

# **PRESIDIO<sup>®</sup>**

Future. Built.

**MANAGED SERVICES CONTRACT**

**SELECT SERVICES**

**SONOMA COUNTY**

**October 3, 2023**

## REVISION HISTORY

Revision	Revision Date	Name	Notes
1.0	07-21-2023	Michael Lambert	Initial Proposal for Select Managed Services
1.1	09-12-2023	Michael Lambert	Updated CEL, ESR Hours, and Term
1.2	10-03-2023	Michael Lambert	Added Master Managed Services Agreement into SOW

Notices: © 2023 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..... 5

3. MONITORING..... 10

4. CLIENT PORTAL & STANDARD REPORTS ..... 12

5. CHANGE MANAGEMENT..... 13

6. PROBLEM MANAGEMENT ..... 16

7. PATCH MANAGEMENT..... 17

8. DISPATCH SERVICES ..... 18

9. VENDOR MANAGEMENT..... 19

10. SERVICE DELIVERY MANAGEMENT..... 20

11. SERVICE TRANSITION MANAGEMENT..... 21

12. CLIENT RESPONSIBILITIES..... 23

13. PRICING & CONTRACT TERM..... 26

14. COVERED EQUIPMENT LIST..... 28

MASTER MANAGED SERVICES AGREEMENT..... 29

APPENDIX A: UNIFIED COMMUNICATION MANAGEMENT – CISCO ..... 34

APPENDIX B: ENTERPRISE CONTACT CENTER OPERATION..... 38

GENERAL DEFINITIONS..... 46

1. SERVICE SUMMARY

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 specific service deliverables are outlined in the Service Appendices. Your Managed Services Support Solution will include the following:

Service Elements

Select Service
<ul style="list-style-type: none"><li>• Service Delivery Center</li><li>• 7 x 24 x 365 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></ul>



---

## 2. SERVICE DELIVERY CENTER

The Service Delivery Center (SDC), also generally referred to as the Network Operations Center (NOC) is the main point of contact for reporting incidents (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, 7 days a week, 365 days a year in three primary locations including Orlando, FL, Dallas, TX, and Minneapolis, MN.

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 Capture Template. The Capture Template 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.
  - Interact with third-party support providers which requires a Client-signed Letter of Agency (LOA) processed during the Service Transition Management phase.

### 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.

#### 2.1.1. 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.

#### 2.1.2. . 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.

### 2.1.3. 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:** Complete 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.

The incident shall be closed by Presidio or Client upon validation of issue remediation and the CI's return to operational stability. Incidents may be closed if no communication from client is received after three (3) attempts

### 2.1.4. 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 several factors as defined in the thresholds).

**Incident Priorities**

IMPACT				
URGENCY		High	Medium	Low
	High	P1	P2	P3
	Medium	P2	P3	P4
	Low	P3	P4	P4

### 2.1.5. Incident Escalation

Incidents are escalated according to a defined process, and at any point, the Client may request escalation via the Presidio SDC 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 requested

## 2.2. Service Level Agreement

Service Level Agreements (SLA) 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 can set or change the priority level of an incident at any time, based on the impact to their specific business.

### Priority Levels

Level	Description
● <b>P1 / Critical</b>	Systems at one or many Client sites are completely unavailable. Affected systems cause significant business impact.
● <b>P2 / High</b>	Systems at one or many Client sites are partially unavailable. Affected systems cause some business impact.
● <b>P3 / Medium</b>	Operational performance of Client sites is impaired while most business operations remain functional.
● <b>P4 / Low</b>	Client is requesting information or a logical change that is covered under their service agreement.

Service Level Agreement	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>Resolution Time</b> The amount of elapsed time between Client initiation of an issue, or the time Presidio Managed Services detects a fault, and the time Presidio Managed Services resolves the incident or provides a workaround. The SLA timer pauses if it is dependent on third party intervention or if input or an approval is required from the client.	4 hours  >95%	24 hours  >90%	3 days  >80%	14 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			

\* Requires customer user subscription 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).

**Resolution Time** achievement percentage is calculated as follows:

Total Incidents within Resolution Time Service Level Target / Total Incidents (for each priority).

### 3. MONITORING

The Presidio Managed Services Framework integrates directly into the customer environment, providing on-site collection of all the critical information required to proactively manage customer components. The Managed Services Framework combines industry know-how with robust processes and procedures, underpinned with many of the best practices in the Information Technology Infrastructure Library (ITIL). Presidio aligns these proven processes with top technologies to create the interlocking framework that serves as the basis for all of Presidio's offerings.

The central-based processing and consolidation capability 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, 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 the Presidio monitoring tools. Once installed, DCA communicates back to the primary collection point where all the customer data is collected and automatically analyzed.

Inside 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.

Threshold values are set for all device types and all devices under collection. The customer can identify critical devices/resources in which they would like to be contacted. Any exceptions to these thresholds are collected and reported.

Presidio will monitor the health and performance via multiple avenues including SNMP polling at set intervals, SNMP traps for critical alerts, when viable other methods as determined by the technology being monitored. Utilization metrics include standard MIB-II and some private enterprise MIB information supported by the application such as LAN utilization, WAN utilization, CPU Utilization, Collisions, Discards.

Presidio's monitoring 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.

#### 3.1. Service Details

- 24X7 Collection of Monitored Component Data
- 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 for root cause analysis. Presidio provides full console services and incident workflow.

#### 3.2. Presidio Data Centers

Presidio's Managed Services data center space includes two redundant 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.

### **3.3. 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.



## 4. CLIENT PORTAL & STANDARD REPORTS

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.

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.



---

## 5. 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 four categories:

1. Standard Changes
2. Normal Changes
3. Emergency Changes
4. Customer Maintenance Changes

### 5.1. 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.

### 5.2. 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.

### 5.3. 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.

#### **5.4. 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 for qualifying alerts at the following levels: the entire company, a specific location or the specific CIs listed in the Change Request (for those events that have a location or CI associated with them). 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.

#### **5.5. 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).

##### **5.5.1. Device-Level Changes**

Device-level changes are defined as configuration requests that typically impact multiple users based on the change, such as configuration. Device-level MACD support is only provided to equipment specified in the CEL. Device-level MACD efforts are reviewed by Presidio relative to the contract for each device-level request and Presidio determines if it falls outside of the scope as defined below:

1. Takes less than 2 hours of time to complete which includes validation, scheduling, execution and testing
2. Does not require planning, design or installation 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. Not a major upgrade or a client request for feature addition.
5. Not an individual project or part of an individual project regardless of whether Presidio Professional Services, internal client or 3<sup>rd</sup> party is performing services.
6. Any new functionality that requires engineering development due to the addition of hardware or software, would require proper planning, designing and execution and would be considered a 'net-new' addition is considered a project.
7. Does not require a Solution Architect or Client Onboarding Manager to facilitate scheduling and planning.
8. Proactive patching for CVSS scores under 9 is not considered a device level change and will be subject to a separate statement of work per the Patch Management section.

For changes not covered by this agreement, Presidio provides a Block of Hours from Professional Services.

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 changes are allowed and limited to a total equivalent of two (2) per device, per month, per device type (example: firewalls, routers, switches, application). A cumulative change example would be 40 routers which would allow 80 configuration changes per month

across all routers. Any change allocations remaining at the end of a service month are considered forfeited and do not roll to subsequent service months.

## **5.5.2. User Changes**

A User Change is change for Collaboration services only impacting any single user-based configuration. 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.

## 6. 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. Presidio Managed Service Problem Management process also helps identify, diagnose, and resolve large scale Incident trends.

Presidio's Problem Management Policy objectives are as follows:

- To identify, diagnose, resolve, and report on Problems
- To update Presidio's Knowledge Base with Problem resolutions and workarounds to Known Errors so they are searchable for information to resolve similar issues

### 6.1. Problem Management Stakeholders

- **Problem Manager** –Overall accountability of the Problem Management Policy.
- **Problem Requestor** – The person who requested the initiation of a Problem Investigation.
- **Problem Management Review Team** – The group who meets weekly to provide status updates of current open Problems.
- **Solutions Provider Group** – Engineers assigned to investigate and resolve Problems.

### 6.2. Problem Management Process

#### Problem Identification

Analyzing available data, identifying/recording problems, and classifying problems according to impact, urgency, and status. Potential problems are identified through proactive and reactive methods:

- Proactive – Auto-generation of problems based on established criteria or reviewing scheduled reports for Incident trends
- Reactive – Responding to an identified large-scale and/or recurring incident trend or an issue identified as a problem during incident diagnosis

#### 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.

#### Problem Resolution

If a fix is discovered and can be reasonably implemented, the member of the Solutions Provider Group initiates the Change Management Process to implement the fix. If a fix is discovered and cannot be reasonably implemented due to factors such as cost, it should be notated in the Known Error Database and reported to the Problem Management Review Team for discussion.

#### Problem Closure

Once the resolution to a Problem is implemented and confirmed as fixed, the Problem will be closed with appropriate details included within the Problem record.

---

## 7. 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.

### 1) Incident Remediation

Patch management for incidents is applied when a Presidio engineer identifies, or a vendor support case directs Presidio to apply a version consistent with a fix for a known error. Patch application is a cooperative decision between the customer and Presidio. Patches are evaluated to ensure that current environmental stability is maintained, and are handled as Change Requests

### 2) Vulnerability Management

Vulnerabilities are defined as a defect reported by a manufacturer that has the potential to affect the overall security of a client device(s). 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>. Vulnerability patches below Critical level are not considered MACD activity and are billed as a separately negotiated addendum to the original SOW as applicable. Not all vendors provide CVSS scores or acknowledge vulnerabilities, and as such, Presidio is not able to notify/remediate unpublished vendor vulnerabilities.

As part of the Patch process, Presidio completes the following:

- For incident remediation patches, Presidio will work with the manufacturer/vendor 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.x, with a score of 9.0 – 10.0, Presidio will assess impacts to the Client and provide recommendations for remediation as applicable. Engagement times may vary dependent on the client environment and will include configuration validation before notification. Presidio allows 5-10 business days as a standard when being notified that the client infrastructure is affected by a vulnerability.
- For critical security vulnerabilities and incident remediation as defined above, Presidio remotely applies updates to affected CIs
- Patches that cover many devices and require the coordination of multiple teams and/or multiple outage windows are performed with the appropriate urgency and scheduled with respect to Presidio resource availability. More than fifteen (15) devices or five (5) locations will require the customer to provide a Point of Contact to assist in the coordination of scheduling the patch application. If the customer cannot provide the appropriate resource, Presidio will provide Project Management oversight at a mutually agreeable rate.

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 deemed out of scope and will require a separate statement of work. 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.



## 8. 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. The service objectives are 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 objective is typically provided to locations within 50 miles of a major metropolitan area.

International locations or 4-hour response guarantees for US locations require a separate customer agreement for coverage, due to additional cost.

Dispatch services not associated with an RMA replacement, which are customer requests for assistance, 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.

## 9. 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: Dispatches by Presidio for vendor managed products/devices are not covered, including RMAs.

## 10. 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)



---

## 11. 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.

### 11.1. Kickoff Meeting

Presidio assigns a Client Onboarding Manager (COM) 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 COM 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 per the signed Statement of Work.
- Aligning Presidio and Client on all major activities, risks, and milestones during Service Transition Management phase.
- Reviewing and scheduling a timeline for completing the Capture Template and covered equipment list (CEL).

### 11.2. Capture Template

Reviewing the Capture Template components and key information is critical to success for Service Transition Management. Contained in the Capture Template is the CEL, which identifies Managed and Monitored CIs. The COM 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 Capture Template, which is provided as part of the Service Transition process.

### 11.3. Presidio Monitoring Framework

The DCA is configured to monitor Managed CIs per the CEL included in the contract. During the network discovery process, the COM 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 COM 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.

#### **11.4. 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.

#### **11.5. 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.

#### **11.6. Remote Training Session**

The COM 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.
- Change management process.

#### **11.7. 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 Capture Template 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 COM and the Client execute a Certificate of Acceptance, concluding the Service Transition Management phase, and the Service Delivery phase commences.

---

## 12. CLIENT RESPONSIBILITIES

### 12.1. Install Monitoring Framework

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

- Customer to provide two external IP addresses and a shipping address.
- Provide an 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 recommend UPS or other acceptable power back-up facilities providing a minimum of 1kVA dedicated to each appliance.

If this SOW includes Monitoring of Windows-based products, our platform requires WMI (Windows Management Instrumentation) to perform advanced monitoring of Windows operating systems and other common Microsoft components/systems such as Active Directory, Exchange, SQL, and SharePoint. Devices that require vendor-supplied PowerShell commands that cannot run on Linux may also fall into this same category.

To achieve proper collection for these types of products, **customers must provide** a Windows resource (server or workstation/physical or virtual) that the LogicMonitor collector can be installed on. The customer is responsible for Windows Licensing. Maintenance and patching of this Windows resource are the responsibility of the customer unless this device is part of the CEL for those services in this SOW.

Presidio will assist with the installation of the collector agent on the customer-provided resource.

#### Basic Windows Collector Requirements:

- Designated Windows Server (2016 or up) is required for the purpose of collecting data from all supported Windows servers within environment
- Provided server must have necessary access to request and receive regular updates and patches
- Service Account to access the server(s) is required with Remote access for WMI permissions

- Hardware specifications for Windows collector to be determined based on number of servers/applications

## 12.2. Training

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

## 12.3. 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.

## 12.4. Capture Template

Utilizing the required information provided by the client, Presidio will complete the Capture Template, which provides the key information critical to success for the Service Transition Management phase. The Capture Template 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).

## 12.5. Service Connectivity and Network Access

The Client is required to provide Read and Write management access to Managed CIs as defined by the Capture Template. Access must be implemented in a timely manner in accordance with the Capture Template. 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.

## **12.6. 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.

### 13. PRICING & CONTRACT TERM

A Pricing Summary for this contract is provided below. Recurring fees begin on the Start of Service (SOS) date and remain fixed unless an Addendum is approved by the Client and Presidio. Changes in the Covered Equipment List (CEL) result in a change in the recurring pricing. Any net change in the device list results in a prorated change to the cost structure and is reflected in the subsequent invoice. Any modification to the Covered Equipment List that results in an increase or decrease of fixed fee invoicing in excess of 30% per invoicing period may be subject to adjusted pricing. Pricing included in this Agreement is valid for 30 days from the date issued.

Coverage Period				
Term	1 Year, 0 Months	Estimated Coverage Period	Start: 1/15/2024	End: 1/14/2025
Billing Frequency			Amount (\$) per Period	
Monthly			\$17,786.08	
Base Managed Services			Base Annual Service Fees	
	Collaboration Services		\$213,432.96	
Subtotal			\$213,432.96	
Non-Recurring Fees				
Service Transition Management		(billed upon execution of contract)		\$0.00
Elective Services Hours – Qty. 2,564*		(Billed as Incurred)		\$500,000.00
Subtotal			\$500,000.00	
Total Fees				
Year 1			\$713,432.96	
Total Contract			\$713,432.96	

\*Elective Service Hours will be billed in increments rounded up to the nearest quarter of an hour.



## **13.1. Statement of Work Term**

The term of this Statement of Work (SOW) ("Term") shall commence on the Actual Coverage Period Start of Service date ("Effective Date") and continue in effect until the end of term as noted in the above table. This SOW is non-cancelable. In the event of an early termination of this SOW for breach, Presidio shall be entitled, without limiting its other remedies under this SOW, at law or equity, to recover any remaining unpaid Service Transition and Installation Fees, along with the remaining cost of any hardware, software, licenses, volume-based subscription, or subscriptions for agents purchased by Presidio to provide services described within this contract.

The County shall have two options to extend this agreement (subject to a review of the ticket count and covered equipment list including CCE Agent Count) for a period of 1 year each by providing written notice to the Contractor thirty (30) days in advance of the expiration of the Initial Term and of the first extension option.

---

## 14. COVERED EQUIPMENT LIST

Management of the following devices is included in the scope of this proposal:

Service	Device Type	Model	Qty.
Collaboration Services	CUBE Voice Gateway	ISR 4431	4
<b>Collaboration Services</b>	<b>UC Application*</b>	<b>Calabrio</b>	<b>1</b>
Collaboration Services	UC Server	C Series	8
Collaboration Services	Hypervisor	Vmware	8
Collaboration Services	Select CCE: 600 Agents (with 0 Email, 0 Chat, 315 CVP Ports, 0 Dialer Ports)		

**\*Supported at the Vendor Managed Service Level as described above in Section 9**

All end-of-life/end-of-support equipment is supported on a business reasonable-effort basis.



## MASTER MANAGED SERVICES AGREEMENT

This Master Managed Services Agreement ("Agreement") and Exhibit A County of Sonoma Insurance Requirements is effective as of the date last signed below, and is made by and between Presidio Networked Solutions LLC, with principal offices at One Penn Plaza, Suite 2832, New York, NY 10119 ("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

<b>Client Company:</b>	Sonoma County	<b>POC:</b>	
<b>Billing Address:</b>	2615 Paulin Drive	<b>POC Phone #:</b>	
	Santa Rosa, CA 95403	<b>POC E-mail:</b>	

### 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 is defined within each SOW. The SOS for service management offerings for original equipment manufacturers shall begin on the date that Presidio submits a purchase order to its vendor for the underlying support contract.

### 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. 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 thirty (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 (Move, Add, Change, Delete) 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.

### 5. 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 Master Managed Services Agreement ("Term") shall be three (3) years from the effective date. The Term of this Master Managed Services Agreement 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.**

## 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's assigned Account Manager or Service Delivery Manager and to the Client at the POC address specified above, or as otherwise specified in a 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 not 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.

**SONOMA COUNTY**

BY: [Redacted Signature]  
NAME: Dan Fruchey  
TITLE: Director  
DATE: Oct 4, 2023

**PRESIDIO NETWORKED SOLUTIONS GROUP, LLC**

BY: [Redacted Signature]  
NAME: Steven Palmese  
TITLE: CIO  
DATE: Oct 4, 2023

**SONOMA COUNTY COUNSEL**

BY: \_\_\_\_\_  
NAME: \_\_\_\_\_  
DATE: \_\_\_\_\_

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.

SONOMA COUNTY

PRESIDIO NETWORKED SOLUTIONS GROUP, LLC

BY: \_\_\_\_\_

BY: \_\_\_\_\_

NAME: \_\_\_\_\_

NAME: \_\_\_\_\_

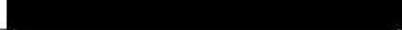
TITLE: \_\_\_\_\_

TITLE: \_\_\_\_\_

DATE: \_\_\_\_\_

DATE: \_\_\_\_\_

SONOMA COUNTY COUNSEL

BY: 

NAME: Tambre Curran

DATE: 10-5-23

## Letter of Agency

Effective Upon SOS

To Whom It May Concern,

Subject: Letter of Agency

The undersigned, Sonoma County, appoints Presidio Networked Solutions as agent (the "Agent") with respect to the following:

- To access and utilize all features and benefits of active maintenance, support or equipment manufacturer agreements Sonoma County has purchased from you.
- To perform maintenance on carrier circuits related to the Presidio Managed environment to allow Presidio to restore service or improve performance problems with carriers.
- To dispatch field maintenance technicians to service equipment, if any, under active maintenance, support or equipment manufacturer agreements Sonoma County has purchased from you.
- Other: \_\_\_\_\_

\_\_\_\_\_

You may deal directly with the Agent on all matters pertaining to the issues set out above and should follow the Agent's instructions with reference thereto. This authorization will remain in effect until further notice.

\_\_\_\_\_  
Client Signature

\_\_\_\_\_  
Client Name/Title (Please Print)

## APPENDIX A: UNIFIED COMMUNICATION MANAGEMENT – CISCO

The Presidio Unified Communications Management (UCM) 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, UCM 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.

### UCM Monitoring

UCM includes standard device-level monitoring as well as advanced collaboration-specific monitoring.

### UCM – Cisco-Specific Monitoring

UCM provides advanced monitoring of the Cisco UC solution. The table below lists examples of the elements in our current toolset can 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.

**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 Call Manager Down Server Node Communication Backup Service Failure Syslog Failures SNMP Failures Processes CPU Utilization Disk Partition Utilization SQL/Database
Unity Alerts	Critical Events Failover Service Failure Unity Port Max Unity Ports Not Registered
CCM Cluster Alerts	CDR/CMR Database Gateway registration
TFTP Alerts	TFTP Port/Network TFTP Service Failure



## Standard Reports

Our UCM Service includes a device-level reporting interface on our Presidio Client Portal that allows Standard reports to be viewed by the client. 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

### 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.
Trunk Summary	Overall trunk availability Impacted trunks Trunk down time Trunk outages Trunk degraded time Trunk busy hour Trunk busy hour by percentage Trunk call types
Call Failure Report	<b>Calls attempted</b> - A call attempt is a request from a phone/device to a PBX to initiate a call, whether that call is successful or not. $\text{Calls attempted} = \text{Calls completed} + \text{Calls rejected} + \text{other failures}$ . <b>Calls completed</b> - A call completed is a call successfully processed by a PBX and terminated with a disconnect cause code that indicates graceful termination. <b>Calls rejected</b> - 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. <b>Call failures</b> - 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. <b>Call failure ratio</b> - The call failure ratio is the percentage of processed calls that failed. <b>Calls processed</b> - A processed call is a call attempt that is processed by a PBX regardless whether the call completed successfully or not. <b>Disconnect cause code</b> - The disconnect cause code indicates why a call terminated abnormally. It may be attributed to either the origination or destination device. <b>Report data</b> - Calls with an origination time within the reporting period.
Long Duration Calls Report	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.
Node Utilization Report	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



Title	Description
	Call statistics Phone utilization Phones inactive
Route Pattern Availability	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. Overall route pattern availability Route pattern availability Impacted route patterns Route pattern down time Route pattern outages Route pattern degraded time

## UCM Service Management

In addition to the details in the main Contract, the following information specifically applies to the UCM.

### 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 CIs to service. Device-based backups are not performed for Monitored-Only CIs.

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 will alert/troubleshoot service failures and related incidents.

### Responsibility Matrix (RACI)

R = Responsible A = Accountable C = Consulted I = Informed

Device	Task	MS	PS	Client
CME	Create user/ephone/DN	R,A		C,I
CME	Add DN to existing hunt group	R,A		C,I
CUC	Setup/decommission voice mail	R,A		C,I
CUC	Change existing subscribers	R,A		C,I
CUCM	Create users/devices/profiles	R,A		C,I
CUCM	Assign directory numbers	R,A		C,I
CUCM	Delete users/devices/profiles	R,A		C,I
CUCM	Major Version Upgrade		R,A	C,I
CUCM	Minor Version (SU) upgrade	R,A		C,I
CUCM	Device Pack Installation	R,A		C,I
CUCM	Move users/devices/profiles to new phone number	R,A		C,I
CUCM	Change existing users/devices/profiles	R,A		C,I

Device	Task	MS	PS	Client
CUCM	New Circuit Turnup (Requiring configuration)		R,A	C,I
CUCM	Add users to/remove users from existing hunt groups	R,A		C,I
CUE	Create/Modify/Delete CUE Subscribers		R,A	C,I
UCCX	Assign skill to agent	R,A		C,I
UCCX	Add agent to team	R,A		C,I
UCCX	Create/modify/delete agents	R,A		C,I

## APPENDIX B: ENTERPRISE CONTACT CENTER OPERATION

The Presidio Enterprise Contact Center Operation (ECCO) Service provides Clients with critical Contact Center Enterprise monitoring, management, and support services. Our service is delivered with a two-tiered approach – best-in-class monitoring coupled with superior 24x7 remote operations support. Our proprietary monitoring service is a unique offering in the industry, providing agentless monitoring of the contact center environment. The system monitors the managed environment and customer call flows, while also performing synthetic transactions. The monitoring solution auto-generates actionable incidents for our management team located in our SDC. Not only is our service proactive, but the holistic approach to contact center management allows our ECCO engineering teams to resolve application and customer impacting issues quicker, greatly increasing efficiency and overall system health.

The pricing contained in this contract is the result of meetings between Presidio and the Client. During these meetings the level of support and estimated workload were discussed. As a result of this meeting Presidio has estimated a monthly contact center incident and/or customer request count of **Thirteen (13)**. This estimated workload comes from a combination of industry-leading Contact Center support experience and Client provided data.

### ECCO Monitoring

The Presidio Monitoring Framework integrates Vigilus monitoring to the Client's Contact Center portfolio. Presidio's Vigilus monitoring service is a unique offering in the industry, providing agentless monitoring of the contact center environment as well as unique call monitoring features.

The Vigilus system constantly monitors the managed environment and auto-generates actionable incidents for our industry leading ECCO team. Unlike other monitoring options, Vigilus eliminates delays caused by incident auto-resolution and event suppression, providing both Presidio and the Client more visibility into the managed environment. This allows for faster response time to outages as well as a more proactive notification for issues before they become business impacting.

The Vigilus call monitoring (or IVR monitoring) application offers our Clients a proactive way to both monitor scripting as well as place periodic calls into their environment through external sources. Presidio utilizing Vigilus offers a more holistic view of monitoring. Not just monitoring the Contact Center, but also the IVR along with integrated systems, manufacturers, and carriers.

When a threshold or alert is triggered, an incident is generated the Presidio ECCO team responds. The ECCO solution requires the use of Remote Desktop Protocol (RDP) in addition to SNMP and other common management protocols. Also of note, the ECCO monitoring solution may require multiple DCAs depending on the size and complexity of Client environment and are determined during the project scoping. The following conditions (Exhibit C-1) are currently monitored through our tools.

**Exhibit C-1. ECCO Monitoring**

Device	Task
Hardware	RAM, CPU, and Disk utilization
Application Monitoring	UCCE Applications (router, logger, peripheral gateways, etc...) Finesse servers CVP Call Servers
Operational Statistics	Agent status IVR/CVP Ports

Device	Task
	Trunk Utilization (Optional)
Call Scripting	CVP Studio scripting elements
Log Aggregation	UCCE (router, logger, peripheral gateways, etc...), CVP, Finesse
Synthetic Transaction	External automated test calls utilizing speech and DTMF

## Reports

Presidio provides a Client Portal for a consolidated view into the entire managed environment. The Client Portal allows access to all tickets created in our Incident Management System, full asset/device management, and system reporting interface.

The ECCO Service with Vigilus includes two levels of reporting. We include a Standard Interface on our Client Portal and an additional Cloud interface directly to Vigilus.

## Dashboards

Presidio provides monitoring and management capabilities of various elements of the Cisco Unified Contact Center (UCC) including:

- Contact Center Enterprise (CCE) Status
- Contact Center Enterprise (CCE) Active Alarms
- Contact Center Enterprise (CCE) Recent Events
- Environment General

### Exhibit C-2. Management Dashboards

Dashboard	Description
Contact Center Enterprise (CCE) Status	Provides Client with easy-to-use expandable views of each portion of their Cisco Unified Contact Center sorted by application (including CVP and Finesse). By expanding any tab in the CCE Status, the Client can easily see the name of each process running on the selected device, its status, and total uptime. The Client can easily see status of each CCE components, status of the private network (if applicable), and Current call volumes per CVP CallServer.
Contact Center Enterprise (CCE) Active Alarms	Tracking alarms is a necessary requirement to determine contact center health. Vigilus has the intelligence to monitor each component of the Cisco Unified Contact Center by looking for abnormal activity. When abnormal activity is detected and alarm is generated to create an incident. The CCE Active Alarms dashboard shows all current active alarms, short description, severity, recommend action (if applicable), and date/time of alarm generation. In addition a Details button allows the Client to quickly dive into each alarm to gather more information about the state, process, and any additional notes generated on the alarm.
Contact Center Enterprise (CCE) Recent Events	Event tracking is a critical requirement to monitoring ongoing alarms. When an alarm is generated status changes can occur due to further alarms or state changes. The CCE Recent Event dashboard shows all recent events date/time stamp, component, and short description. In addition a Details button allows the Client to quickly dive into each event to gather more information about the state, process, severity, and any additional notes generated on the event.
Environment General	Provides a numerical display of Active Alarms, Events Today, and Devices Requiring Attention

## Standard Reports

The Presidio Management Platform provides standard reports for additional visibility to various elements of the Cisco Unified Contact Center (UCC) including:

- Monitoring
  - Collectors
  - Device Metrics
- Activity
  - Alarms
  - Event
- Performance Metrics

### Exhibit C-3. Standard Reports

Report	Description
Monitoring – Collector and Device Metrics	Provides information on Vigilus collectors in the environment including locations and device metrics such as RAM, CPU, Disk, and application status
Activity – Active Alarms Report	Alarms are crucial to alerting Clients and support personnel of issues or potential issues that may impact the contact center. The Active Alarms Report provides information about the state, process, and any additional notes generated on the alarm.
Activity – Recent Event Report	Detailed information regarding events impacting current alarms is important when monitoring ongoing performance of a contact center. The Recent Event Report outlines events providing information about the state, process, severity, and any additional notes generated on the event.
Performance Metrics	Virtual Machine performance is critical to contact center components. The Performance Metrics report provides a visual representation of selected metrics across CCE virtual machines including . RAM utilization, CPU utilization, available disk space.

## ECCO Services

In addition to main Contract details, the following information specifically applies to the ECCO Service.

### **System Backups**

Presidio shall perform back-up processes for Cisco routers, switches, and other IOS-based configuration devices. This includes definition and execution of service restoration process for managed devices. The configuration back-ups are stored on the Presidio Monitoring Framework and available for use by Presidio in bringing current or replacement Managed CIs to service. Device-based backups are not performed for Monitored-Only CIs.

Client Backup Process Requirements:

- Responsible for Back-up servers, Cisco Unified Communications systems, and Cisco Contact Center systems. The Client is responsible for ensuring backups run successfully.
- Perform backup on Managed CIs that do not run Cisco IOS or where the back-up mechanism is not supported, the Client is responsible for ensuring backups run successfully.

Presidio shall provide best-practices recommendations to the Client in support of their non-IOS device-based backups.

## **MACD Services**

As part of the ECCO Select service MACD's are included. A MACD is defined by Presidio as a Move, Add, Change, or Deletion to an existing user, script, or configuration element in the Contact Center. MACD's are expected as part of typical Contact Center operations. For the purpose of this contract MACD's are expected to be requested at a rate of five percent (5%) of the total agent volume monthly.

MACD is any single activity on an individual covered configuration element that meets the following criteria:

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 part of a project or a project in itself.
6. Is not part of a bulk request of users or configuration elements.

## **Elective Change Services**

An Elective Change is requested by the Client and is often the result of changes in the Client network or business processes. Elective Changes are typically requests for new configurations that are not considered MACD. For example new Precision Queues, skill groups, and scripts would be an Elective Change. The Client identifies the change requirement and must submit the Elective Change Service request on the Client Portal.

Elective Changes are scheduled services the Client must request in advance of service delivery. Elective Change service delivery response time is not defined by the Service Level Objectives in the Contract. In order to minimize Elective Change Services response time the Client may purchase a block of hours in advanced for execution of these changes

For requested Elective Change Services, the Client must have a sufficient balance of hours on account to cover their requested change based on time estimations provided by Presidio at the time the change is requested. All Elective Change hours must be used within the duration of an annual Contract period. If a multiple year Contract is purchased, the hours allocated to each year must be used completely by the end of the year. If the Client has hours remaining on their account balance at the end of the Contract year, and the Client has purchased or is purchasing additional year(s) of service, the previous years' unused hours are carried over. Hours from the subsequent year may not be borrowed against and used in the current year.

Presidio shall provide a monthly Elective Change Report that accounts for opening balance, credits, debits and remaining balance of hours. The Client has the option to purchase additional Elective Change hours as needed.



---

## **Patch Management**

Included in the ECCO Select service is Microsoft operating system patching and application patching required as part of general maintenance. Windows systems outside the Contact Center environment are not included in patching scope.

Operating system patching can be requested as frequently as quarterly for all Contact Center Windows components. Since Cisco is no longer recommending Microsoft patches for their environment, the customer is required to provide the patches they would like applied to the Contact Center Microsoft environment. In the event the customer does not wish to provide patch management oversight, access to windows update will be required for all Contact Center Microsoft environment. As with any patching, the ECCO team will test functionality of the Contact Center environment after patches have been installed. In order to meet the customer's preferred patch management schedule, all Windows patching should be requested at least a week in advance. To stay in accordance with best-practices, operating system patches are applied during Enterprise Contact Center application maintenance patching windows.

Application maintenance patching on the Enterprise Contact Center solution is defined by Cisco as any Engineering Special or Maintenance Release. Application Minor Release patching may be covered in the event they do not require the following:

- Planning or design Services
- Data migration or use of the Enhanced Data Migration Tool (EDMT)
- VMWare update
- Hardware migration or upgrade
- Windows or SQL update or migration
- Additional of appliances or virtual machines

## **Service Elements**

The following breakdown lists some of the tasks typically requested in Enterprise Contact Center Operation support. All requests or elements listed in this document fall under the specific guidelines as outlined in your scope of work. These guidelines supersede all categorizations outlined in this document.

MACD is any single activity on an individual covered configuration element that meets the following criteria:

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 part of a project or a project in itself
6. Is not part of a bulk request of users or configuration elements

## **Synthetic Transaction – Customer Experience (CX) Testing**

As part of the ECCO Essential service, Clients can elect to have Presidio provide Synthetic Transactions or CX testing and alerting for their environment. As part of this engagement with Presidio the client can elect to have up to two (2) dialed numbers configured along with testing of up to twenty thousand (20,000) minutes per year. Additional dialed numbers and minutes are available for a fee.



On a failure of any test a ticket will be generated in Presidio's ticketing system and the Client will be notified. All tests will have the accompanying date/time, number dialed, recording, pass/fail step, and an expected response vs received response comparison. As an added benefit this testing can alert on carrier failures to deliver the test call as well as any unexpected schedule changes (such as holidays).

**Exhibit C-4. Service Element Classification**

Overview	MACD	Elective Change	Professional Services
<b>Agent/Supervisor</b>			
Bulk addition of agent groups		X	
Move, Add, Change, or Deletion of existing agent	X		
Agent/Supervisor team, attribute, or skill change	X		
Add or promote supervisor	X		
Informal agent/supervisor training	X		
Formal agent/supervisor training			X
Finesse/CTIOS/CAD screen-pop modification		X	
New Finesse/CTIOS/CAD screen-pop			X
Finesse gadget modification			X
New Finesse gadget			X
<b>CCE Configuration</b>			
Agent Desktop Settings configuration change	X		
New Precision Queue or SkillGroup		X	
New Attribute addition to current Precision Queue	X		
New Global Variable		X	
Global Variable modification	X		
<b>Scripting</b>			
CallType add (existing scripting)		X	
Dialed Number add (existing scripting)	X		
Operational hours change	X		

Overview	MACD	Elective Change	Professional Services
Holiday Schedule update	X		
Activate emergent, open, or closed condition (existing scripting)	X		
Prompt change	X		
Menu change		X	
Self-Service IVR scripting change			X
Custom CVP Studio elements			X
Queue Treatment change	X		
New Call Flow			X
Courtesy or Agent Request Call Back Modification		X	
New Courtesy or Agent Request Call Back			X
Modification to Whisper Announcement	X		
New Whisper Announcement			X
New/Enable Agent Greeting			X
Reporting			
Existing report modification (existing data elements)		X	
Existing report modification (new data elements)			X
New custom report			X
Supervisor report access	X		
Existing dashboard modification (existing data elements)		X	
Existing dashboard modification (new data elements)			X
New dashboard			X
Informal customer requested report training		X	
Formal Reporting Training			X
Outbound Dialer			
New dialer campaign			X
Dialer campaign configuration modification	X		

Overview	MACD	Elective Change	Professional Services
Dialer mode modification		X	
Dialer Skill Group modification		X	
Email / Chat			
New mailbox			X
New chat entry point			X
Chat entry customization			X
Keyword routing modification		X	
New keyword routing			X
Contact flow modification	X		
Knowledge-base modification			X
New chat/email agent	X		
Chat/Email agent skill/attribute modification	X		
Patching			
Engineering Special patching (Incident Remediation)	X		
Maintenance Release patching (Incident Remediation)	X		
Minor Release patching		X*	X*
Major Release patching			X
Customer backup verification	X		
Maintenence window testing	X		
License update	X		
Operating System patching (during UCCE software patching)		X	

*\*Note – Version dependent*

## 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 Incident:** 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 through the Client Portal, email 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 led by the Service Delivery Manager to provide metrics on Client performance during the previous period. The data presented is also used to obtain the Clients' insight into areas of Service Delivery improvements. Depending on contact specifics, this is typically a Quarterly Business Review (QBR).

**Capture Template:** 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.

**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).

**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 database 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 Delivery 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 Managed Services.

**Service Delivery Center (SDC):** Network Operations Center (NOC) are the primary facilities where Presidio technicians and engineers remotely support Clients.

**SLO:** Service Level Objective.

**Service Management System:** Presidio Incident Management Platform where Client CI information and Incident Management information is maintained.

---

**Exhibit A**

With respect to performance of work under this Agreement, Consultant shall maintain and shall require all of its subcontractors, consultants, and other agents to maintain insurance as described below unless such insurance has been expressly waived by the attachment of a *Waiver of Insurance Requirements*. Any requirement for insurance to be maintained after completion of the work shall survive this Agreement.

County reserves the right to review any and all of the required insurance policies and/or endorsements, but has no obligation to do so. Failure to demand evidence of full compliance with the insurance requirements set forth in this Agreement or failure to identify any insurance deficiency shall not relieve Consultant from, nor be construed or deemed a waiver of, its obligation to maintain the required insurance at all times during the performance of this Agreement.

**1. WORKERS COMPENSATION AND EMPLOYERS LIABILITY INSURANCE**

- a. Required if Consultant has employees as defined by the Labor Code of the State of California.
- b. Workers Compensation insurance with statutory limits as required by the Labor Code of the State of California.
- c. Employers Liability with minimum limits of \$1,000,000 per Accident; \$1,000,000 Disease per employee; \$1,000,000 Disease per policy.
- d. Required Evidence of Insurance: Certificate of Insurance.

If Consultant currently has no employees as defined by the Labor Code of the State of California, Consultant agrees to obtain the above-specified Workers Compensation and Employers Liability insurance should employees be engaged during the term of this Agreement or any extensions of the term.

**2. GENERAL LIABILITY INSURANCE**

- a. Commercial General Liability Insurance on a standard occurrence form, no less broad than Insurance Services Office (ISO) form CG 00 01.
- b. Minimum Limits: \$1,000,000 per Occurrence; \$2,000,000 General Aggregate; \$2,000,000 Products/Completed Operations Aggregate. The required limits may be provided by a combination of General Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance. If Consultant maintains higher limits than the specified minimum limits, County requires and shall be entitled to coverage for the higher limits maintained by Consultant.
- c. Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured retention exceeds \$100,000 it must be approved in advance by County. Consultant is responsible for any deductible or self-insured retention and shall fund it upon County's written request, regardless of whether Consultant has a claim against the insurance or is named as a party in any action involving the County.
- d. County of Sonoma, its Officers, Agents and Employees shall be endorsed as additional insureds for liability arising out of operations by or on behalf of the Consultant in the performance of this Agreement.
- e. The insurance provided to the additional insureds shall be primary to, and non-contributory with, any insurance or self-insurance program maintained by them.
- f. The policy definition of "insured contract" shall include assumptions of liability arising out of both ongoing operations and the products-completed operations hazard (broad form contractual liability coverage including the "f" definition of insured contract in ISO form CG 00 01, or equivalent).
- g. The policy shall cover inter-insured suits between the additional insureds and Consultant and



include a “separation of insureds” or “severability” clause which treats each insured separately.

**h. Required Evidence of Insurance:**

- i.** Certificate of Insurance.

**3. AUTOMOBILE LIABILITY INSURANCE**

- a.** Minimum Limit: \$1,000,000 combined single limit per accident. The required limits may be provided by a combination of Automobile Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance.
- b.** Insurance shall cover all owned autos. If Consultant currently owns no autos, Consultant agrees to obtain such insurance should any autos be acquired during the term of this Agreement or any extensions of the term.
- c.** Insurance shall cover hired and non-owned autos.
- d.** Required Evidence of Insurance: Certificate of Insurance.

**4. PROFESSIONAL LIABILITY/ERRORS AND OMISSIONS INSURANCE**

- a.** Minimum Limit: \$1,000,000 per claim or per occurrence.
- b.** Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured retention exceeds \$500,000 it must be approved in advance by County.
- c.** If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.
- d.** Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.
- e.** Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

**5. CYBER LIABILITY INSURANCE**

**Network Security & Privacy Liability Insurance:**

- a.** Minimum Limit: \$2,000,000 per claim or per occurrence, \$2,000,000.00 aggregate.
- b.** Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Consultant in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs (including notification costs), regulatory fines and penalties as well as credit monitoring expenses.
- c.** If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.
- d.** Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.
- e.** Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

---

**Technology Errors and Omissions Insurance:**

- a. Minimum Limit: \$2,000,000 per claim or per occurrence, \$2,000,000.00 aggregate.
- b. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Consultant in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs (including notification costs), regulatory fines and penalties as well as credit monitoring expenses.
- c. The Policy shall include, or be endorsed to include, property damage liability coverage for damage to, alteration of, loss of, or destruction of electronic data and/or information “property” of the County in the care, custody, or control of the Consultant. If the Consultant maintains broader coverage and/or higher limits than the minimums shown above, the Entity requires and shall be entitled to the broader coverage and/or the higher limits maintained by the contractor. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to the Entity.
- d. If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.
- e. Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.
- f. Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

**6. STANDARDS FOR INSURANCE COMPANIES**

Insurers, other than the California State Compensation Insurance Fund, shall have an A.M. Best's rating of at least A:VII.

**7. DOCUMENTATION**

- a. The Certificate of Insurance must include the following reference: Managed Services - Communications.
- b. All required Evidence of Insurance shall be submitted prior to the execution of this Agreement. Consultant agrees to maintain current Evidence of Insurance on file with County for the entire term of this Agreement and any additional periods if specified in Sections 1 – 4 above.
- c. The name and address for Additional Insured endorsements and Certificates of Insurance is: County of Sonoma, its Officers, Agents and Employees, Information Systems Department, 2615 Paulin Dr., Santa Rosa, CA 95403.
- d. Required Evidence of Insurance shall be submitted for any renewal or replacement of a policy that already exists, at least ten (10) days before expiration or other termination of the existing policy.
- e. Consultant shall provide immediate written notice if: (1) any of the required insurance policies is terminated; (2) the limits of any of the required policies are reduced; or (3) the deductible or self-insured retention is increased.
- f. Upon written request, certified copies of required insurance policies must be provided within thirty

(30) days.

**8. POLICY OBLIGATIONS**

Consultant's indemnity and other obligations shall not be limited by the foregoing insurance requirements.

**9. MATERIAL BREACH**

If Consultant fails to maintain insurance which is required pursuant to this Agreement, it shall be deemed a material breach of this Agreement. If Consultant is unable to secure the required insurance amounts following written notice of the material breach, County, at its sole option, may terminate this Agreement and subject to the applicable limitation on liability contained in Agreement may obtain damages from Consultant resulting from said breach. These remedies shall be in addition to any other remedies available to County.