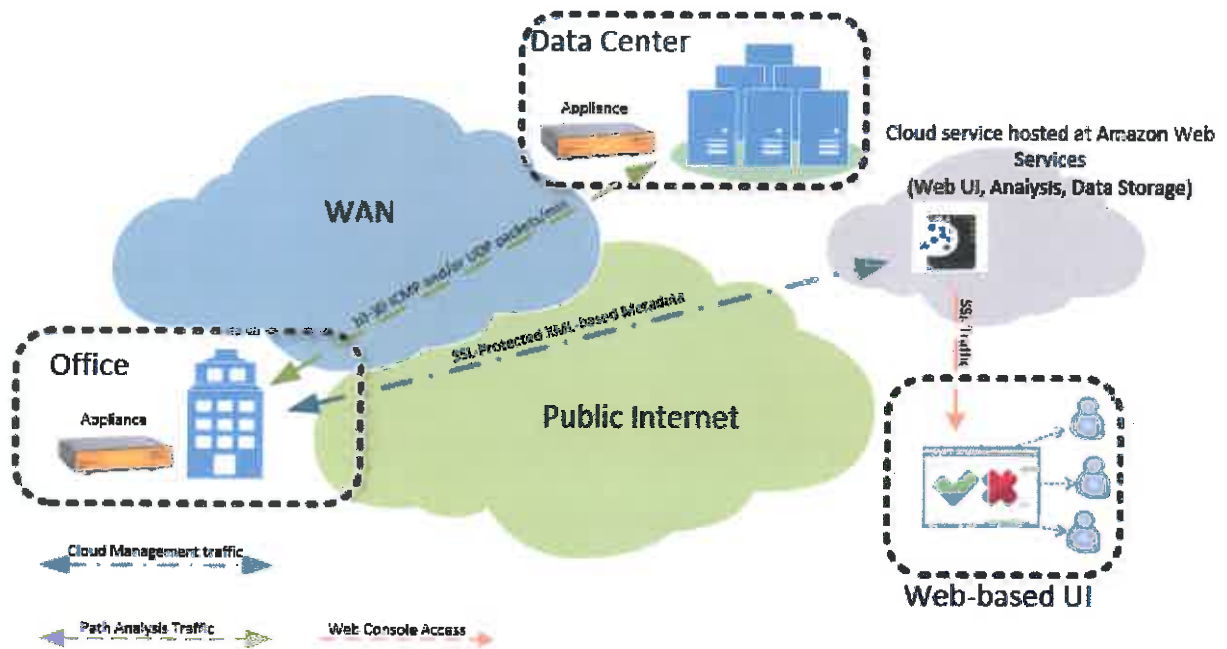
- Total and utilized capacity
- Data loss
- Voice loss
- Latency
- Data Jitter
- Voice Jitter
- ICMP response time
- MOS

Continuous monitoring is performed for each path that is created using ICMP and UDP packets which can simulate different types of traffic. If a threshold is reached for any of the metrics measured, diagnostics are automatically ran on the path to determine where the issue may be occurring.

If necessary, Avtex may monitor the type of traffic traversing WAN circuits. With a port mirror configured and connected to the appliance, Avtex will be able to break down traffic on your network. The function works similar to Netflow, which can identify data down to which protocol is used. This data can be categorized into different groups (i.e. "streaming media", or "social networking"). The information is then graphed, which will help identify and visualize the amount of bandwidth that each class is using.



**Appliance and Laptop Communication:**





## Client Device Installation and Configuration Requirements

- Provide a resource that has appropriate access to the network equipment for the purpose of review and documentation. Outbound access on TCP 443, 5721 and 80 are required. Please advise if a web proxy is used.
- Ensure the following ports and protocols are allowed along the entire network path which is to be monitored:
  - ICMP echo
  - ICMP echo reply
  - ICMP TTL expired
  - ICMP destination unreachable - port unreachable
  - ICMP destination unreachable - fragmentation needed and DF set
  - UDP ports 45056 through 49151 - default port range used by UDP traceroute and AppView Voice Tests
  - UDP port 3239 - default port opened at the target appliance for testing on dual-ended paths
- Provide SNMP community string from client for all devices to be monitored
- Identify switch port to be used for AppNeta and PathSolutions management interface
- Identify switch port to be used for FlowView (if requested)
  - Configure SPAN port for monitor interface
  - Alternatively, the AppNeta device can site in-line
- Install AppNeta M30 at client location. Connect management and monitor port to interfaces previously identified
  - If static IP addresses are required, the client will need to provide the IP address, subnet mask, gateway, DNS servers, NTP server, and web proxy.
- Install PathSolutions laptop at client location. Connect management port to interface previously identified
  - Optional: Customer may provide a VM with Kaseya agent for Avtex to access and install/run polling tools instead of using a laptop.
  - Minimum Requirements for VM are:
    - For networks with less than 5,000 total interfaces:
    - Pentium 800Mhz Processor or faster (Virtual server is fine)
    - 1 GB of free disk space
    - 1 GB of RAM for the service (2 GB RAM for the server)
    - 100 MBPS Network Interface Card

- Windows 2008, Windows 2012 (32bit or 64bit)
- Clear counters on all interfaces that are to be monitored

## Voice Readiness Assessment Services Overview

The following sections outline our services and deliverables for State of West Virginia:

### **Avtex Professional Services**

#### **Senior Network Engineer**

- Remote assessment kick-off meeting:
  - Discuss the required steps of the assessment
  - Discuss State of West Virginia requirements for the assessment
  - Discuss State of West Virginia concerns regarding the network in detail
- Review the current network design
- General network review using State of West Virginia provided diagrams
  - Determine expected voice paths and the devices that will be involved in the assessment
  - Review potential traffic congestion points
- QoS Configuration Deployment Review
- Configure paths in AppNeta
- Configure Voice Assessment in AppNeta
- Configure FlowView in AppNeta
- Configure devices to be monitored in PathSolutionsWAN utilization review
- Voice Device Inventory Discovery: This test will identify all devices on the network that are suitable for voice testing.
- Voice LAN and WAN Path Validation
- Examine the path of VoIP traffic from end to end. The statistics are produced for Mean Opinion Score, Jitter, Latency, and packet loss
- Confirm QoS markings are honored end to end and all ports are set to full duplex
- Review current and expected traffic patterns and the estimated load it will place on the network

#### **Project Manager**

- Schedule and host Internal kickoff call
- Schedule and host External kickoff call
- Provide documentation on VoIP network requirements and assessment pre-requisites
- Schedule and host ongoing status meetings (minimum weekly is typical)

- Track project status and loop in current SMEs as appropriate
- Orchestrate shipping logistics of network devices
- Create and work off project plan
- Manage change, risks, hours, communications, and budget
- Drive and track any project escalations to resolution

#### **Deliverables**

Avtex will supply State of West Virginia with reports pertaining to circuit utilization, service quality, data performance, voice performance, and voice testing results. Reports can be provided hourly, daily, weekly and monthly.

#### **Out of Scope Items**

- Redesign of the network. This can be provided under a separate agreement.
- Troubleshoot network related issues. This can be provided under a separate agreement.
- Network device configuration. This can be provided under a separate agreement.
- Network equipment, software, cabling, or services to upgrade the network.

#### **Appliances**

This assessment includes a maximum time of 2 weeks per-site to perform from the date the appliances are received by the customer. After completion of the VRA, the customer will be required to return all Avtex provided hardware within 10 business days. If an extension is needed, Avtex approval will be required. Violation of this agreement will result in a charge of \$600/month per device with no included services.

## Project Implementation

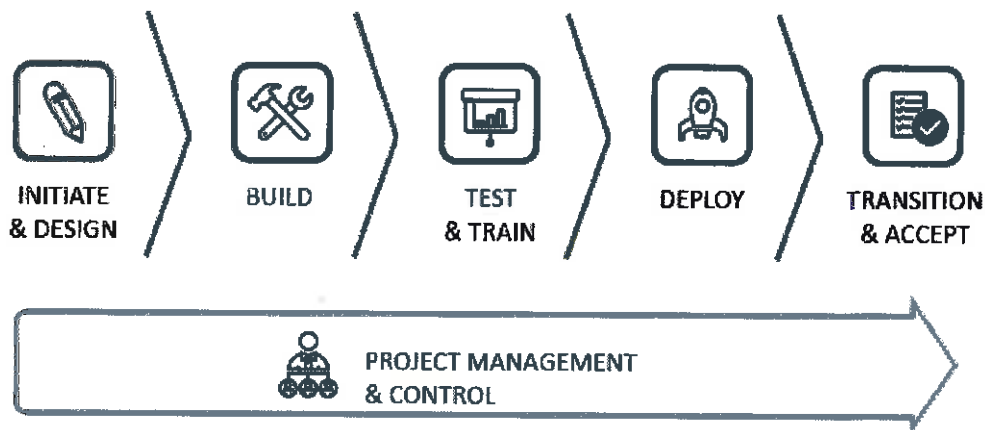
After receipt of a signed contract, Avtex will assign a Project Manager to State of West Virginia. The Project Manager will be State of West Virginia's single point of contact throughout the implementation process.

### Avtex Project Process

The Avtex Project Process and Management approach works hand in hand with the customer's project team. The Avtex Project Manager is the main point of contact on the Avtex Project Team once the project is initiated. Our project managers are trained in various industry standard project management processes, including Waterfall and Agile Scrum, and most carry project management credentials in those methodologies.

Our Project Manager will bring implementation knowledge and experience for deploying similar projects and help your project team understand and plan for the tasks they will need to complete to hit target timelines. A regular cadence of planning and status meetings will be scheduled with the core project team, and regular additional project communication will be provided through status and budget reporting and dedicated SharePoint project portals for collaboration.

The Avtex Standard Project Process methodology follows a five (5) Phase process, with Project Management throughout the project.



### Initiate & Design

Avtex will assign the project team upon signature and the project team will work with the sales team to transition the project into delivery and kick-off the project with the client. Any design workshops, final design documentation required and infrastructure readiness will occur during this phase.

### Build

Avtex engineers, developers, and application consultants will complete installation, configuration and custom development work included in the scope of the project. Base functionality and unit testing is completed by resources as part of their efforts during the solution build out.

## Test & Train

The test and train phase requires resources other than the original engineer, developer and or consultant to test the solution to verify it meets agreed upon designs, and most importantly requires the customer to test the solution and confirm the required functionality and business cases are tested to ensure it meets designs and business needs. Adjustments will be made based on test results if they did not meet the design requirements. Occasionally new requirements result from business test cases that may require change requests, which will be handled through the project change management process.

Avtex trainers will train your key resources, i.e. SMEs, Team Leads, Trainers, Administrators during this phase, most often prior to UAT to ensure your UAT testers are able to effectively complete test scripts. Customers' trainers then complete preparations for their end user training in the Deploy Phase.

## Deploy

The Deploy Phase is putting the new solution into a production environment, or the final environment included in the solution and scope.

## Transition & Accept

The Transition & Accept phase handles transitioning the environment from the project team to the appropriate support organization, be that an Avtex Support team or the customer's support organization. Most projects include a short Post Implementation Support / Hyper Care period of about two weeks, unless otherwise agreed to, to handle post production questions and punch list items to ensure that smooth transition. This phase also includes any additional environment refreshes, switch-overs and any training that requires production data to complete.

## Project Management and Control

Project Management encompasses the project and occurs from the beginning of the project until the project is accepted and closed.

## Avtex Professional Services

### CX Assessment

As described in the Executive Summary

### Business Analysis

The Business Analyst is responsible for working with the customer to review business goals, objectives, and customer journey through the Contact Center and work with the Avtex project team to document and help in the successful delivery of those goals and objectives. The Business Analyst role is occasionally shared in some areas, and some technical design sessions may be led by a skilled developer working in concert with a Business Analyst and Project Manager were appropriate. The Business Analyst will also be assigned to assist with kicking off the User Acceptance Testing phase and support onsite project cutovers and first day of service and projects require.

- Complete CIC Configuration Design (IA Playbook) Meetings and Documentation
  - Roles, Workgroups, Users, Skills, Recordings

- Complete IVR & Call Flow Design Meetings and Documentation
  - Map out call routing in Visio
  - If included: Email, chat, callbacks, and utilization routing for media types
- Complete Review of Out of the Box Reports
- Complete and Document Reporting Requirements
- Additional Tasks as Assigned
  - User Acceptance Testing (UAT) Kick-off & Guidance, if not provided by a Training Consultant
  - Participate in UAT status and issue tracking calls
  - Support for Go-live

### Project Management

- ▣ Project kickoff and project planning session
- Business Assessment
- ▣ Application Assessment
- Reporting Assessment
- Solution Design Document and Project Plan
- ▣ Project timeline
- Change management plan
- ▣ Communication plan
- Project acceptance criteria
- ▣ Risk Assessment
- ▣ Assist with Test Plan creation
- Test with Client sponsors
- Training plan
- ▣ Weekly status reports
- ▣ Provide Cutover support
- Provide First Day of Service support
- ▣ Manage Post-Cutover issue resolution
- ▣ Transition plan
- Quality Assessment Review



## System Engineering

- Configure applicable PureConnect server applications (Excludes “provisioning” tasks that will be performed by Genesys)
- Configure data and/or telephony integration to applicable State of West Virginia infrastructure or third-party systems and devices.
- Configure PureConnect Administrator items (e.g. Users, Roles, Permissions, Phone Management) based on information that will be provided by State of West Virginia.
- 
- Skype for Business Integration
  - Configure SIP connectivity to the Microsoft Lync Server or Skype for Business platform
  - Configure PureConnect stations for connectivity to Skype for Business voice endpoints
  - Install the PureConnect Presence Integration service on the Skype for Business Trusted Application server(s)
  - Configure status mapping as per the business requirements gathered during design meetings
- Interaction Recorder
  - Configure Recording Initiation, Retention, and Security policies according to customer requirements.
- Perform base functionality testing
- Provide instruction for installation of client applications – State of West Virginia is responsible for installations and may optionally use a tool such as SCCM to automate the deployment of client applications. If desired, subsequent updates can be managed automatically by PureConnect’s Interaction Update service.
- Provide support and configuration as needed during Quality Assurance and User Acceptance Testing
- Provide Cutover Support
- Provide First Day of Service and Second Day of Service Support
- Provide additional post-cutover issue resolution

## Application Development

- Design and configure ACD routing
- Configure Interaction Attendant inbound call routing
- Perform Application Development Unit Testing
- Turn over system for QA and User Acceptance Testing
- Provide Cutover Support
- Provide First Day of Service and Second Day of Service Support

- Provide additional post-cutover issue resolution

## Training

- Training will be provided onsite unless where otherwise mutually agreed.
- Avtex Trainer will meet with State of West Virginia team to determine specific training requirements, schedule, and agenda.
- Train the Trainer is proposed to prepare State of West Virginia to deliver remaining and ongoing end-user training.
- The Scope of Work includes the following Training classes:
  - Base Training Engagement Package (0000-00)
    - The Base Training Engagement Package is required for all Training engagements. Each individual class is on top of the Base Training Engagement Package which includes the following:
      - Training Kick-off Meetings (Avtex Internal and Customer Facing)
      - Design Review
      - Build Training Plan
      - Scheduling
      - Pertinent Status/Project Team/Review Meetings (Avtex Internal and Customer)
    - One of the following depending on which agent client application is selected:
      - Interaction Desktop: Contact Center Agent (1001-10)
        - Learn the basics and advanced features of Interaction Desktop for managing personal interactions, voicemail, faxing as well as multi-media ACD interactions
      - Interaction Connect: Contact Center Agents (1006-19)
        - Learn the basics and advanced features of Interaction Connect (web client) for managing personal interactions, voicemail, faxing as well as multi-media ACD interactions
    - Interaction Desktop: Business User – TTT (1002-19)
      - Learn the basics and advanced features of Interaction Desktop for managing personal interactions, voicemail, faxing.
    - ICBM Supervisor (1020-19)
      - Learn the basics and advanced features of ICBM for creating personal views of live queue and user statistics, create alerts based on statistical data thresholds and live monitor interactions.
    - ICBM Reporter (1022-19)

- Learn the features of ICBM Interaction Reporter Reports for creating reports based on pre-defined parameter selections. Learn how to export and print reports and manage report filters.
- ICBM Recorder (1024-19)
  - Learn the features of ICBM for accessing, bookmarking, tagging, and exporting recordings.
- ICBM Quality Manager (1026-19)
  - Learn the features of ICBM Quality Manager and Recorder to create questionnaires and score recordings.
- Scheduled Reports (1080-10)
  - Learn to use the Schedule Reports client to automate the delivery of ICBM Reporter and Report Assistant reports via email, file location and/or printer.
- Interaction Administrator Standard (1040-20)
  - Learn to make common adds/moves/changes under the People Container
- ICBM Dialer Views for Supervisor Monitoring (1032-20)
- ICBM Dialer Management for Administration (1033-20)
- ▣ Systems go-live support
- Additional Information <http://www.avtex.com/training/>

### Quality Assurance

Avtex assigns a second resource that did not complete the initial server configuration and development to complete a secondary set of Avtex testing in key areas prior to turning the solution over to customers for User Acceptance Testing. This role can be filled by a single resource or a limited set of multiple resources. The QA resources are business analysts, training consultants, project managers or other engineers and developers as the project scope and timeline demands.

- ▣ Complete assigned QA Base Functionality Tests for in scope server configuration.
- Complete assigned QA Tests on in scope call flows.
- ▣ Complete assigned QA Tests on in scope custom development.
- Report any issues found during assigned QA Tests for Support & Stabilization updates.

### Documentation

Avtex will provide a set of standard documentation to State of West Virginia, including the following items:

- ⦿ Architecture diagram that illustrates the final system configuration, including locations, connectivity, devices, and quantities
- ⦿ Auto-Attendant and/or IVR call flow diagrams based on the standard Avtex Visio design template
- Description of other customizations where applicable

The PureConnect product documentation library is available in electronic format and may be accessed via the online Resource Center at [https://help.genesys.com/cic/desktop/welcome\\_page.html](https://help.genesys.com/cic/desktop/welcome_page.html). The documentation package may also be installed on a user's desktop for reference when an internet connection is not available.

## Implementation Assumptions

Except where otherwise indicated in this Statement of Work, the Avtex Professional Services estimate for this project is based on the following assumptions:

- A single cutover event, during which all relevant locations, departments, and groups will be prepared to “go live” on the system. Each scheduled event requires additional cutover and post-cutover support.
- Onsite “go live” support for cutover and go live support is assumed to be for a single location with two resources.
- Onsite training is assumed to be for a single location.
- A single project phase, during which the entire proposed solution will be designed, developed, tested and delivered. Multiple design, build, testing and deployment phases require re-engagement of resources to repeat the applicable sequence of events in the Avtex Project Process and will require evaluation of impact from a budget, resource and timeline perspective.
- Avtex support for up to three (3) weeks of Customer User Acceptance Testing (UAT).
- The majority of Avtex services will be performed remotely. Travel expenses are not included in the project cost estimate.
- The change management process will be used to address any requests that were not explicitly included in the Statement of Work.

## State of West Virginia Responsibilities

### ■ Network infrastructure

- Switching, routing, firewall devices and configuration
- Voice and data circuits
- Quality of Service Requirements
  - An effective Quality of Service policy is based on the guidelines listed below. Please consult the PureConnect Quality of Service Technical Reference document for additional details: [https://help.genesys.com/cic/mergedprojects/wh\\_tr/desktop/pdfs/qos\\_tr.pdf](https://help.genesys.com/cic/mergedprojects/wh_tr/desktop/pdfs/qos_tr.pdf). Avtex can provide a Voice Readiness Assessment if State of West Virginia is uncertain of network readiness or has performance concerns.
  - Summary:
    - Full Duplex is enabled on all voice network devices.
    - Latency in one direction is less than 150ms (for both SIP & RTP)
    - Jitter is less than 30 milliseconds.

- Mean Opinion Score (MOS value) for the G.711 audio codec is 4.1 or greater and for the G.729 audio codec is 3.9 or greater.
    - RTP packets include the proper markings for service priority queuing following the DSCP model
    - Network segments do not exceed a packet loss rate of one per cent (1%).
    - Network bandwidth is sufficient to allow for approximately 84kb/s per call using the G.711 audio codec and 21kb/s per call using the G.729 audio codec.
    - VLAN settings are set in accordance with the PureConnect Quality of Service Technical Reference.
    - VoIP compliant software and firmware for all VoIP network components, to support standard techniques for delivering VoIP QoS. Techniques including but not limited to the leveraging of 802.1p, 802.1q and packet queuing by Differentiated Services tags at network congestion points.
  - Other Requirements
    - DHCP services with Opt. 160 or other enabled for IP phone provisioning
    - DNS services – The Avtex Engineer will provide required parameters
    - Static IP addresses for all PureConnect servers
    - LAN switch hardware that provides IEEE 802.3af Power over Ethernet (PoE) for IP desktop phones or provide power brick A/C adapters.
  - Port Maps and Data Flow Diagrams
    - The port maps and data flow diagrams illustrate the default ports numbers and protocols used for network connections between workstations, devices, and PureConnect servers. Please consult the following document:  
<http://docs.avtex.com/pureconnect-pre-install/PureConnect Port Maps and Data Flow Diagrams.pdf>
- **Data Infrastructure:**
  - Active Directory services and applicable accounts
  - Supported mail platform
    - Please consult the following page for supported mail platforms and versions:  
<http://testlab.genesys.com/ProductsPage.aspx?ProductType=12>
    - Please refer to the following information on Microsoft Exchange Web Services connectivity: <http://docs.avtex.com/pureconnect-pre-install/PureConnect Exchange Web Services Requirements.pdf>
  - Supported mail client: <http://testlab.genesys.com/ProductsPage.aspx?ProductType=30>
  - Supported backup, anti-virus, and security procedures (for servers located on-premise)





AES encryption protect your systems from login to logout. All information is encrypted before it is transferred. In addition to the ease and security of the product, Kaseya keeps detailed information about who, what and when of a session. An access-detailed, text-based account of every action that occurred during the remote-control session is available to Avtex management.

### Out of Scope

- Installation and configuration of user workstations
- Installation and configuration of database server software and hardware
- Installation and configuration of mail server software and hardware
- Network Infrastructure - hardware, wiring and cabling

### Pricing

Quantity	Component	Unit Price	Extended Price
<i>Avtex Professional Services:</i>			
1	PureConnect Implementation Services		\$ [REDACTED]
<b>Total Avtex Professional Services:</b>			\$ [REDACTED]

Terms conditions of the solution support are found in the Customer Support Agreement CSA attachment "Avtex - State of West Virginia – Base Configuration Premier CSA(Final v1.2).pdf". The costs are provided in section 1 Term and Amount.

\*Please see pricing proposal for full cost breakdown



**Attachment SO-2 - State of WV – Carahsoft SOW (Legacy Cisco UC)**

Please find the attachment beginning on the following page.

# **PRESIDIO®**

Future. Built.

## **CARAHSOFT SOW TO THE STATE OF WEST VIRGINIA**

**MANAGED SERVICES CONTRACT**

**SELECT SERVICES**

**November 19, 2018**

## REVISION HISTORY

Revision	Revision Date	Name	Notes
1.0	11/19/2018	Andy Pagley	Initial Draft

**Notices:**

© 2013 Presidio. All Rights Reserved. This document and its contents are the confidential and proprietary intellectual property of PRESIDIO and may not be duplicated, redistributed or displayed to any third party without the express written consent of PRESIDIO.

Other product and company names mentioned herein may be the trademarks of their respective owners.

## TABLE OF CONTENTS

1. SERVICE SUMMARY .....	4
2. SERVICE DELIVERY CENTER.....	4
3. MONITORING.....	9
4. CLIENT PORTAL.....	12
5. STANDARD REPORTS.....	12
6. CHANGE MANAGEMENT.....	12
7. PROBLEM MANAGEMENT.....	15
8. PATCH MANAGEMENT.....	15
9. CARRIER MANAGEMENT.....	16
10. DISPATCH SERVICES.....	16
11. VENDOR MANAGEMENT.....	16
12. SERVICE DELIVERY MANAGEMENT.....	17
13. UNIFIED COMMUNICATION MANAGEMENT SERVICES.....	18
14. SERVICE TRANSITION MANAGEMENT.....	24
15. CLIENT RESPONSIBILITIES.....	26
MASTER MANAGED SERVICES AGREEMENT.....	29
GENERAL DEFINITIONS.....	33

## 1. SERVICE SUMMARY

This Managed Services Contract is designed to provide a thorough understanding of Managed Services activities and deliverables. The main body of this proposal outlines the service deliverables for Presidio Managed Services. The Service Appendices provide details on Client-selected services, including any custom offerings.

Select Service is built on the Presidio Managed Services Delivery Framework, which combines industry-leading technologies, proven processes and highly certified personnel. The service includes all of the integrated Service Elements, identified in Exhibit 1. Presidio also provides the option of adding Custom Elements to supplement the Select offering. These elements are scoped separately.

Service Elements drive the level of service for each of the Presidio Managed Services offerings and are defined in the sections that follow. Details for the Legacy Cisco Unified Communications environment are included in Section 13 - Unified Communication Management Services. Your Managed Services Support Solution will include the following:

**Exhibit 1. Select Service**

Select Service
<ul style="list-style-type: none"> <li>• Service Delivery Center</li> <li>• 24x7x365 Monitoring</li> <li>• Client Portal</li> <li>• Standard Reports</li> <li>• Change Management                             <ul style="list-style-type: none"> <li>• MACD (Move, Add, Change, Delete)</li> </ul> </li> <li>• Problem Management</li> <li>• Patch Management</li> <li>• Dispatch Services</li> <li>• Vendor Management</li> <li>• Carrier Case Management</li> </ul>

## 2. SERVICE DELIVERY CENTER

The Service Delivery Center (SDC) is the central point-of-contact to Presidio Managed Services for daily support activity and is also generally referred to as the Network Operations Center (NOC). It is the main point of contact for reporting incidents (disruptions or potential disruptions in service availability and/or quality) and for Clients making service requests (routine requests for services). Presidio's Service Delivery Center team is staffed 24 hours a day, 365 days a year in three primary locations including Orlando, FL, Lewisville, TX and Hauppauge, NY.

The SDC will deliver Tier 1 through Tier 3 technical support using Presidio's Information Technology Infrastructure Library (ITIL)-based processes. Presidio defines technical support levels as follows:

### Tier 1: Technician Support

The Service Delivery Technician (Tier 1) is responsible for effective Client service support using workflow and incident management tools. Tier 1 technicians follow Presidio's standard ITIL-based processes, as well as specific Client processes as defined by Service Delivery



Management. Technicians utilize our incident management system to manage the incident queue for resolution or follow up, interface with Tier 2 engineering for advanced engineering support as needed and maintain Client communication during escalations. Initial support for basic Client issues is supported at Tier 1.

## **Tier 2: Engineering Support**

The Service Delivery Engineer (Tier 2) is responsible for effective Client service using advanced engineering skills. Tier 2 engineers use defined ITIL-based processes for effective Incident and Change Management. In addition, the engineer interfaces with vendor support engineering or Presidio Professional Services to provide timely resolution.

## **Tier 3: Advanced Technical Support**

Tier 3 is the highest level of support in a three-tiered technical support model responsible for handling the most difficult or advanced incidents and overseeing problem management for Clients.

The Client may communicate incidents to the Service Delivery Center using the following methods (in addition to auto-generated incidents):

- Telephone (P1 Incidents must be opened via a call into the SDC)
- Opening a ticket on the Client Portal (defaults to a Priority 4 incident)
- Email (defaults to a Priority 4 incident)

Client personnel contacting the Presidio SDC must be authorized to do so as defined in the Run Book. The Run Book is a set of defined procedures developed during the Service Transition Management process for maintaining the everyday operation of the Client environment. The SDC cannot respond to support requests from non-authorized personnel and will not engage with the Client through indirect methods for incident notification. Client personnel authorized to contact the SDC must be qualified to interact on a technical basis at a level required to support efforts by Managed Services.

Once an incident has been opened, an email notification will be sent to the caller and all contacts subscribed to receive notifications that match the conditions of the incident.

## **2.1. Incident Management**

Presidio will perform the following during the management of incidents identified through monitoring of the environment or by direct Client notification:

- Event identification, logging and management
- Alert Review to assess if it is an actual alert or system anomaly
- Clear system anomalies and close the incident
- Group related relevant events into a single incident to reduce notifications (parent/child incident correlation)
- Prioritize incidents based on impact and urgency
- Notify Client of the incident within the notification service level
- Restore Service

- Take complete ownership of service restoration or remotely assist onsite personnel as needed to facilitate service restoration.
- Remotely facilitate hardware replacement and software updates determined to be required by Presidio.
- Remotely apply patches to remediate an incident or problem identified by Presidio and handled as a normal Change, if required.
- Interact with third-party support providers (e.g., Cisco Technical Assistance Center [TAC]). This requires a Client-signed Letter of Agency (LOA) processed during the Service Transition Management phase. Carrier Case Management is only included in the Select tier of services.

## 2.1.1. Incident Prioritization Classification and Prioritization

Incidents need proper classification and prioritization. Classification and prioritization are described as follows:

- **Classification** - Determined by choosing the correct service offering, category and subcategory as it pertains to the incident.
- **Prioritization** - Assigning impact and urgency calculates the appropriate priority.

## 2.1.2. Determining Classification and Prioritization

Based on the information placed in the incident during its creation, the incident is reviewed and the correct classification, urgency and impact are selected.

Priority is based on the combined impact and Urgency assignments, reflecting the level of adverse impact to the Client systems.

## 2.1.3. Impact Definition

Impact refers to the business impact of the system impacted. The initial impact is pre-defined from the alerting tool based on the type of alarm received or Client request.

There are three categories of impact:

1. **High:** Incident affecting an entire site or multiple sites.
2. **Medium:** Incident affecting multiple users.
3. **Low:** Incident affecting one or few users.

## 2.1.4. Urgency Definition

Urgency is the extent to which the incident's resolution can bear delay. The initial urgency is pre-defined from the alerting tool based on the type of alarm received or Client request.

Presidio Incident and Problem urgency and corresponding priority levels are defined as follows:

1. **High:** Full service outage of a critical system or VIP is affected, requires urgent response.
2. **Medium:** Client's ability to function is partially impacted, requires the SDC to respond as soon as possible.
3. **Low:** No impact on the Client's ability to function; is more informational in nature and a response is not critical.

Presidio retains the case priority even if there is a reduced severity of impact until incident resolution. The case may be left open for a prescribed period while operational stability is being assessed.

The incident shall be closed by Presidio or Client upon validation of issue remediation and the CI's return to operational stability.

Complete detail for open and closed tickets resides on the Client Portal and is used to support incident management and problem management processes.

**2.1.5. Priorities for Tools Generated Incidents**

Presidio monitoring tools apply the following priorities for auto-generated incidents, generally indicating the condition shown (the actual condition is determined by a number of factors as defined in the thresholds).

**Exhibit 4. Incident Priorities**

		IMPACT		
		High	Medium	Low
URGENCY	High	P1	P2	P3
	Medium	P2	P3	P4
	Low	P3	P4	P4

**2.1.6. Incident Escalation**

Incidents are escalated according to a defined process. At any point in the incident management process, the Client may request escalation via the Presidio SDC Supervisor to address concerns about the handling of the incident. If service restoration requires activities by a third-party provider, Presidio initiates and manages the process.

For a High Severity (P1 or P2), Clients are asked to call Presidio Managed Services. The SDC will initiate a live handoff to an engineer. If further escalation of an existing ticket or after business hours escalation is required, the Client should request to speak to the SDC Supervisor or Manager. The Client is provided with a list of five escalation levels in case needed, including the SDC Supervisor at Level 1.

Upon resolution, the Client is notified the incident is resolved and provided with the opportunity to verify services have been restored satisfactorily. Following incident resolution and Client notification, the incident is closed by Presidio. Reports regarding incident management are available on the Client Portal.

**2.2. Service Level Objectives**

Service Level Objectives (SLO) are specifically aligned to incident priorities and response times for service requests. Presidio categorizes each issue by priority reflecting the level of adverse impact to Client systems. Priority provides a reasonable and accurate reflection of the number and complexity and business impact of systems affected. Clients have the ability to set or change the priority level of an incident at any time, based on the impact to their specific business. Exhibit 5 describes the priority levels assigned. Exhibit 6 describes the Service Level Parameters.

Exhibit 5. Priority Levels

Level	Description
● P1 / Critical	Systems at one or many Client sites are completely unavailable. Affected systems cause significant business impact.
● P2 / High	Systems at one or many Client sites are partially unavailable. Affected systems cause some business impact.
● P3 / Medium	Operational performance of Client sites is impaired while most business operations remain functional.
● P4 / Low	Client is requesting information or a logical change that is covered under their service agreement.

Exhibit 6. Service Level Objectives

Service Level Objective	P1 ●	P2 ●	P3 ●	P4 ●
<b>Acknowledgement Response Time(*)</b> The amount of elapsed time between Client initiation of an issue, or the time Presidio Managed Services (MS) detects a fault, and the time Presidio MS creates an incident report and notifies Client via e-mail that an incident has been created.	15 minutes >95%	30 minutes >90%	4 hours >80%	8 hours NA
<b>First Access Response Time</b> The amount of elapsed time between Client initiation of an issue, or the time Presidio MS detects a fault, and the time an assigned Presidio MS technician connects to the system, or otherwise contacts Client, and begins remote diagnosis and troubleshooting.	30 minutes >95%	1 hour >90%	8 hours >80%	3 days NA
<b>MACD Request Completion Time</b> The amount of elapsed time between Client request of a User Change and the completion of the change measured in US business hours.	8 business hours NA			

*\*Does not apply to ticket integrated customers, nor contracts with no client contacts subscribed to notifications.*

**Acknowledgement Response Time** achievement percentage is calculated as follows:  
 Total incidents acknowledged within Service Level Target / Total Incidents (for each priority).

**First Access Response Time** achievement percentage is calculated as follows:



Total Incidents within First Access Response Time Service Level Target / Total Incidents (for each priority).

**MACD Request Completion Time** is the amount of elapsed time between Client request of a User Change and the completion of the change measured in US business hours.

### 3. MONITORING

Presidio's monitoring is implemented through an extensive set of integrated tools that work in unison to manage a customer's environment. These tools provide device health monitoring and reporting, enable event consolidation, provide an interface for remote diagnostics and exchange information with the IT Service Management (ITSM) platform to support advanced capabilities such as automated incident creation.

The Presidio Data Collection Agent (DCA) comes pre-configured with all of the Presidio monitoring tools. Once installed, Presidio's experienced team configures the customer DCA to communicate back to Presidio's primary collection point where all of the customer data is collected and automatically analyzed.

Inside of Presidio's ITIL compliant Service Desk system, every component managed is defined as a configuration item in the Configuration Management Database (CMDB) and all events and data are tracked back to the individual Configuration Items.

Presidio will monitor the health and performance via multiple avenues including SNMP polling at set intervals, SNMP traps for critical alerts, and when viable, other methods as determined by the technology being monitored.

#### Service Details

- Tool Setup and Deployment
- User Orientation
- 24X7 Collection of Monitored Component Data
- Technical Support on Tool and Collection Process
- Real-time Threshold Monitoring and Exception Notification Event management

Presidio provides monitoring and instrumentation problem resolution services with best-practice processes supported by a state-of-the-art toolset. The service starts with a component, and then performs polling for events. Alarms are consolidated and efficiency is optimized root cause analysis. Presidio provides full console services and incident workflow. The components of the service include:

- Surveillance
  - The instrumentation mechanism is present and active for devices that are monitored and filtering of conditions is established to provide preventive, early warning of out-of-normal conditions.
- Detection
  - Out-of-normal conditions are identified by the surveillance mechanism and conditions are forwarded to collection engines for automated analysis.

- Consolidation
  - The condition is compared to other active conditions to establish relationships and the condition is identified from many as actual, or most probable, common cause of all related conditions and an alert is forwarded to the ITSM system.
- Isolation
  - The operator validates the isolated incident using automated alert data, available documentation, skill and judgment. The operator then identifies the absence or presence of a known error condition.
- Respond and Inform
  - The incident and resolution data are reviewed and the instrumentation problem management process begins. The problem management team identifies appropriate systemic action and advises surveillance if filtering requires an adjustment.
- Learn
  - The incident and resolution information are reviewed and the instrumentation problem management process begins. The problem management team identifies appropriate systemic action and advises surveillance if the filtering requires adjustment.

## **Performance Management**

Performance planning includes information collection, forecasting, analysis, decision-making, and decision support. Performance planning is a strategic part of capacity management. Through capacity planning, future requirements are forecasted, and plans are prepared to ensure that resource capacity will be available when needed. Presidio's Monitoring solutions will detect conditions as capacity approaches predetermined thresholds, alert operations staff to these conditions via the operations console and initiate escalation and incident investigation automatically.

## **Monitoring Framework**

This section describes the design of the monitoring solution including the various components of the solution and the infrastructure to support those components.

## **Presidio Data Centers**

Presidio's Managed Services data center space includes two separate facilities. Each facility features dual home connectivity to two network carriers and a data center infrastructure consisting of independent compute, storage, security and network infrastructure. Each infrastructure component has multiple levels of redundancy to avoid a service outage with a single failure of a component.

## **Presidio DCA**

The monitoring framework requires installation of the Presidio Data Collection Appliance (DCA) on the Client network. Each DCA contains a complete copy of Presidio monitoring tools, including the core monitoring framework software and a local collection database.



The DCA is installed on the Client premises on a single subnet configured with Secure Socket Layer (SSL) tunnel to the Presidio monitoring framework. It is recommended that the DCA be installed within the Client data center at the network core. Additional Presidio appliances may be required, depending on the services the Client purchased and the number, type and location of monitored devices and systems.

## **Presidio Monitoring Solution(s)**

The Presidio monitoring Solution provides continuous monitoring of the health and availability of heterogeneous systems and networks. The service provides an extensive range of servers, voice applications, routers and wireless access points for monitoring. Certain server and application settings can also be changed to provide as much information that is available from SNMP and other native system or application utilities that can alert support teams when failures or events occur. Powerful event management capabilities correlate information and pinpoint the root cause of a problem. The service uses the following techniques to find infrastructure problems:

*Mapping* – The Presidio monitoring solutions walk the devices mapping the topology and stores in a model of the environment and all the devices

*Polling* - Actively reach out to every intelligent device every 5 minutes and ask it about its state of health

*Log reading* - Scanning the logs of every device for symptoms (where available and by request)

*Trap listening* - Filtering for those which are warning alarms sent by intelligent devices or other element management systems when they detect a problem (where available and by request)

*Consolidation* - Use expert rules to relate symptoms to the known topology, the devices known to be there and other symptoms recently obtained

## **Monitoring Notification and Escalation**

Incident notification informs Presidio and the Client that an Incident has been recorded.

### **Notification and Escalation**

- Automated, policy-based actions used to further customize event notifications
- Typically used to create unique notification timing based on business operational requirements (i.e. suppress memory alarms on certain servers if they are less than 30 minutes in duration during application peaks)
- Grouping policies can be based on customer, component type, description, etc.

### **Dynamic Modeling**

- Ability to give individual devices unique attributes which can be used for workflow or business unit needs (through the ITSM System)
- Identify critical devices which may need higher priority action or lower priority action (i.e. only needs escalation during prime time)
- Ability to set platform type used on operations, ticketing, workflow, troubleshooting

## Console Configurations

- Operations console configurations to alter views of accounts, devices, classes of events, events requiring action, etc.

## 4. CLIENT PORTAL

Presidio Managed Services includes a Web-based Management Portal. The Client Portal is remotely accessible by Clients and provides access to key information and services with respect to their managed services. Capability includes:

- Facilitating communication with the Presidio Service Desk, including request management.
- Viewing progress of service activities and the level of service being delivered.
- Viewing, creating and updating incident tickets and change requests.
- Viewing the status of CIs under contract.

Instructions to access and navigate the portal are provided in the remote training session during Service Transition.

## 5. STANDARD REPORTS

Presidio Managed Services come with a suite of standard reports. Presidio provides reports for managed CIs, including performance, availability, and inventory reports. The Client reports are accessible via the Client Portal. Report details are provided in the Service Appendices and are specific to each service contracted with Presidio.

## 6. CHANGE MANAGEMENT

Change Management ensures that changes to managed CIs are evaluated, coordinated and communicated to all impacted parties to minimize adverse impact on the Client Production environment.

Changes fall into three categories:

1. Standard Changes
2. Normal Changes
3. Emergency Changes

### 6.1. Standard Changes

A Standard Change is a change to a service or infrastructure for which the approach is pre-authorized by Change Management and that has an accepted and established procedure to provide a specific change requirement. Standard Changes do not require authorization from Technical, Customer or Change Management Approvers prior to implementation. Standard Changes have low to no risk and have no impact to the Production environment when performed.

Standard Changes should not have outages associated with them. There is no designated Lead Time for Standard Changes.

## 6.2. Normal Changes

A Normal Change is a change to a service or infrastructure planned and implemented within designated Lead Times. They follow the Normal Change process defined in the Change Management Policy. Normal Changes require authorization from the Technical Approver (designated by who is performing the implementation), Customer Approver and Change Manager Approver. Normal Changes require fully detailed implementation plans, back out plans, test plans and justification for performing the change.

The Lead Time for a Normal Change is 2 days (48 hours) from the time the Change Request is submitted until the time it can be implemented. This allows time for the Change Request to be reviewed and approved by all appropriate parties. It also allows time for Presidio Managed Services to properly assign resources to the Change Request.

If a Normal Change is required to be processed sooner than the 2 day lead time, it is flagged as Expedited. All requests for Expedited Normal Changes require a valid business related justification.

## 6.3. Emergency Changes

An Emergency Change is a change to a service or infrastructure that requires implementation as soon as possible due to a critical issue or service or infrastructure outage. Emergency Changes must be related to a Priority 1 (P1) or Priority 2 (P2) incident or request and may be logged after the P1 or P2 is resolved.

If an Emergency Change is logged after the resolution of a P1 or P2, it must be logged within 24 hours of the incident, Request, or Problem Resolution. Approval of an after the fact Emergency Change is a validation that the Emergency Change was required at the time it was performed. Emergency Changes are approved by the Emergency Change Advisory Board. There is no designated Lead Time for Emergency Changes.

## 6.4. Customer Maintenance Changes

A Customer Maintenance Change is a change to a service or infrastructure being performed directly by the customer and not Presidio that has the potential for alerts to be created. This type of Change Request is submitted for the purpose of suppressing monitoring on the CIs listed in the Change Request. These Change Requests are pre-approved and have no designated Lead Times. Customer Maintenance Change Requests are submitted either by the customer through the Presidio Customer Portal or by a member of the Service Delivery team for the customer.

## 6.5. Moves, Additions, Changes, Deletions (MACD)

Presidio offers Request Management for Managed CIs. The MACD process provides a model for managing and executing moves, additions, changes and deletions of hardware and software configuration items in the Client's environment. MACD service is defined within two categories: 1) Device-level changes and 2) User changes per contracted UC/Collaboration services. Definitions for each category are provided below with additional details for contracted services within the Service Appendices (if applicable).

## 6.5.1. Device Level Changes

Device-level changes are defined as configuration requests that typically impact multiple users based on the change, such as configuration. Presidio reviews the Contract for each device level request and determines if it falls outside of the scope as defined below:

1. Takes less than 2 hours of time to complete.
2. Does not require planning or design efforts.
3. Does not include any activity with a material operational impact. (i.e., the change cannot affect the normal physical operation of the device).
4. Is not an upgrade or feature addition.
5. Is not a project or part of a project.

For changes not covered by this agreement, Presidio provides a separate Contract from Professional Services. Device-level MACD support is only provided to equipment specified in the CEL.

A single device level change (MACD) is defined as one change per device; multiple changes to a single device are considered multiple MACDs regardless of whether it is made on the same service request. Presidio reserves the right to determine if the activity qualifies as a MACD activity. Device level MACD work does not apply to the Security Incident and Event Management Service which is defined in the separate contract.

For device-level changes, up to two changes per Ci per month are allowed. Changes are allotted monthly and must be used during the target month of service. Any change allocations remaining at the end of a service month are considered forfeited and do not roll to subsequent service months.

## 6.5.2. User Changes

A User Change is change for Collaboration services impacting any single user-based configuration, including moves, additions, changes or deletions; e.g., a request to add/delete a user profile. Details are provided in the MACD section of the Unified Communications Service Appendix.

The MACD option for the Users must be included in the covered device list for Presidio to perform user changes. The monthly allotment of MACDs is 5% of the managed Users per month and requires 100% of managed Users to be covered in agreement.

Presidio tracks the MACD tickets for the 3-month period and notifies the Client of trends. If the average MACD counts are exceeding the target limits, it may show evidence of an operational or training issue Presidio can address with the Client. If no operational issues exist and the MACD requests from the Client normally exceed the 5% limit for Users by more than 10%, Presidio will work with the customer to adjust the billing for user changes.



---

## 7. PROBLEM MANAGEMENT

Problem Management is a process that supports Incident Management. A problem is created for tracking activities that lead to identifying a root cause and resolution to the incident's underlying error.

Problem Management has two major categories:

1. Problem Identification
2. Problem Diagnosis

### 7.1. Problem Identification

The process starts with analyzing available data, identifying and recording problems, and classifying problems according to impact, urgency, and status.

### 7.2. Problem Diagnosis

The Problem is assessed to determine potential resolutions, which can include both temporary workarounds as well as permanent fixes. If a permanent fix is possible and cost-justifiable, a recommendation is made to the Client to correct the error by initiating a change via Change Management.

## 8. PATCH MANAGEMENT

Presidio provides Patch Management to customers who have contracted for Select Level services. There are two areas where patch management is applied: 1) Incident Remediation and 2) Vulnerability Management.

Patch management for incidents is applied when a vendor support case directs Presidio to apply a version consistent with a fix for a known error. Vulnerabilities are defined as a defect reported by a manufacturer that has the potential to affect the overall security of a client device or devices. These vulnerabilities are typically resolved with a software workaround or a patch issued by the manufacturer. Vulnerability patches are applied when there is a CVSS score that is a 9.0 or higher (Critical) as defined by the CVSS specifications listed at <https://www.first.org/cvss/specification-document>. Due to the unknown nature of the number of releases during any given year, Presidio will provide up to two vulnerability patches per device per year beginning on the Start of Service date of the contract. Additional vulnerability patches are not considered MACD activity and are billed as a separately negotiated addendum to the original SOW as applicable. Vulnerability patches are not proactively applied as part of any other service level.

Patch application to remediate incidents and mitigate known security vulnerabilities is a cooperative decision between the customer and Presidio. Patches are evaluated to ensure that current environmental stability is maintained. Patches to remediate an incident, vulnerability or problem identified by Presidio are handled as a Change Request.

As part of the Patch process, Presidio completes the following:

- For incident remediation patches, Presidio will review manufacturer field notices to determine impact and urgency to the Client system and existing software levels.
- For vulnerabilities classified as Critical per the Common Vulnerability Scoring System, CVSSv3, with a score of 9.0 – 10.0, Presidio will assess impacts to the Client and provide recommendations for remediation as applicable.
- For critical security vulnerabilities and incident remediation as defined above, Presidio remotely applies updates to affected CIs following the approved Change Management process.

If the Patch application necessitates a full upgrade in version level, requires a physical change to the existing hardware configuration or impacts dependent technologies, the effort is evaluated and may be subject to a separate project agreement. Covered equipment with software where the software maintenance has reached end of support or has lapsed, is not covered by the Patch Management element.

Client-requested patches for obtaining additional features or functions are out of scope of this section and must be handled as a separate agreement as referenced in “Device Level Changes” under the Change Management section of this document.

## 9. CARRIER MANAGEMENT

Presidio provides operational handling of carrier cases with third-party data and voice carriers for incident remediation. For most Clients under management by Presidio, there is a strong telecommunication vendor dependency. This service element enables Presidio to open tickets, for Clients who have provided a signed Letter of Agency (LOA) and the requisite circuit information, on behalf of the Client for any circuits directly connected to devices under Presidio management. Presidio manages the case throughout the incident resolution process.

## 10. DISPATCH SERVICES

Dispatch Services include scheduling qualified field technicians to replace failed equipment associated with an RMA only. Prior to the dispatch, Presidio coordinates with the Client to set proper expectations for timing of the replacement work. This service is either a 7x24x4 hour response or an 8x5xNext Business Day (NBD) response depending on the associated vendor maintenance attached to the failed component. The 4-hour response is provided to locations within 50 miles of a major metropolitan area.

International locations require a separate customer agreement for coverage, due to additional cost for coverage outside the United States.

Dispatch services not associated with an RMA replacement, which are customer requests, are billable engagements at a rate that is based upon the level of effort and location and will be reviewed with the client prior to engagement.

## 11. VENDOR MANAGEMENT

Presidio provides operational coordination of incident resolution involving products supported by third-party vendors as specified in the device list of this contract. Presidio support requires the Client to provide necessary account, contract and support information at the time of on-



boarding. Support information includes, but is not limited to, vendor support hours of operation, contact numbers, escalation contacts and any applicable SLAs.

For incidents involving third-party vendors, Presidio can only commit to SLA attainment consistent with the Client's service level agreements with the vendor, and is dependent on vendor resource availability. For incident management involving third-party vendors, Presidio will open tickets with the vendor and manage the case throughout the incident resolution process.

Note that dispatches by Presidio for vendor managed products/devices are not covered, including RMAs.

## 12. SERVICE DELIVERY MANAGEMENT

The assigned Service Delivery Manager (SDM) manages client satisfaction in the delivery of IT services and ensures program objectives are met. This person provides the client a primary point of contact within Presidio Managed Services, and provides operational leadership to the account team and client stakeholders. The SDM also ensures that the team understands the various technology services that Presidio delivers to the client.

The Service Delivery Manager provides management to multiple service delivery projects within the account and assumes responsibility for all aspects of account performance (technical, contractual and administrative). The following are standard SDM responsibilities:

- Maintain configuration management database, support documentation and any agreed upon special procedures
- Work with other Managed Services departments to maintain and improve customer SLO metrics
- Manage Customer satisfaction
- Meet agreed upon client deliverable schedules and manage expectations
- Manage appropriate internal and external resources to meet deadlines
- Facilitate customer meetings and teleconferences
- Maintain active communication internally and externally
- Deliver Quarterly Business Review (QBR) to the client (can be remote or on-site per client discretion)

### 13. UNIFIED COMMUNICATION MANAGEMENT SERVICES

The Presidio Unified Communications Management Service (UCMS) delivers support for a full range of collaboration services for Cisco unified collaboration, video, and third-party devices and applications. As a key offering within Presidio's Collaboration Services Portfolio, UCMS enables organizations to accelerate the adoption of advanced collaboration technologies by providing Managed Services through a team of highly certified engineers combined with state-of-the-art IT Service Management facilities.

#### UCMS Monitoring

UCMS includes standard device-level monitoring as well as advanced collaboration-specific monitoring.

#### UCMS – Cisco-Specific Monitoring

UCMS provides advanced monitoring of the Cisco UC solution. Exhibit B-1 lists the elements in our current toolset that we monitor. If a configured threshold for a CI is reached, the alert generates an incident for our SDC to resolve. Please note, as the Presidio Monitoring Framework evolves, this list may change.

Exhibit B-1. Monitored Toolset Element

Title	Description
Device Statistics	Gateways – Status, Reachability, Busy Call Attempts Phones – registered phone discrepancy Dial Plan – Route Group, Route List, Route Pattern, Trunk Status
Cisco Server Hardware	Disk, Fan, Power Supply, Temperature, Voltage Communications Manager Parameters Location Statistics – Bandwidth Utilization Media Resources – Hardware conferences, Media Termination Point (MTP), Music on Hold (MoH), Software Conferences, Transcoders, Video conferencing resources (/DSP based)
Communications Manager Server Alerts	Cisco Unified Call Manager (CUCM) Service Cisco Call Manager (CCM)Process CCM Agent Process Computer Telephony Integration (CTI) Manager Database SNMP TFTP
Unity Alerts	Critical Events Failover Service Failure Unity Port Max Unity Ports Not Registered
CallManager Alerts	CallManager Down Database Failure Heartbeat Issues CTI Manager Down Backup Service Failure SNMP Failure Syslog Failure
CCM Cluster Alerts	CDR/CMR Database Issues Gateway registration issues
CCM Server Alerts	Process issues CPU Utilization Disk Partition Utilization SQL/Database Issues

Title	Description
Cisco TelePresence Alerts	Gatekeeper Rejected Video Calls Video Bandwidth Exceeded Call Jitter Exceeded Call Packet Loss Exceeded Ethernet Down HDMI Cable Down HDMI Power Failure Latency Exceeded Packet Loss Exceeded Jitter Exceeded Peripheral Down SNMP Status Down
TFTP Alerts	TFTP Port/Network issues TFTP Service Failure

**Standard Reports**

Our UCMS Service includes a device-level reporting interface on our Presidio Client Portal that allows Standard reports to be viewed by the client. This is included in both the Essential and Select service levels. Standard Reports include four pre-configured reports and data are retained for 6 months.

In addition to the Client Portal reports, the following Collaboration Reports are provided as shown in Exhibit B-2.

**Exhibit B-2. Collaboration Reports**

Title	Description
Trunk Availability	Availability is based on connectivity from the PBX, registration status within the PBX and the member channel status. Not all factors are available for all trunks.
Trunk Utilization	Utilization is expressed in terms of the number of channels occupied. It is calculated by dividing the total duration of all processed calls across the IP or PSTN trunk(s) by the sampling period. For example: 12 x 5-minute calls (60 minutes) divide by 10-minute sampling period = 6 channels occupied, or 12 x 5-minute calls (60 minutes), divide by 1-hour sample period = 1 channel occupied. Calls originated outside the sampling period are also counted, but only for part of the call, which falls within the period.
Trunk Summary	Overall trunk availability Trunk availability Impacted trunks Trunk down time Trunk outages Trunk degraded time Trunk utilization Trunk busy hour Trunk busy hour by percentage Trunk call types
Call Failure Report	Calls attempted - A call attempt is a request from a phone/device to a PBX to initiate a call, whether that call is successful or not. Calls attempted = Calls completed + Calls rejected + other failures. Calls completed - A call completed is a call successfully processed by a PBX and terminated with a disconnect cause code that indicates graceful termination. Calls rejected - A rejected call is either a call attempt that is received but not processed by a PBX due to throttling when the PBX is under high load, or a call that failed due to resource limitations. Call failures - A failed call is a call attempt that is processed by a PBX but the call terminated abnormally with a disconnect cause code indicating that the call failed.

Title	Description
	<p>Call failure ratio - The call failure ratio is the percentage of processed calls that failed.</p> <p>Calls processed - A processed call is a call attempt that is processed by a PBX regardless whether the call completed successfully or not.</p> <p>Disconnect cause code - The disconnect cause code indicates why a call terminated abnormally. It may be attributed to either the origination or destination device.</p> <p>Report data - Calls with an origination time within the reporting period.</p>
Long Duration Calls Report	<p>Lists calls with duration exceeding the long duration threshold. This list of calls may help to identify device malfunctions, configuration errors or abuses of the system. Calls with a disconnection time within the reporting period are included in this report. Disconnection time is chosen to ensure these long calls will be captured in the report, as CDRs are only generated at the end of a call.</p>
Node Utilization Report	<p>High CPU Utilization            Node CPU Utilization            Call Load Balance            Phone Load Balance            Call Load Report            Busy hour statistics            Busy hour call attempts            Busy hour grade of service            Calls attempted            Calls rejected            Node call load            Phone Report            Phones configured and registered            Call types            Call statistics            Phone utilization            Phones inactive</p>
Route Pattern Availability	<p>Availability is derived from availability of trunk members belonging to the route pattern. Trunk availability is based on connectivity from the PBX, registration status within the PBX and the member channel status. Not all factors are available for all route patterns.</p> <p>Overall route pattern availability            Route pattern availability            impacted route patterns            Route pattern down time            Route pattern outages            Route pattern degraded time</p>

**UCMS Service Management**

In addition to the details in the main Contract, the following information specifically applies to the UCMS.

**System Backups**

Presidio performs back-up processes for Cisco ASR and ISR-based voice gateways, VG-series analog gateways, and other IOS-based voice CIs. This includes definition and execution of service restoration process for Managed CIs. The configuration back-ups are stored on the Monitoring Framework and available for use by Presidio in bringing current or replacement Managed CI's to service. Device-based backups are not performed for Monitored-Only CI's.

Presidio provides best practice recommendations to the Client in support of their Unified Communications applications backups. The Client is responsible for the configuration and storage of the backup jobs. Presidio monitors the backup services utilizing Cisco RTMT and alert/troubleshoot on service failures and related incidents.

Standard Services

Exhibit B-3 lists examples of the typical operations performed by our SDC for UCMS Clients.

**Exhibit B-3. SDC Typical Operations**

Device	Task
CER	DB Replication
CER	CER troubleshooting (phone tracking, ERL mapping)
CER	Integration with CUCM troubleshooting
CME	General Troubleshooting
CME	Integration with CUCM troubleshooting
CUC	Call handler troubleshooting
CUC	Subscriber troubleshooting
CUC	DB Replication
CUC	Failover troubleshooting
CUC	Integration with CUCM troubleshooting
CUCM	IP Phone troubleshooting
CUCM	Jabber Client troubleshooting
CUCM	Dial plan troubleshooting
CUCM	Resource troubleshooting (Xcode, MTP, Conf)
CUCM	DB Replication
CUCM	Backup and Disaster Recovery troubleshooting
CUCM	Debugging calls on gateway
CUCM	Call failure troubleshooting
CUCM	Troubleshooting Basic QoS (limited to managed components only)
CUE	Hardware replacements
CUE	Integration with CME troubleshooting
CUPS	Subscriber troubleshooting
CUPS	DB Replication
CUPS	Configuration issues
CUPS	Integration with CUCM troubleshooting
UCCX	CAD\Supervisor client troubleshooting
UCCX	Inbound calling troubleshooting
UCCX	Outbound campaign troubleshooting
UCCX	Call Recording Troubleshooting for supported 3 <sup>rd</sup> party vendors
UCCX	DB Replication
UCS	Upgrades - Firmware - In response to a bug or vulnerability
UCS	Hardware replacements - Drives
Video	Troubleshooting MSE8000 series including MCU\Telepresence server series blade
Video	Troubleshooting integration VCS to CUCM
Video	Troubleshooting Cisco media Experience MXE
Video	Cisco Telepresence Exchange integration with TMS
Video	Telepresence Healthpresence and Telepresence educator
Video	Media Services- Cisco Content Server and streaming, troubleshooting and monitoring streaming



Device	Task
Video	Jabber video client and integration troubleshooting
Video	B2B video troubleshooting

**Moves, Adds, Changes and Deletions (MACDs)**

With the Select Service level, Presidio offers both user changes and device-level changes. The MACD section within this Statement of work defines the scope of both change types, along with any associated volume limitations. In the following tables, examples of both user and device-level changes are provided.

**Exhibit B-4. Device-Level Change Examples**

Device	Task
CER	CER Configuration (ELIN, ERL, alerts, etc.)
CME	Configuration (dial-peers, hunt lists, other dial plan elements)
CUC	Bulk changes to subscribers
CUC	VM distribution lists
CUC	Auto attendant routing changes/menu structure changes
CUC	Uploading licenses
CUC	Auto attendant schedule changes
CUC	Call Handler Configuration
CUC	Scheduling, TOD routing
CUCM	Translation pattern adds/changes/deletes
CUCM	New DID assignments using number expansion
CUCM	New call blocking configurations on H323/SIP gateways
CUCM	Adding to or modifying existing call blocking configurations
CUCM	Codec manipulations
CUCM	Bulk changes to phones/users
CUCM	Building new hunt groups
CUCM	Music on Hold changes
CUCM	Uploading licenses
CUCM	Uploading new firmware
CUCM	Changes to gateways
CUCM	Generating simple CDR reports (few numbers, narrow date range)
CUCM	Creating/modifying Forced Authorization Codes/Client Matter Codes
CUCM	Translation pattern adds/changes/deletes
CUCM	Dial plan configuration
CUCM	License Activation
CUCM	Backup and Disaster Recovery Setup
CUCM	Minor updates/patching (elective, on request - no new features)
CUE	Configuration (auto attendant scripting, voicemail subscribers, etc.)
UCCX	Skill group assignments
UCCX	Team assignments
UCCX	Script modifications (holidays, hold music)



Device	Task
UCCX	Minor script changes (TOD Routing, trigger additions etc.)
UCS	Upgrades - Firmware - On request/coinciding with application patching
Voice GW	Dial-peer configuration
Voice GW	SIP Configuration changes (SIP Profiles, Translations, etc.)
Video	Adding/removing search rules in VCS – compared to route patterns in CUCM
Video	Adding/removing transformation rules, pipes, and bandwidth allocation/site in VCS
Video	Issuing firmware licenses for all Telepresence products
Video	Assist in firmware upgrades for Telepresence products, including infrastructure
Video	Adding/removing endpoints on TMS
Video	Managing and pushing global directory to video endpoints

### Exhibit B-5. User MACD Changes Examples

Device	Task
CME	Create user/ephone/DN
CME	Add DN to existing hunt group
CUC	Setup/decommission voice mail
CUC	Change existing subscribers
CUCM	Create users/devices/profiles
CUCM	Assign directory numbers
CUCM	Delete users/devices/profiles
CUCM	Move users/devices/profiles to new phone number
CUCM	Change existing users/devices/profiles
CUCM	Add users to/remove users from existing hunt groups
CUE	Create/Modify/Delete CUE Subscribers
UCCX	Assign skill to agent
UCCX	Add agent to team
UCCX	Create/modify/delete agents

---

## 14. SERVICE TRANSITION MANAGEMENT

Service Transition Management is a phased process in which Presidio implements Managed Services. It includes uploading information into the Monitoring Framework, including the Service Management System and configuration of the DCA. This consists of all steps required to activate and onboard Managed Services.

### 14.1. Kickoff Meeting

Presidio assigns a Project Manager (PM) to act as a single point-of-contact during the Service Transition Management phase. The external Kickoff Meeting indicates the initiation of the kickoff phase and is typically conducted via web or voice conferencing. The Kickoff Phase, as well as all remaining phases within Service Transition Management, is typically facilitated by the PM in collaboration with a Presidio Engineer.

This Service Transition Management phase includes the following activities:

- Coordinating, scheduling, and executing the Kickoff Meeting.
- Reviewing deliverables included in this Managed Service Contract.
- Reviewing services purchased, as indicated on the Client Purchase Order (PO).
- Aligning Presidio and Client on all major activities, risks, and milestones during Service Transition Management phase.
- Reviewing and scheduling a timeline for completing the Runbook and covered equipment list (CEL).

### 14.2. Runbook

Reviewing the Runbook components and key information is critical to success for Service Transition Management. Contained in the Runbook is the CEL, which identifies Managed and Monitored CIs. The PM develops a Project Plan for subsequent steps with distribution to project contacts. The required information must be uploaded into the Monitoring Framework. The Client is responsible for providing the information included in the Runbook, which is provided as part of Service Transition process.

### 14.3. Presidio Monitoring Framework

The DCA is configured to monitor Managed CIs per the CEL included in the contract. During the network discovery process, the PM communicates any discrepancies between identified CIs and requested Managed CIs in the CEL. Additional documentation specifying addressing, ports, and protocols is provided and reviewed with Client during kickoff.

Requested additions beyond the Managed CIs defined in the PO are subject to incremental service fees and additional Service Transition Management intervals. The PM communicates with sales personnel to add any additional items via an Addendum.

Implementing the Monitoring Framework includes the following:

- Preparing, configuring, and testing DCA.
- Shipping DCA to the designated Client premise.

- Remotely assisting Client with DCA installation; on-site installation support is available at client request.
- Establishing SSL over HTTP connectivity between Presidio and the Client premises.
- Configuring Presidio internal systems in preparation for service delivery.

Presidio inputs managed and monitored-only CI information into Monitoring Framework and the Service Management system. Service, support and escalation processes are also configured in the Service Management system during the Transition phase with input and agreement from the Client. This completes the implementation of the Monitoring Framework.

#### 14.4. Managed Device Preparation

The Monitoring Service element is dependent upon:

1. Network connectivity to Managed CIs.
2. Configuration of SNMP.
3. Trap Receiver destination IP address.
4. Provision of login and enable passwords.

A required device-specific configuration is supplied to Client, including community strings and host destination addresses.

#### 14.5. Setup and Modeling of the Application

Setup and modeling of the application is 100% Presidio's responsibility and includes the installation software components of the Monitoring Framework. Managed device information from the collection stage is loaded, and each individual device is configured for required monitoring statistics/reporting. Presidio and the Client resolve any network connectivity, firewall, or routing issues between CIs and DCA.

#### 14.6. Remote Training Session

The PM will schedule remote training sessions as necessary. These sessions are conducted via WebEx provided by Presidio.

The objectives of the training session are reviews of:

- Services to be delivered.
- Service documentation.
- Presidio and Client responsibilities during the service delivery process.
- Processes for obtaining service.
- Service escalation process.
- Client Portal overview.

#### 14.7. Start of Service (SOS)

The SOS milestone begins the Service Term, and is contingent on the timely completion of all activities as identified in the Runbook project schedule. Presidio works with the Client to meet the Start Date milestone and validate that the Service Transition Management phase is complete before Managed Services commences. Notification/Escalation and Event Management does not occur until a detailed operations handover has been performed, all required documentation and procedures are put in place. At the agreed-upon start date, the PM and the Client execute a

Certificate of Acceptance, concluding the Service Transition Management phase, and the Service Delivery phase commences.

## 15. CLIENT RESPONSIBILITIES

### 15.1. Install Monitoring Framework

Client shall provide the following with respect to the installation of the DCA:

- Provide appropriate secure rack-mount location for the DCA with suitable environmental conditions.
- Install the DCA and network connectivity per Presidio-supplied guidelines or allow Presidio to access appropriate location to deploy the DCA.
- Provide communications facilities and services including internet and network configuration. Communication facilities and services must be maintained for the duration of the service term.
- Provide a resource to support the installation of the DCA. These activities include:
  - Installing the DCA in a suitable equipment rack and connecting to network.
  - Power connection to Uninterruptible Power System (UPS) or other facility with continuous uninterrupted power.
  - Power-up.
  - Notification to Presidio that installation is complete.
- Provide suitable commercial power, and recommends UPS or other acceptable power back-up facilities providing a minimum of 1kVA dedicated to each appliance.

### 15.2. Training

The Client shall provide training coordination support, including identifying trainees and trainee contact information.

### 15.3. Transition Management

To ensure Presidio's ability to provide services for Managed CIs, Presidio requires the Client to:

- Assign a Project Manager or equivalent to represent the Client during the Service Transition Management phase.
- Assign a Technical Lead or equivalent to assist Presidio with establishing the network access required for Managed Services.
- The Client Project Manager and Technical Lead must attend the Project Kickoff Meeting and training sessions.

## 15.4. Runbook

Utilizing the required information provided by the client, Presidio will complete the Runbook, which provides the key information critical to success for the Service Transition Management phase. The Runbook provides information, such as:

- Detailed CI inventory information.
- Definition of Client-specific support policies including:
  - Points of contact and profile data
  - Change management procedures
  - Notification policy
  - Escalation policy
- Manufacturer maintenance and support contract information and contract number (e.g., Cisco SMARTnet).
- Provide as-built documentation including detailed design, network implementation plan(s), site survey(s), and bill of materials (if available).

## 15.5. Service Connectivity and Network Access

The Client is required to provide Read and Write management access to Managed CIs as defined by the Runbook. Access must be implemented in a timely manner in accordance to the Runbook. This includes SNMP, syslog, and other defined protocols as necessary to support services.

The Client will maintain manufacturer maintenance and support contracts covering hardware and/or software as may be applicable on all Managed CIs for the duration of the Managed Services contract. Client must provide support contract details, LOA and all other Client documentation and authorization required to facilitate incident resolution.

If the Client elects not to maintain such coverage, Presidio provides reasonable business effort only and may not have access to necessary manufacturer resources, such as support and software updates to facilitate repair.

In cases of special support arrangements; e.g., Client stocking their own spares (self-insuring), Client acquiring manufacturer support on a Time and Materials (T&M) basis, or instances of no manufacturer maintenance and support, the Client must provide a sparing strategy for replacement of devices, and the replacement and recovery of device functionality is the sole responsibility of the Client.

## 15.6. Communication and Change Management

Presidio has a co-management approach to Managed Services, allowing the Client and other Client-approved vendors to retain access to Managed CIs. Because multiple parties can make changes to the environment, Presidio requires anyone with access to the Client's environment to follow a consistent and documented Change Management process. This process is reviewed and agreed-upon prior to completion of the Service Transition Management phase.

The Client will:

- Notify Presidio in advance if scheduled or unscheduled maintenance of Client's Managed and Monitored-Only CIs will impact the:

- DCA monitoring of Managed CIs.
- Proper operation or network connectivity of Managed CIs.
- Maintain responsibility for informing Presidio of Client employee status changes.
- Provide and maintain a list of Client employees authorized to request changes.
- Provide and maintain an escalation path within the Client's employee base.



## MASTER MANAGED SERVICES AGREEMENT

This Master Managed Services Agreement ("Agreement") is effective as of the date last signed below, and is made by and between Presidio Networked Solutions LLC, with principal offices at 8161 Maple Lawn Blvd. Suite 150, Fulton, MD 20759 ("Presidio") and the client named below, on behalf of client and its affiliates ("Client"). In consideration of the mutual covenants and conditions herein contained, and other good and valuable consideration, the receipt and sufficiency of which is hereby mutually acknowledged, the parties agree as follows:

### 1. Client information

Client/Company:		POC:	
Billing Address:		POC Phone #:	
		POC E-mail:	

### 2. Scope; Coverage Period and Fees

Presidio shall provide the services ("Services") as defined in each attached Statement of Work (each, an "SOW") and the associated Service Appendix, with respect to the software ("Software") and/or related hardware ("Hardware") (collectively, the "Equipment") referenced in the Covered Equipment List ("CEL"), and subject to Presidio's acceptance of such Equipment as eligible for Services coverage pursuant to Section 5 below. The Equipment covered by this Agreement includes only the items on the CEL. The Start of Service ("SOS") date will be specified in the SOW, provided that for service management offerings, including Presidio Support Services ("PSS") for Cisco and other vendors, the SOS begins on the date that Presidio submits a purchase order to its vendor for the underlying support contract. A PSS agreement is independent from other Presidio Managed Services, and does not necessarily co-terminate with other managed services agreements.

### 3. Billing

Immediately upon (or prior to) execution of each SOW, Client shall issue a purchase order to Presidio for the Services requested therein. Presidio will have the right to withhold performance of the Services until such time as a purchase order, issued in conformance with this Agreement, is provided by Client. Presidio will reference the purchase order number on all invoices submitted to Client. Any preprinted terms and conditions on Client's purchase order (or other forms) which are in addition to or in conflict with this Agreement shall be null and void, even if purportedly acknowledged in writing by Presidio. Presidio will bill Client as specified in each SOW. Unless otherwise specified in an SOW, recurring Services will begin billing on the earlier of: (a) forty-five (45) business days from full execution of the SOW, or (b) the SOS, as determined by Presidio and communicated to Client. Service transition management fees, as specified in the SOW, shall be billed upon full execution of this Agreement and the applicable SOW. Client shall be invoiced thirty (30) days in advance of the current Service period. Cisco Partner Shared Support (PSS) offerings will be billed in advance for the duration of that agreement, for all years of the agreement. All invoices issued under this Agreement are due thirty (30) days from the date received by Client. All past due amounts shall bear interest at the rate of one percent (1.0%) per month or, if less, the maximum permissible rate under applicable law. In addition to the charges due for the Services or otherwise hereunder, Client shall pay or reimburse Presidio for any taxes, duties, fees and/or charges resulting from Presidio's performance of this Agreement which are levied by any taxing or other governing authority, except for taxes based upon Presidio's net income. Quotes provided by Presidio are valid for 30 days from the date issued.

### 4. Additional Services and Fees

The parties recognize that from time to time, Client may request maintenance and support or other Presidio services that fall outside the scope of this Agreement. The parties will discuss any requested out-of-scope services and negotiate the terms therefor in good faith. Services specifically considered outside the scope of this Agreement include, without limitation, the following: (a) correction of errors not attributable to Presidio or the manufacturer; (b) electrical work external to the Equipment; (c) installation, de-installation, reinstallation, or relocation; (d) supplies, accessories, or attachments; (e) "no fault found" (problem with equipment not provided by Presidio and/or not covered under this Agreement); and (f) MACD volumes or other managed services in excess of the terms per the Statement of Work and associated appendices. Additionally, material services requiring more than 2 hours will be treated as billable engagements. The threshold for services considered to be "material" is based on the time required for resolution. Client will be notified before billable work is performed, and such work will not begin until authorized by Client.

## 6. Equipment Configuration

Prior to the SOS, the Equipment configuration will be verified by Presidio. If the configuration cannot be verified via remote access, an on-site audit may be performed at Presidio's discretion and as agreed by Client. Client shall bear the reasonable expenses of the on-site audit, which shall be billable at Presidio's standard rates. Should this verification process indicate a change from the original configuration identified by Client, the Services Fees will be modified accordingly. Thereafter the Equipment will be reviewed ninety (90) days prior to the start of each coverage year to verify its configuration. Should the review indicate a change from the original Agreement configuration, the Services Fees will be modified accordingly. Presidio will advise Client of any condition which would render the Equipment ineligible for the Services hereunder. Client shall be responsible for correcting, at its expense, any such condition prior to or during the term of Presidio Services being provided.

## 6. Term

The initial term of this Agreement ("Term") shall be three (3) years from the effective date. The Term will automatically renew for additional one (1) year periods unless Client terminates the Agreement by giving prior written notice to Presidio (as specified in Section 8, below) at least sixty (60) days before the then-current Term expiration date. Notwithstanding anything to the contrary, any such notice of non-renewal shall not take effect, and this Agreement shall remain in force, until the end of the term of any and all outstanding SOWs. The term of Services under each SOW shall be as specified therein. Each SOW is strictly non-cancelable for any reason whatsoever. The Client will not, under any circumstances, be entitled to receive any refund for any third-party components of the Services.

## 7. Client Responsibilities

Subject to reasonable confidentiality/security obligations as accepted by Presidio in writing, Client shall grant Presidio full and free remote and/or physical access to the Equipment at all times during the Term of each SOW, including all required access credentials (e.g. IP addresses, SNMP community strings, passwords, etc.). For monitoring tiers of service, Client shall provide Presidio with at least one publicly-routable IP address for monitoring VPN connectivity and one IP address for the Presidio monitoring collection station. Client will provide all pertinent network diagrams and documentation. Client shall provide and maintain an up-to-date list of authorized contacts and escalation information, including third-party vendor contact information, letters of authority, maintenance schedules and device configurations. Client shall ensure that the Equipment meets, at all times, the manufacturer-approved configuration specifications and is covered by a then-current vendor maintenance and support program. **Client acknowledges and agrees that the foregoing factors are critical for Presidio to perform the Services, and Presidio's performance hereunder or under any SOW may be delayed or suspended if Client does not comply with its obligations in this Section.**

## 8. Notices

Day-to-day notices, authorizations and other official communications under this Agreement shall be transmitted in writing by email to Presidio at \_\_\_\_\_ and to Client at the POC address specified above, or as otherwise specified in an SOW. Legal and termination notices shall be sent by nationally-recognized overnight courier (signature required), to Presidio Networked Solutions LLC, Attn: General Counsel, One Penn Plaza, Suite 2832, New York, NY 10119, and to Client at the address and POC set forth in Section 1 above. Email notices are effective upon actual receipt; overnight courier notices are deemed given upon delivery as determined by signature, or refusal to accept delivery.

## 9. Assignment

Neither party may assign or transfer this Agreement or any rights or obligations hereunder without the written consent of the other party. Any required consent shall not be unreasonably withheld, conditioned or delayed. Notwithstanding the foregoing, Presidio may assign this Agreement without Client's consent in connection with a merger or other sale of Presidio's business as a going concern.

## 10. Warranties, Remedies and Limitations

Presidio warrants that the Services will be performed in a good and workmanlike manner, in accordance with all applicable laws and regulations. In the event this warranty is breached, Presidio shall promptly render/re-perform conforming Services. **THE FOREGOING WARRANTY IS MADE IN LIEU OF ALL OTHER WARRANTIES, GUARANTEES OR CONDITIONS PERTAINING TO THE SERVICES, WHETHER WRITTEN OR ORAL, STATUTORY, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY AS TO MERCHANTABILITY, NONINFRINGEMENT OR FITNESS FOR ANY PARTICULAR PURPOSE. ALL SUCH OTHER WARRANTIES ARE HEREBY EXPRESSLY DISCLAIMED. PRESIDIO IS NOT RESPONSIBLE FOR ANY WARRANTY OFFERED TO CLIENT BY ANY OTHER PARTY. THE FOREGOING WARRANTY AND**

REMEDY SHALL CONSTITUTE PRESIDIO'S SOLE AND EXCLUSIVE OBLIGATION, AND CLIENT'S SOLE AND EXCLUSIVE REMEDY FOR BREACH OF WARRANTY HEREUNDER, NOTWITHSTANDING ANY FAILURE OF THE FOREGOING REMEDY TO FULFILL ITS ESSENTIAL PURPOSE.

## 11. Non-Solicitation

During the term of this Agreement and for a period of twelve (12) months thereafter, Client will not, without the prior written consent of Presidio, solicit for employment any Presidio employee who was directly involved in the performance of this Agreement or any SOW. Notwithstanding the foregoing, Client shall be restricted from engaging in normal recruiting and hiring practices, including the placement of ads directed toward the general public and/or the use of recruiters, so long as such recruiting efforts are not specifically targeted at Presidio employees with whom Client became acquainted through this Agreement.

## 12. Confidentiality

Both parties recognize that during the course of this Agreement, one party ("Receiving Party") may acquire knowledge, confidential or proprietary business information or trade secrets from the other party ("Disclosing Party") which: (a) has been marked as confidential, (b) whose confidential nature has been made known to the Receiving Party, or (c) that due to the nature of the information, should be reasonably understood to be confidential (collectively, "Confidential Information"). Confidential Information, whether marked or not, shall specifically include, but not be limited to: (1) technical information such as methods, processes, formulae, compositions, systems, techniques, inventions, machines, computer programs and research projects; (2) business information such as client lists, pricing data, supply sources, financial and marketing data, production, or merchandising systems or plans, business policies or practices, and (3) any non-public personal information, including but not limited to personally identifiable financial, credit card or medical information. The Receiving Party agrees to keep all Confidential Information in a secure place and further agrees not to publish, communicate, divulge, use, or disclose, directly or indirectly, for his, her or its own benefit or for the benefit of another, any Confidential Information except as specifically required in accordance with performing its duties under this Agreement and as allowed by applicable law. The obligations of confidentiality contained herein shall apply during the Term of this Agreement and for a period of three (3) years thereafter. As applicable, upon termination or expiration of this Agreement, the Receiving Party shall deliver all confidential records, data, information, and other computer media or documents produced or acquired during the performance of this Agreement and all copies thereof to the Disclosing Party, provided that either party may, subject to the confidentiality provisions hereof, keep such copies as may be required of it by applicable law. Confidential Information shall remain the property of its owner/original discloser and nothing herein should be construed as granting a license, title, or any other rights to that information. This obligation of confidentiality shall not apply with respect to information that 1) was in the public domain prior to disclosure, 2) is available to the Receiving Party from third parties having the legal right to disclose the same on an unrestricted basis, 3) is disclosed by Disclosing Party to others on an unrestricted basis, or 4) is developed by Receiving Party independently without reference to any Confidential Information of the Disclosing Party. Either party may disclose Confidential Information to a court or government body having competent jurisdiction pursuant to an order therefrom, provided that the Receiving Party provides any legally permissible prior written notice of disclosure to the Disclosing Party and takes reasonable actions to avoid and/or minimize the extent of such disclosure.

## 13. Limitation of Damages

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW: (A) EACH PARTY'S ENTIRE LIABILITY UNDER THIS AGREEMENT AND ALL SOWS, WHETHER ARISING OUT OF THE SERVICES OR FROM SUCH PARTY'S NEGLIGENT OR OTHER ACTS OR OMISSIONS, SHALL BE LIMITED TO THE CHARGES AND FEES ACTUALLY PAID FOR THE SERVICES GIVING RISE TO THE CLAIM, AND (B) REGARDLESS OF THE LEGAL OR EQUITABLE BASIS OF ANY CLAIM OR OF ACTUAL NOTICE, NEITHER PARTY SHALL BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL LOSSES OR DAMAGES, INCLUDING, WITHOUT LIMITATION, DATA LOSS, EVEN IF THE PARTY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## 14. Default

Except as otherwise provided herein, in the event of any material breach of this Agreement by either party which continues for more than thirty (30) days after receipt of reasonable written notice of the breach, the aggrieved party may at its option: (a) if Client, suspend payments for so long as the breach continues uncorrected; and/or (b) if Presidio, suspend performance hereunder for so long as the breach continues uncorrected; and/or (c) to avail itself of any and all remedies available to it at law or equity, whether or not it elects to suspend its performance as permitted hereby.



**15. Subcontracting**

Presidio reserves the right to subcontract such portions of the Services to subcontractors of Presidio's choosing as it deems appropriate, provided that no such subcontract shall relieve Presidio of primary responsibility for performance of such Services.

**16. Indemnification**

Each party shall indemnify the other with respect to any third-party claim alleging: (a) bodily injury (including death) or damage to tangible property, to the extent such injury or damage is caused by the negligence or willful misconduct of the indemnifying party, (b) breach of any representations, warranties or obligations under this Agreement; or (c) violation of any applicable law or regulation. Each party will promptly advise the indemnifying party of the claim and turn over its defense. The party being indemnified must cooperate in the defense or settlement of the claim, but if properly and timely tendered to the indemnifying party, then the indemnifying party must pay all litigation costs, reasonable attorney's fees, settlement payments and any damages awarded; provided, however, the indemnifying party shall not be required to reimburse attorney's fees or related costs that the indemnified party incurs either to fulfill its obligation to cooperate, or to monitor litigation being defended by the indemnifying party.

**17. Publicity**

Unless required by law, neither party shall disclose the existence of, or any term or condition of, this Agreement to any third party (other than its parent or an affiliate) without the prior written consent of the other party. Neither party shall publish any advertising, sales promotion, press releases or publicity matters relating to this Agreement without the prior written approval of the other party.

**18. Miscellaneous**

The failure by either party to enforce any provision of this Agreement will not constitute a present or future waiver of such provision, nor limit such party's right to enforce such provision at a later time. All waivers by a party must be made in a written notice signed by the waiving party. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid, the remaining provisions shall continue in full force and effect and the parties shall substitute for the invalid provision a valid provision which most closely approximates the economic effect and intent of the invalid provision. This Agreement may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. Execution of this Agreement at different times and places by the parties hereto shall not affect the validity hereof. This Agreement constitutes the entire Agreement between Presidio and Client with respect to the subject matter hereof and supersedes all previous negotiations, proposals, commitments, writings, advertisements, publications and understandings of any nature whatsoever and in any manner whatsoever relating thereto. No agent, employee or representative of Presidio has any authority to bind Presidio to any affirmation, representation or warranty unless specifically included within this Agreement. Nothing in this Agreement shall be interpreted or construed so as to create any relationship between the parties other than that of independent contracting entities. Neither party shall be authorized to obligate, bind or act in the name of the other party, except to the extent Presidio is expressly authorized to do so by this Agreement. Neither party shall be responsible for delays or failures in performance (other than an obligation to pay money) resulting from fires, government requirements, acts of God or other causes beyond the reasonable control of the party whose performance is affected, and upon giving prompt notice to the other party such affected party's performance shall be suspended during the continuance of any such cause. The rights and obligations of the parties hereunder, and all interpretations and performance of this Agreement shall be governed in all respects by the laws of the State of New York, except for its rules with respect to the conflict of laws. Venue for any action hereunder shall be exclusively in the state or federal courts having competent jurisdiction and located in New York, New York. Each party hereby irrevocably waives its right to trial by jury.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

CARAHSOFT

West Virginia

BY: \_\_\_\_\_

BY: \_\_\_\_\_

NAME: \_\_\_\_\_

NAME: \_\_\_\_\_

TITLE: \_\_\_\_\_

TITLE: \_\_\_\_\_

DATE: \_\_\_\_\_

DATE: \_\_\_\_\_

## GENERAL DEFINITIONS

**Advanced Logic Profile:** Set of patented elements performing processing on millions of simultaneous, complex systems and network management flows to determine the precise root cause of an incident.

**Auto-Generated:** Ticket opened in the Incident Management System as a result of the monitoring tools. It differs from manual cases, which are manually opened by a system user either through the Client Portal or via phone.

**Business Hours:** Normal business hours for a company operating in the United States based upon local office time; i.e., traditionally 8 a.m. to 5 p.m. Monday through Friday.

**Business Reviews:** Regularly scheduled meeting, including Presidio governance and service delivery team, to provide metrics on Client performance during previous period. The data presented is also used to provide Clients insight into areas of Service Delivery improvements.

**Carrier:** Provider of voice and data transport services.

**Change Advisory Board (CAB):** Group or committee of stakeholders responsible to analyze and review submitted change requests and take action to accept or reject the change.

**Change Management:** Presidio process to receive, authorize, execute, and communicate changes to managed components.

**Change Request:** Client request for service, as related to Agreement, made by electronic format.

**Client Notification:** Communication to inform the Client that an Incident has been recorded.

**Client Portal:** Online Web user interface supplied for Client to receive and submit information to and from the Presidio Service Desk.

**Client Premise(s):** Physical Client location(s) where the DCA resides.

**Configuration Item (CI):** Component that needs to be managed to deliver an IT service.

**Contract:** Statement of Work (SOW).

**Covered Equipment List (CEL):** Document completed by the Client during the Service Transition Management phase. Document contains information about the managed equipment covered in this agreement and includes but is not limited to make, model, serial number, access credentials and IP addresses.

**DCA:** Monitoring and management solution used in the delivery of Managed Services. It consists of one or more appliances containing system and application software.

**Elements:** Basic network service when unbundled and an enhanced service when bundled into a service tier.

**Incident:** Event not part of the standard operation of a service and causes or may cause an interruption to, or reduction in, the quality of that service.

**Incident Management:** Process to detect an incident, notify the Client about the incident, and resolve the incident.

**Incident Resolution:** Process to restore services on managed components.

**Known Error:** Incident with a defined root cause and resolution.

**Letter of Agency (LOA):** Formal document that authorizes Presidio to act as the Client's agent for purposes of facilitating, tracking and/or providing services with carriers, maintenance contract providers, and other general-service providers.

**Management Hub:** Core of the Monitoring Framework system; provides an aggregation point for data compiled from multiple probes and integrates with tools data base and Client Portal.

**Management Services:** Service that provides Monitoring, Incident Resolution, Reactive Problem Management, Service Level management and Standard Changes to resolve all Incidents.

**Manual Cases:** Cases that a system user manually opens on the Client Portal or via phone.

**Manufacturer Field Notice:** Electronic notification from the manufacturer about product-related issues.

**Manufacturer Maintenance and Support Contract:** Contractual agreement between Client and Managed Components manufacturer that grants access to manufacturer-provided services, such as Managed Element hardware replacement, software patches, and technical support, necessary to maintain good working order.

**Message Bus:** Connects data collected from Probes with the Management Hub.

**Monitoring:** Detecting events on Managed CIs or Monitored-Only CIs.

**Monitoring Framework:** Presidio's integrated technology and tools required for delivering monitoring and managed services.

**Monitored-Only CI:** CI monitored by Monitoring Framework but not fully managed by Presidio Managed Services.

**Patch:** Small fix to a problem using a piece of software code.

**Problem:** Underlying cause of one or more Incidents.

**Problem Analysis:** Investigating problems to determine root cause.

**Problem Management:** Process to find and resolve the root cause of a Problem and prevention of incidents.

**Service Addendum:** Bilaterally agreed to document modifying scope of agreement.

**Service Deliver Center Supervisor:** Role within the Presidio Service Desk with management responsibilities for Client issues, escalations and staff.

**Service Delivery:** Phase after Transition Management when Presidio begins to deliver Services.

**Service Deliver Center (SDC):** Network Operations Center (NOC) is the primary facilities where Presidio technicians and engineers remotely support Clients.

**Service Management System:** Presidio Incident Management Platform where Client CI information and Incident Management information is maintained.

**SLO:** Service Level Objective.



**Vendor Management:** Presidio provides monitoring only (if monitoring framework is deployed), first-level support (triage only), alert and notification of monitored faults, and coordination of the supporting vendor/support teams on the Client's behalf throughout the troubleshooting process. Presidio does not provide second- and third-level troubleshooting and support for these devices. This support can only be provided on equipment with an existing manufacturer's warranty or current maintenance support contract.