# AV Managed Services SOW

***WA AV Master Contract ("CUSTOMER")***

***Continuant ("SUPPLIER")***

5050 20th Street East
Tacoma, WA 98424
(800) 652-9920

| *Application Coverage* | *Maintenance and Managed Services* | *# of Locations* |
|---|---|---|
| **AV** | **Incident Management**<br>**Event Management**<br>**Change Management**<br>**Problem Management**<br>**Capacity Management**<br>**Request Fulfillment Management**<br>**Asset Management**<br>**Service Level Management**<br>**Preventative Maintenance** | **1** |
| | **TOTAL MONTHLY PRICE:** | **$219.63** |

| | |
|---|---|
| Commencement Date: | TBD |
| Term: | 72 Months |

**Commencement Date:** TBD

**I agree to the terms and conditions of this Agreement.**

Customer Signature _____ Date _____

Customer Print Signature _____ Date _____

## Table of Contents

## Purpose

The purpose of this Statement of Work is to document the scope of tasks Continuant shall undertake and responsibilities that Continuant shall assume as part of its obligation to provide Continuant Managed Services (CMS) to the Customer and to document the allocation of responsibilities between the Parties with regard to certain operational processes.

## 1. Objectives

### 1.1. Objectives Overview

Continuant will provide incident management services to the State of Washington for programming and hardware on the covered equipment list. All coverage is for equipment as installed per the Continuant provided “as built” and does not apply to anything outside this defined environment. The Customer desires to use such services and products to achieve business goals and objectives. The Parties have entered into this SOW to support achievement of the Customer’s objectives. The Objectives are as follows:

- Implement consistent services and processes governing the maintenance and management of the Customer’s in-scope systems at the in-scope Sites.
- Optimize and enhance the Customer’s in-scope systems and realize continuous improvement in technology and service levels.
- Provide year-over-year reductions in the count and duration of outages through a high-touch service delivery experience, utilizing highly efficient processes and tools consistent with leading industry standards.

### 1.2. Global Service Desk

The Continuant Global Service Desk will be the primary communication point for services. The Customer will have several ways of interacting with the Global Service Desk. Customer Service Desk activities shall include the following:

- Perform initial analysis, troubleshooting, and diagnostics for Event Management
- Provide proactive communication of service delivery
- Manage escalations to ensure timely and high-quality resolution
- Provide life-cycle management of all service requests and incidents
- Provide Technical Support for general advice and help on covered systems
- Document manufacturer hardware maintenance contracts, and coordinate activities for reporting, release management, or other Continuant services relying upon manufacturer contract information if purchased

### 1.3. Technical Support (TAC)

Continuant makes available to customers a dedicated team of engineers to provide across-the-board AV Technical Support (TAC). TAC is designed to provide technical support for the

customer when the customer has a question about their covered environment. Customer can access Continuant TAC when following the below guidelines and attributes:

- Command Instructions
- Terminology Definitions
- Programming/Configurational Vetting
- Does not require changes or programming
- Does not require onsite technical resources
- Does not require scheduled maintenance window
- Does not require discovery
- Can be completed in 15 minutes or less.

Continuant TAC will stop at 15 minutes. All work will be billed at current Time & Material rates that exceed 15 minutes. Continuant will advise the customer of the rates and obtain customer approval before providing any additional support.

# 2. Service Transition

## 2.1. Service Transition Overview

Service Transition is the period of time between Commencement and Service Operation. During Service Transition Continuant will enable and deploy Continuant Managed Services to the Customer. Continuant will assign a Project Manager responsible for Service Transition activities and deliverables. The Project Manager will work with the State of Washington to establish a mutually agreed upon Service Activation date, whereby Service Transition activities will be complete and Service Operation begins. Continuant will make every effort to provide services to Customer upon Commencement and during the Service Transition period; however, service level agreements as defined in this SOW will not apply until Service Activation.

## 2.2. Service Connectivity and Network Access

Continuant Management Services are delivered using a collection of secure network protocols and communication ports. Customer must allow the collection of data for Managed Components. Customer will:

- Provide Read and Write management access to Managed Components as defined by the SAK.
- Provide read management access for components that are monitored only.
- Implement access in a timely manner in accordance with the SAK, including: SNMP, syslog, and other defined protocols as necessary to support CMS.

## 2.3. Continuant Remote Access and Event Management

The Continuant owned Monitoring Platform will allow remote access and monitoring for all managed components supported by CMS.

The Monitoring Platform includes a suite of management applications that consists of all management software and hardware required for the delivery of CMS. The Monitoring Platform

is deployed on the Customer's network in a single configuration instance or multiple instance configurations depending on the number, type, and location of the managed components.

The Monitoring Platform is an integral part of CMS and is installed during Service Transition for the duration of the CMS term. During the CMS term, Customer is granted a nonexclusive and nontransferable license to use the hardware and the software resident solely on the supplied Monitoring Platform. Customer must return any and all associated Monitoring Platform materials (devices and documentation) and connectivity devices to Continuant immediately upon expiration or termination of the CMS term.

Customer will use reasonable efforts to provide and maintain the Monitoring Platform in good working order. Customer shall not, nor permit others to, rearrange, disconnect, remove, attempt to repair, or otherwise tamper with the Monitoring Platform. Should this occur as a result of Customer actions without first receiving written consent from Continuant, Customer will be responsible for reimbursing Continuant for the cost to repair any damage thereby caused to the equipment on Customer's premises. Under no circumstance will Continuant be held liable to the Customer or any other parties for the interruption of Service, missed Service Level Agreements (SLA), or for any other loss, cost, or damage that results from the improper use or maintenance of the Monitoring Platform.

Unless otherwise agreed upon, title to all Monitoring Platforms shall remain in the possession of Continuant. Continuant expects that, at the time of removal, the Monitoring Platform shall be in the same condition as when installed, except what normal wear and tear is expected. Customer shall reimburse Continuant for the depreciated costs of any Monitoring Platform whereby the condition of which is deemed beyond normal wear and tear.

Continuant, or its subcontractors, shall be allowed access to the Customer Premises (location occupied by Customer or Customer's end user) to the extent reasonably determined by Continuant for the inspection or emergency maintenance of Continuant-supplied Monitoring Platforms.

Any delay by the Customer with supporting these Remote Access requirements may result in time and material charges for Service Requests and Incident Management Services.

The Continuant Monitoring Platform security compliance documentation is available upon request.

### 2.4. Service Activation Kit ("SAK")

Continuant will send the State of Washington a Service Activation Kit, which provides key information critical to success for commencement of CMS Service Operation. Customer is responsible for filling out all applicable areas in the SAK. SAK will include:

- Customer representative contact name
- Location of the site(s) to be managed
- Location of managed applications
- Network connectivity detail for the Monitoring Platform
- Device location and naming scheme
    - Managed IP addresses and system detail, SNMP community strings
    - Telnet and password access
    - Definition of Customer-specific support policies
- Maintenance contract or software support contract information

Customer will complete tasks defined in the SAK to enable management access to managed systems which may include setting up SNMP traps, and system logs.

Customer will provide as-built documentation including detailed design, Network implementation plan(s), site survey(s), and bill of materials. Data and documentation will be obtained from Continuant or an applicable Continuant subcontractor(s) as necessary to facilitate proper service commencement.

**Any delay or error by the customer in providing this information could delay service transition.*

### 2.5. Monitoring Platform Installation

For those cases where the Monitoring Platform or other components of CMS service delivery reside on the Customer's Premises the Customer must provide an appropriate secure rack-mount location for the Monitoring Platform (or components) with suitable environmental conditions for network server operation.

Customer will also provide the following:

- Installation of the Monitoring Platform and network connectivity per Continuant-supplied guidelines.
- Communications facilities and services including internet and network configuration. The communication facilities and services must be maintained for the duration of the service term.
- A resource to support the installation activities of the Monitoring Platform, which may include:
  - Racking
  - Connection to Network
  - Power connection to UPS or other facility with continuous uninterrupted power
- Suitable commercial power, and an uninterruptible power system (UPS) or other acceptable power back-up facilities providing a minimum of 1kVA dedicated for the Monitoring Platform.

## 3. Managed Services

### 3.1. Incident Management Services Overview

Incident management, both onsite and remote, ensures that normal service operation is restored as quickly as possible and the business impact is minimized. Continuant is responsible for prioritization and management of all incidents throughout their lifecycles. Remote incident management activities may include remote diagnostics, troubleshooting, and remote support for onsite personnel. Remote Incident Management is provided 24/7 for all covered sites. Onsite Incident Management is not included in Continuant's standard Incident Management offering. Onsite Incident Management can be purchased as 8/5 or 24/7 coverage.

### 3.2. Remote Incident Management

Remote incident management is provided 24/7 and ensures that normal service operation is managed through remote connectivity. Priority 1 incidents will receive 24/7 coverage. Priority 2-

4 will receive 24/7 remote monitoring and will be logged and addressed at the start of normal business hours the following day. Activities may include:

- Resolve service disruptions and performance degradations on Managed Components.
- Manage incident escalations to ensure timely and high-quality resolution of all issues by monitoring time remaining to meet SLAs.
- Utilize Incident remediation procedures to collect any additional data required to diagnose and match to known errors in Continuant knowledge base.
- Remote labor to repair or replace a failed part or device and the subsequent testing to confirm correct operation of the device and its interface and operation with associated equipment, communication facilities and services.
- Remotely facilitate hardware replacement and software updates determined to be required by Continuant.
- Utilize and update Continuant's ITSM platform with relevant information relating to an Incident.
- Make an initial determination of the potential resolution.
- Resolve as many Incidents as possible during the Authorized User's initial contact with the Service Desk, without transferring the call or using any escalation.
- Resolve Incidents requiring Tier 1-3 Support and close the Incident after receiving confirmation from the affected Authorized User that the Incident has been resolved.
- Resolve Incidents arising from or related to the Services, including break/fix Hardware and Software support.
- Retain overall responsibility and ownership of all Incidents until the Incident is closed subject to Customer approval.
- Software support services – includes remote installation assistance and basic usability assistance on minor firmware, patches and bug fixes (all managed components must include Original Equipment Manufacturer (OEM) software support coverage when applicable). Software support services do not include the purchase of subscriptions that provide entitlement and rights to use future minor versions (point releases), future major releases of software, or patches.

### 3.3. 8/5 Onsite Support (Optional)

Continuant will provide 8/5 Onsite Support that ensures normal service operation is restored as quickly as possible and the business impact is minimized through dispatch of local technicians. Continuant is responsible for managing the lifecycle of all incidents. Activities may include 8/5 Dispatch of local technicians for diagnostics, troubleshooting and/or parts replacement (parts not included unless they are covered under Hardware Replacement Services). Customer ensures access to building during normal business hours.

### 3.4. 24/7 Onsite Incident Management (Optional)

Continuant will provide 24/7 Onsite Support that ensures normal service operation is restored as quickly as possible and the business impact is minimized through dispatch of local technicians. Continuant is responsible for managing the lifecycle of all incidents. Activities may include 24/7 Dispatch of local technicians for diagnostics, troubleshooting and/or parts replacement (parts

not included unless they are covered under Hardware Replacement Services). Customer ensures 24/7 access.

### 3.5. Incident Prioritization

#### 3.5.1. Incident Prioritization Overview

Continuant classifies and prioritizes incidents according to Impact and Urgency. Continuant will evaluate Incident Impact and Urgency to classify all Incidents into Priority 1 (P1), Priority 2 (P2), Priority 3 (P3) and Priority 4 (P4) Incident categories.

#### 3.5.2. Impact Definitions

An Incident is classified according to its impact on the business (the size, scope, and complexity of the Incident).

Impact is a measure of the business criticality of an Incident, often equal to the extent to which an Incident leads to degradation of a Service. Continuant will work with Customer to specify Impact for each Managed Component during Service Transition. There are four Impact levels:

- **Widespread –** Entire Network is affected (more than three quarters of individuals, sites or devices)
- **Large –** Multiple sites are affected (between one-half and three-quarters of individuals, sites or devices)
- **Localized –** Single site, room and/or multiple users are affected (between one-quarter and one-half of individuals, sites or devices)
- **Individualized –** A single user is affected (less than one-quarter of individuals, sites or devices)

#### 3.5.3. Urgency Definition

Urgency defines the criticality of the Incident to Customer's business. Continuant will work with Customer to understand and set the proper Urgency level. There are four Urgency levels:

- **Critical –** Primary business function is stopped with no redundancy or backup. There may be an immediate financial impact to Customer's business.
- **High –** Primary business function is severely degraded or supported by backup or redundant system. There is potential for a significant financial impact to Customer's business.
- **Medium –** Non-critical business function is stopped or severely degraded. There is a possible financial impact to Customer's business.
- **Low –** Non-critical business function is degraded. There is little or no financial impact.

Continuant will downgrade the incident priority in accordance with the reduced severity of Impact or Incident resolution. The case may be left open for a prescribed period while operational stability is being assessed.

The Incident Ticket will be resolved by Continuant or Customer upon validation of the issue remediation and the system's returning to operational stability.

### 3.6. Change Management

### 3.6.1. Change Management Overview

Change Management is the process of assessing, controlling, managing and performing changes to “Customers” AV Infrastructure. The primary goal of this process is to ensure that all potential risks of performing Changes are mitigated while they are being planned and implemented. The Change Management process ensures proper preparation, communication and approvals are achieved. All Changes to configurations will be properly recorded against each affected CI in the Configuration Management Database (CMDB).

- Standard – Standard changes are defined as well-known, repeatable and thoroughly documented procedures. These procedures present a low risk to operations and business services as determined by a standard risk assessment. Standard Changes are preauthorized by the Change Advisory Board to be implemented per terms agreed upon with the customer. If the Service owner is concerned about the risk and/or potential impact of a change on other services, then a Normal or Emergency change should be considered.
- Normal – Normal changes are defined as medium/high risk to business services and therefore must follow the normal change management process. Due to the potential risk and impact, normal changes must be reviewed, prioritized and scheduled by the Change Advisory Board (CAB). The Urgency of Normal Changes may be upgraded to accelerate the timeline for implementation given customer business justification of an impending business impact.
- Emergency – Emergency changes are defined as high risk to the business and required to be implemented as soon as possible – without proceeding through the normal change management process. They may be required to resolve a break/fix situation that has resulted in a service degradation or interruption in service. They may also be needed to address an imminent interruption in service. Emergency Changes should leverage existing Standard Change procedures where applicable to reduce the associated risk. These Changes should also be related to a corresponding Incident where a service disruption or potential disruption has been recorded.

With a standard, formal approach, the potential for Change-related Incidents is diminished, the quality of the Changes is improved, and their impact upon the day-to-day operations of the organization is controlled. Change Management identifies all affected parties, systems, and infrastructure before the Change is authorized, scheduled, and approved for implementation. CIs are kept current by updating the CMDB after approved Changes have been completed.

### 3.6.2. Continuant’s Change Management responsibilities consist of the following activities:

- Raise and record Changes.
- Assess the impact, costs, benefit, and risk or proposed Changes.
- Confirm business justification and obtain approval.
- Perform Changes in Customer’s AV environment pertaining to CMS, including Changes to individual components and coordination of Changes across all components.
- Make all Changes in accordance with Change Management Procedures as approved by Customer CAB.
- Review and close all Changes.
- Coordinate with the Customer over the Change life cycle of all Changes for all Managed Components.

- Collect data on every Change attempted, including:
  - The reason for Change
  - Detailed description of Change
  - Whether the Change was successful from the perspective of the Authorized Users of the system
- Summarize the Changes made, and report results to the customer.
- Provide an audit trail for all Changes to the production environment in order to determine the Change made and the authorization to make the Change.
- Conduct Post Implementation Reviews (PIR) on Changes as requested by Customer.

3.6.3. Change Manager

Responsible for the day-to-day execution of the Change Management process within a functional area / domain and:

- Ensures correct execution of the Change Management process within a functional area / domain or application
- Maintains oversight of all RFCs within a functional area / domain or application
- The Change Manager is responsible for reviewing all metrics / reports that apply to his/her domain or application of responsibility and will take appropriate actions
- Tables all Request for Changes (RFCs) for a Change Advisory Board (CAB) meeting, issues an agenda and circulates all requests for changes to Change Advisory Board members in advance of meetings to allow prior consideration
- Decides which CAB members will come to which meetings, who gets specific RFCs depending on the nature of the RFC
- Convenes urgent CAB or ECAB meetings for all urgent or Emergency RFCs
- Participates in CAB meetings when a Change may affect a Managed Component
- Authorizes acceptable changes, either alone or after a CAB or ECAB has taken place
- Issues change schedules
- Liaises with all necessary parties to coordinate change building, testing and implementation, in accordance with schedules
- Updates the change log with all progress that occurs, including any actions to correct problems and/or to take opportunities to improve service quality
- Reviews all implemented changes to ensure that they have met their objectives
- Perform Post-Implementation Review for any failed Changes
- Reviews all outstanding RFCs
- Analyses change records to determine any trends
- Audits and closes RFCs
- Produces regular management reports

3.6.4. Change Approvals

All changes must be approved by Customer and Continuant in advance before any Change to the AV environment, with the exception of standard pre-approved Changes.

3.6.5. Change Implementation

Continuant is responsible for the management, coordination, and implementation of all agreed upon Changes, including:

- Consultative engineering support for Changes, as required
- Pre-Change device configuration backup
- Processing and administering all Customer RFCs
- Post-Change testing, customer verification, and documentation (e.g., Installation Quality/Operations Quality (IQ/OQ, network diagrams, site documentation, circuit information, maintenance activation, etc.)
- Notify Customer of completion of Change when requested
- If the implementation of the Change does not go as planned (e.g., causes an adverse results), execute the back-out plan (unless otherwise agreed by Customer) and notify Customer
- Post-Change CMDB Updates

3.6.6. Change Review Process

Continuant will review all implemented Changes to assess the following:

- If the Change has had the desired effect and met its objectives
- If the Customer requestor is satisfied with the results
- If there have been no unexpected or undesirable side-effects
- If the implementation plan worked correctly
- If the Change was implemented on time and to cost
- If the back-out plan functioned correctly, if it was needed
- If the Change was implemented in alignment with the change process

3.6.7. Change Window Requirements

Continuant will be available (8x5,24x7,365) to support Changes pending mutually agreed upon Customer Change Window preference. Continuant shall perform Changes and test equipment in a manner that is least disruptive to customer's business operations, including performing service affecting Changes outside of Normal Business Hours (if option is selected) and in accordance with customer Work Instructions. Continuant shall only implement Changes during a scheduled Change window. For Changes that cannot be implemented during the customer's specified Change windows, the parties will mutually agree on a date/time window in which to perform the Change. CUSTOMER will provide access to facilities, Equipment and Site contacts for all change events where onsite Continuant access is required.

3.6.8. Change Schedules

Continuant shall maintain a schedule of planned Changes on an on-going basis. The latest version of this schedule should be available to relevant stakeholders within the network organization. This schedule must contain details of all the Changes approved for implementation and their proposed implementation dates and times.

3.6.9. Change Priority and Categorization

Every Change under this Attachment SOW must be allocated a priority and timing that is based on the impact of the Change and the urgency of the Change. This 'Priority code' should be reviewed and should be used as a basis for the Change priority. Each Change must be categorized to reflect the impact of the Change on the customer Group in terms of the risk and impact on the Service.

3.6.10. Change Advisory Board (CAB)

A Change Advisory Board (CAB) is an advisory body for higher risk changes. The CAB is a body that exists to support the authorization of changes and to assist change management in the assessment and prioritization of changes. When a CAB is convened, members should be chosen who are capable of ensuring that the Change is adequately assessed from both a business and a technical viewpoint.

The Change Manager will chair the Continuant CAB, and potential members include:

- Customer(s)
- User manager(s)
- User group representative(s)
- Applications developers/maintainers
- Specialists/technical consultants
- Services and operations staff, e.g. service desk, test management, ITSCM, security, capacity
- Facilities/office services staff (where changes may affect moves/accommodation and vice versa)
- Contractor's or supplier's representatives

- Example CAB Meeting Agenda
  - Review the minutes from the last meeting
  - Review changes implemented during the previous period, including:
    - Failed changes
    - Backed-out changes
    - Successful changes
    - Incidents resulting from implemented changes
  - Review/Assessment of proposed Requests for Change (RFCs)
    - Risk and impact in terms of:
      - Service and Service Level impact
      - Capacity and performance
      - Security and compliance
      - Financial
    - Resources involved
    - RFC prioritization

## 3.7. Problem Management

3.7.1. Problem Management Overview

Problem Management is the process responsible for managing the lifecycle of all problems. The primary objectives of problem management are to prevent problems and resulting incidents from happening, to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented.

Continuant's Problem Management offering includes the activities required to diagnose the root cause of incidents identified through the Incident Management process, and to determine the resolution to the problems. Continuant will also maintain information about

problems and the appropriate workarounds and resolutions, to reduce the number and impact of incidents over time.

Continuant will provide value through Problem Management by utilizing Incident Management and Change Management to ensure that AV solutions service availability and quality are increased. When incidents are resolved, information about the resolution is recorded. This information is then used to speed up the resolution time and identify permanent solutions, reducing the number of and resolution time of Customer incidents. This results in less downtime and less disruption to the End Customers' business critical systems.

Continuant shall provide the following services for all Problem Management:

- Identify and triage Problem Management events
- Conduct root-cause analysis
- Implement and confirm Problem Management resolution
- Monitor, communicate Problem Management status
- Perform trend analysis and reporting
- Track the frequency and impact of recurring Incidents
- Diagnose the underlying root cause of Problem Management events
- Provide the expected resolution time for outstanding Problem Management events
- Help identify developing Service concerns or Problem Management events and actions plans to implement in such situations; implement such plans after consultation with, and approval by, Customer
- Identify weaknesses or potential weaknesses in the data infrastructure, component reliability and availability and other information at the disposal to the Continuant
- Perform analysis revealing trends that lead to the identification of specific (potential) Problem Management areas that need further investigation
- Assist the Customer with manufacturer's recurring equipment failure remediation
- During operational meetings agreed upon by the parties, present the results of all Problem Management analysis to Customer and recommend appropriate strategies and procedures to address identified concerns or issues

On a quarterly basis, Continuant will meet with Customer to review the Problem Management reports and related recommendations to reduce the volume and impact of Problem Management events.

### 3.7.2. Known Error Database

A known error is a condition identified by successful diagnosis of the root cause of a recurring Incident (i.e., a problem), and the subsequent development of a work-around or solution to this problem. All the relevant details of the problem must be recorded so that a full historic record exists. This must be date and time stamped to allow suitable control and escalation. A cross-reference must be made to the incident(s) which initiated the "Problem Record". Continuant will maintain a Known Error Database (KEDB) to track the following:

- Service details
- Equipment details
- Date/time initially logged
- Priority and categorization details
- Incident description
- Details for all diagnostic or attempted recovery actions taken

### 3.7.3. Root Cause and Preventative Action Plan

Continuant will provide a report of the root cause and corrective action analysis for all Critical/P1 Incidents plus any other Incidents flagged for Problem Management. This report will provide, at a minimum, the following items:

- The root cause and scope of the Incident, including any impacted service level(s)
- Identification and analysis of obstacles in recovering Services or affected Equipment
- A preventative action plan to be implemented to prevent future occurrences and
- A preventative action plan for other systems/environments.

The preventative action plans described in parts 3 and 4 will include due dates for performance of incremental tasks and completion of remedial measures and parties responsible for performance. Continuant will use reasonable effort to deliver a preliminary version of this report within five (5) business days and deliver the final version of the report via email no later than ten (10) business days after the applicable Incident has been resolved. In addition, Continuant will participate in Customer requested root cause analysis meetings to explain Incidents, Incident response, impacts, short term restoration plans and any follow-up action plans.

## 3.8. Event Management

Continuant will provide 24x7 event management that includes system monitoring and management of events for AV equipment where applicable. Continuant will identify critical components in Customers' environment and define key events for the specific system components. Continuant will provide structured levels of notifications to Customer for significant events detected in Customer's environment. Continuant Event Management will trigger Incident Management where applicable.

- Implementation of Continuant's Event Management Services requires Monitoring Platform Connectivity and Installation.
- Continuant will manage the Event Management software and tools required for Event Management.

## 3.9. Preventative Maintenance

### 3.9.1. Preventative Maintenance Overview

Continuant will perform Preventative Maintenance Services on customer AV Systems and Multimedia Systems. The Preventative Maintenance shall include cleaning the systems and ensure that the systems are operating per design specifications. Supplier shall provide necessary (AV OEM) System Firmware Updates as required. Request changes to programming code that fall outside of standard scope will be handled as part of Change Management.

Preventative Maintenance will be completed semi-annually at agreed upon dates. The following tasks are associated with our Preventative Maintenance offering:

- Inspect and test all system control functions and panels. Verify that all control functions perform in accordance with system specifications. Confirm that all software operations, associated hardware, and system pre-set and default conditions are properly set.

- Test control system and codec software/ firmware, working with product suppliers as necessary (e.g. Crestron, QSC). Update firmware if necessary to latest version.
- Test all AV signal sources and display. Ensure that all input and output audio and video signals meet system specifications, including but not limited to level, phase, separation, noise, distortion and frequency response in accordance with manufacturer's and system designer performance specifications.
- Calibrate and align all systems and equipment, including audio room balance, per recommended manufacturer and system design procedures. This applies to all system components such as servers, cameras, speakers, microphones, video monitors for video and computer signals, scan converters, projectors, switchers, amplifiers, mixers, echo cancellers, codecs, multiplexes etc. as applicable.
- Perform video conference calls if required. Co-ordinate with PC support to ensure proper standardized performance and certification of the facility.
- Perform general maintenance and clearing of all system components. Clean all monitor faces, touch screens, camera lenses and projector optics. All audio, video and control cables, patch fields and hardware inspected, tightened and repaired as necessary.
- Provide a detailed checklist and report of all maintenance activities and findings to the designated facilities manager. Maintain a log of regular visits, activities and results.
- Conduct end user reviews to ensure employees are properly utilizing the AV environment. Even if everything checks out on the technical side, there may be modifications to improve the user experience, bringing greater staff productivity and efficiency.

## 3.10. Asset Management

### 3.10.1. Asset Management Overview

Continuant will maintain asset data of all AV infrastructure deployed, or Managed Components and Configuration Items. The assets will be maintained within an ITSM Configuration Management Database (CMDB). Continuant will maintain asset information through the lifecycle, from deployment to decommissioning. Customer is responsible for providing all assets required and maintaining the proper data center environments.

The Configuration Management Database(CMDB) may store the following information:

- Part number
- Serial number
- Model number
- Version
- # of licenses
- # of available licenses
- MAC address
- IP address
- Firmware, version number
- Location – physical address

### 3.10.2. Hardware Replacement Services

Continuant will manage the Customer's hardware support contract when possible by opening support tickets and requests on behalf of the Customer. Customer must provide Continuant with a Letter of Agency (LOA) for representation.

Continuant will provide hardware replacement on specified Covered Equipment at no charge if it is under warranty by the manufacturer. In the event of a defective product, Continuant will make repairs or provide replacements of the defective product with either a new or refurbished equivalent model at Continuant's discretion.

If the failed equipment is not covered under warranty, Continuant will provide replacement parts at the customer's expense and can expedite shipping based on customer requirements and approval.

- Replacement equipment will be shipped according to customer SLA's.

3.10.3. Extended Warranty

Continuant will provide a standard 3-year warranty on all equipment that is installed by Continuant. Continuant will provide a 5-year warranty on all Crestron equipment at no extra charge. For all other equipment, the customer may purchase an extended warranty for 5 years at a cost of 10% of the equipment's original purchase price.

## 3.11. Capacity Management

3.11.1. Capacity Management Overview

Continuant will monitor and report on infrastructure system capacity and utilization on a monthly basis, advise on license usage, and implement license updates when necessary. The Customer shall be responsible for the purchase of new licenses and providing the licenses to Continuant.

## 3.12. Request Fulfillment Management

3.12.1. Request Fulfillment Management Overview

Continuant will perform Request Fulfillment Management services for moves, adds, changes, or deletions ("MACD") for end-user account management for supported Products upon proper submittal of such request to the Service Desk using an agreed-upon MACD request template. Customer MACDs can include changes to any individual account configuration settings and may include, but may not be limited to, VMR assignments, chairperson and conference PINs, RPRM registrations, WebSuite accounts, and e.164 extensions. Continuant will provide such services for up to twenty-five (25) MACDs with a one (1) business day turnaround SLO. MACD requests of more than twenty-five (25) shall be performed with an SLO as quoted by the Service Desk based upon the nature of the project.

## 3.13. Reporting Services

3.13.1. Reporting Services Overview

Reporting services cover the standard reports Continuant produces and provides to customer on a periodic basis in order to facilitate Managed Services governance and Service Delivery review. The reports listed below are only produced and delivered when the corresponding Managed Service has been purchased by customer.

Managed Services Governance is conducted via Quarterly Business Review meetings that Continuant and Customer hold. All standard Managed Services reports are delivered

in accordance with the QBR cadence. Highlights of the reports are discussed in the QBR meeting and the full reports are provided to the customer as supplemental material.

A Monthly Service Review is provided by the Named Account Manager to discuss billing and SLA compliance.

3.13.2. Service Level Management

- Time to Notify SLA Compliance
- Incident Resolution SLA Compliance by Priority
- Service Request Fulfillment SLA Compliance by Category

3.13.3. Incident Management

- Number of Incidents created for the reporting period by Priority (P1-P4) Number of Incidents closed for the reporting period by Priority (P1-P4)
- Number of Incidents created for the reporting period by Category
- Number of Incidents closed for the reporting period by Category
- Mean Time to Restore Service by Priority (P1-P4)
- Case Origin of Incidents
- Number of outstanding Incidents at the end of the reporting period by Status (Open, In Progress, On-Hold, Resolved)
- Incident Resolution SLA Compliance

3.13.4. Change Management

- Number of Changes Requested
- Number of Changes Processed
- Time for Change Approval/Rejection
- Average time from registering an RFC (request for change) with Change Management until a decision on the RFC is reached
- Number of changes that resulted in in incidents with downtime
- Change Acceptance Rate
- Successful vs unsuccessful changes
- Number of Emergency Changes

3.13.5. Problem Management

- The number of problems (opened and closed and backlog)
- The percentage of problem reviews successfully performed
- The percentage of problem reviews completed successfully and on time
- The backlog of outstanding problems and the trend
- Number and percentage of problems that exceeded their target resolution times

- Percentage of Problem RCAs delivered within SLA targets

3.13.6. Event Management

- Number and trend of events logged and investigated
- Number and trend of incidents resulting from event detection and analysis
- Number of Major incidents resulting from event detection
- Number of events caused by existing problems and known errors
- Top event types by asset

3.13.7. Asset Management

- List of Asset Licenses
- List of Assets by Category
- Retirement Activity
- Asset Reconciliation

3.13.8. Event Management

- Number and trend of events logged and investigated
- Number and trend of incidents resulting from event detection and analysis
- Number of Major incidents resulting from event detection
- Number of events caused by existing problems and known errors
- Top event types by asset

## 3.14. Service Level Management

3.14.1. Service Level Management Overview

Continuant's Service Level Management (SLM) offering tracks performance against negotiated service level targets called Service Level Agreements. Continuant will monitor and report on service levels where applicable and provide reports in Monthly Service Reviews. Service Level Agreement (SLAs) apply only to work performed on Managed Components that are managed exclusively by Continuant. Continuant is bound by and adheres to the SLAs during the Service Delivery phase. Within the SAK, the "Customer" and Continuant must document their agreement to formally acknowledge the completion of the Service Transition process for each Serviced Location. The Service Delivery phase commences upon agreement between Continuant and the "Customer" that the Service Transition phase is complete and that the Service Delivery phase has been reached. SLM and SLAs do not apply during service transition.

The following metrics are subject to Service Level Agreements:

- Time to Notify (TTN)
- Time to Restore Service for Incidents (TTR)
- Time to deliver an RCA for Major Problems

## 3.15. Service Level Agreement

### 3.15.1. Time to Notify (TTN)

Continuant will respond to incidents and service requests raised through the management platform by electronically notifying a specified Customer contact(s) within the TTN timeframe. Continuant SLAs are as follows:

| *Cases* | *Time to Notify Specified Contact* | *SLA Target* |
|---|---|---|
| **All Incidents and Service Requests** | 15 Minutes from case opened time/date. | 95% of cases. |

### 3.15.2. Time to Restore (TTR)

TTR refers to the time elapsed between the failure which caused the Incident and when Continuant restores the managed component to an acceptable operational state. Continuant SLAs are as follows:

| *Incident Level* | *Time to Restore* | *SLA Target* |
|---|---|---|
| **P1 Incidents** | 4 Hours | 95% |
| **P2 Incidents** | 12 Hours | 95% |
| **P3 Incidents** | 72 Hours | 95% |
| **P4 Incidents** | 120 Hours | 95% |

### 3.15.3. Time to deliver an RCA for Major Problems

Continuant will deliver a RCA document for every Major Problem. The table below lists the Continuant SLA for completing a RCA document for a Major Problem.

| *Cases* | *Time to deliver an RCA* | *SLA Target* |
|---|---|---|
| **All Major Problems** | 10 business days | 95% of cases |

### 3.15.4. SLA measurements exclude the following conditions from the elapsed time:

- Delays caused by Customer in resolving the qualifying issue (for example, waiting for response on change window or on-site resources)
- Any mutually agreed schedule of activities that causes service levels to fall outside of measured SLA defined obligations
- SLA will be “paused” for hardware replacement delivery to the customer location, either from a manufacturer maintenance agreement or hardware replacement services from Continuant
- Delays or faults caused by third party equipment, services or vendors, such as Carriers in resolving the qualifying issue
- Other factors outside of Continuant’s reasonable control for which Continuant is not responsible
- Acquisition and installation time of new software to be installed on the Managed Component due to software defects or bugs

## 3.16. Escalation Process

The Continuant Service Desk is responsible for managing escalations and coordinating communications of any escalations. Escalation Process adherence a typical escalation path and threshold period beyond which the matter is escalated to the next level is mentioned below. Threshold period indicates the time that has elapsed since an issue was first raised.

Escalation Path and Response Times

- Customer services desk to Continuant Service Desk
- Customer Regional Lead to Continuant Service Delivery Manager
- Customer Corporate Lead to Continuant Director of Operations
- Escalation Response Times:

| *Continuant Service Desk Available 24/7/365* | | |
|---|---|---|
| ***Escalation Time – P1/P2 Only*** | ***Level*** | ***Personnel*** |
| **< 30 Minutes** | Level 1 | Service Desk |
| **< 1 Hour** | Level 2 | Service Desk Lead |
| **< 2 hours** | Level 3 | Service Delivery Manager |
| **< 6 hours** | Level 4 | Director, Operations |
| **< 8 hours** | Level 5 | President, Continuant |

# 4. Network Operation Center Services

While most support organizations provide a one-time network assessment, Continuant provides an on-going assessment to consistently monitor, enhance, and improve the Customer's AV environment. Continuant's Network Operation Center Services may include the following:

- Accelerate planning cycles by identifying potential risks and gaps
- Improve network resilience and availability
- Ensure maximum bandwidth availability
- Ongoing analysis for optimal performance
- 24x7 event monitoring & management
- Health and performance monitoring
- Expert analysis, and diagnostics

# 5. Customer Responsibilities

## 5.1. As-built Documentation

Customer will provide as-built documentation, including detailed design, network implementation plan(s), site survey(s), and bill of materials. Data and documentation will be obtained from Continuant or an applicable Continuant subcontractor(s) as necessary to facilitate proper service commencement.

## 5.2. Additional Items

The Customer will also provide these additional items:

- Installation of the remote monitoring platform

- Establish network connectivity per Continuant-supplied guidelines.
- Communications facilities and services including internet and network configuration. The communication facilities and services must be maintained for the duration of the service term.
- A resource to support the installation activities of the Monitoring Platform
- Connection to Network
- Power connection within the facility with continuous uninterrupted power, suitable commercial power, and an uninterruptible power system (UPS) or other acceptable power back-up facilities providing a minimum of 1kVA dedicated for the monitoring platform.

## 6. Location

| *Location* | *Application(s)* | *Managed Service(s)* | *Monthly Price* |
|---|---|---|---|
| **TBD** | • **AV** | **Incident Management**<br>**Event Management**<br>**Change Management**<br>**Problem Management**<br>**Capacity Management**<br>**Request Fulfillment Management**<br>**Asset Management**<br>**Service Level Management**<br>**Preventative Maintenance** | $219.63 |

## 7. Appendix: Glossary of Terms

AV – Audio Visual

BOM – Bill of Material

CAB – Change Advisory Board

CI – Configuration Item

CMDB – Configuration Management Database

CMS – Continuant Managed Services, Configuration Management System

CPU – Central Processing Unit

CSR – Customer Service Representative

DML – Definitive Media Library

ECAB – Emergency Change Advisory Board

IOS – Internetwork Operating System

IP – Internet Protocol

IQ – Installation Quality

IT – Information Technology

ITSCM – Information Technology Service Configuration Management

ITSM – Information Technology Service Management

KEDB – Known Error Database

LOA – Letter of Agency

MAC – Media Access Control

MTBF – Mean Time Between Failures

MTBSI – Mean Time Between Service Incidents

MTRS – Mean Time to Restore Services

OEM – Original Equipment Manufacturer

OQ – Operations Quality

P1 – Priority 1

P2 – Priority 2

P3 – Priority 3

P4 – Priority 4

PC – Personal Computer

QA – Quality Assurance

RCA – Root Cause Analysis

RFC – Request for Change

RPO – Recovery Point Objectives

RTO – Recovery Time Objectives

SAK – Service Activation Kit

SAN – Storage Area Network

SFTP – Secure File Transfer Protocol

SIP – Session Initiation Protocol

SLA – Service Level Agreement

SNMP – Simple Network Management Protocol

SOW – Statement of Work, Scope of Work

SSR – Simple Service Request

T&M – Time and Materials

TDM – Time Division Multiplexing

TTF – Time to Fulfill

TTN – Time to Notify

TTR – Time to Restore

UPS – Uninterruptible Power Supply