OKLAHOMA
Office of Management
& Enterprise Services

State of Oklahoma

Office of Management and Enterprise Services

STATE OF OKLAHOMA STATEWIDE CONTRACT WITH PRESIDIO NETWORKED SOLUTIONS LLC

This State of Oklahoma Statewide Contract #1117 - LAN Managed Services & Phone System Support ("Contract") is entered into between the State of Oklahoma by and through the Office of Management and Enterprise Services ("State") and PRESIDIO NETWORKED SOLUTIONS LLC ("Supplier") and is effective as of the date of last signature to this Contract. The initial term of the Contract shall be for one (1) year with three (3) one-year options to renew.

Purpose

The State is awarding this Contract to Supplier for solutions for Local Area Network (LAN) Managed Services and Phone System Support, as more particularly described in certain Contract Documents. Supplier submitted a proposal containing exceptions to the Solicitation. This Contract memorializes the agreement of the parties with respect to the negotiated terms of the Contract that is being awarded to Supplier.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1.   The parties agree that Supplier has not yet begun performance of work under this Contract. Issuance of a purchase order is required prior to payment to a Supplier.

2.   The following Contract Documents are attached hereto and incorporated herein:

2.1.   Attachment A - Solicitation;
2.2.   Attachment B - General Terms;
2.3.   Attachment C - Statewide Contract Terms;
2.4.   Attachment D - IT Terms;
2.5.   Attachment E1 -Pricing Sheet;
2.6.   Attachment E2 – Value Add;
2.7.   Attachment E3 – Additional Bidder Terms;
2.8.   Attachment E4 - Master Terms between Bidder & State;

2.9. Attachment E5 – Third Party Information; and

2.10. Attachment F - Requested Exceptions.

3. The parties additionally agree:

3.1. Except for information deemed confidential by the State pursuant to applicable law, rule, regulation or policy, the parties agree Contract terms and information are not confidential and are disclosable without further approval of or notice to Supplier.

3.2. To the extent any term or condition in any Contract Document, including via a hyperlink or uniform resource locator, conflicts with an applicable Oklahoma and/or United States law or regulation, such term or condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, the State or Customer makes no representation or warranty regarding the enforceability of such term or condition and the State or Customer does not waive the applicable Oklahoma and/or United States law or regulation which conflicts with the term or condition.

4. The State's terms will prevail over any terms and conditions or hyperlinks included in the Supplier's Master Managed Services Agreement (MMSA). The parties may deviate from and/or override the State's terms via mutual written agreement.

5. Any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

[REMAINDER OF PAGE LEFT INTENTIONALLY BLANK]

Signatures

The undersigned represent and warrant that they are authorized, as representatives of the party on whose behalf they are signing, to sign this Contract and to bind their respective party thereto.

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES:

By: _Dan Cronin_
Dan Cronin (Feb 25, 2025 08:33 CST)

Name: Dan Cronin

Title: Chief Information Officer

Date: Feb 25, 2025

PRESIDIO NETWORKED
SOLUTIONS, LLC

By: _Keith Strohman_
Keith Strohman (Feb 24, 2025 12:08 EST)

Name: Keith Strohman

Title: Vice President

Date: Feb 24, 2025

3

Attachment E1:
STATE OF OKLAHOMA CONTRACT WITH PRESIDIO
NETWORKED SOLUTIONS LLC RESULTING FROM
SOLICITATION NO. EV00000168
PRICING SHEET

PRESIDIO

MANAGED SERVICES PRICING QUOTE

State of Oklahoma (OMES)
Phone:
Fax:
E-mail:

Quote Name: Collaboration Support-1Yr Pricing
Prepared By: DomChavez
Date Prepared: 2023-04-12
Version: 001

Contract Type	Service Level	Contract Term
New Contract	Select	1 year, 0 months

Product/Service Name	Service	DeviceType	Quantity	UnitPrice	Extension
UC Application Primary	Collaboration Services	UC ApplicationsNMs	1	$508.80	$6,106.00
UC Application Redundant	Collaboration Services	UC ApplicationsNMs	1	$289.32	$3,472.00
UC Other/Third Party (Vendor Managed)	Collaboration Services	UC ApplicationsNMs	1	$276.27	$3,315.00
Server - Non-blade, CiscoC-Series, includes host	Collaboration Services	UCServers	1	$249.40	$2,993.00
Contact Center Express Agent/ User	Collaboration Services	UC Users	1	$16.3S	$196.00
Workspace BundleUser (Call Control +Voicemail + Presence) w/MACD	Collaboration Services	UC Users	1	$4.67	$56.00
Gateway, Analog, Medium	Collaboration Services	Voice Gateways	1	$49.88	$S99.00
Voice Gateway- SIP/CUBE - Complex	Collaboration Services	Voice Gateways	1	$249.40	$2,993.00
Voice Gateway- T1/PRI/SIP - Standard	Collaboration Services	Voice Gateways	1	$149.65	$1,796.00
Cisco UCS BladeChassis	DataCenterServices	Servers and Virtualization	1	$920.88	$11,051.00
ESX Hypervisor - managed (vCenter)	DataCenterServices	Servers and Virtualization	1	$429.75	$5,157.00
Fabric Interconnects (1 pair,includes UCS Manager)	DataCenterServices	Servers and Virtualization	1	$1,702.63	$20,432.00
Carrier Case Management	Network Services	Network Devices	1	$25.00	$300.00
Network Device: Switch(Access, Branch)	Network Services	Network Devices	1	$59.72	$717.00
Network Device: Switch(Datacenter,Core)	Network Services	Network Devices	1	$151.65	$1,820.00

	Quantity	ACV	TCV	Year1	Monthly	Quarterly
Standard Recurring	**15**	**$61,000.44**	**$61,003.00**	**$61,000.44**	**$5,083.37**	**$15,250.11**
Network	*3*	*$2,836.44*	*$2,837.00*	*$2,836.44*	*$236.37*	*$709.11*
Data Center	*3*	*$36,639.12*	*$36,640.00*	*$36,639.12*	*$3,053.26*	*$9,159.78*
Collaboration	*9*	*$21,524.88*	*$21,526.00*	*$21,524.88*	*$1,793.74*	*$5,381.22*
Additional Recurring						
StandardNon-Recurring			**$10,000.00**	**$10,000.00**		
AdditionalNon-Recurring						
TOTAL	15	$61,000.44	$71,000.44	$71,000.44	$5,083.37	$15,250.11

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 SDM 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)

MYPRESIDIO

MyPresidio is a self-service portal that is providing an easy-to-use and customizable for customers' activities including shopping, ordering, maintenance contracts, and device management. MyPresidio enhances Presidio's customer experience by providing a single, integrated tool for our customers to use for automation of daily tasks.

MyPresidio key features include:

- Quote and order history

- Product catalogs

- Punchout to Cisco Commerce Website (CCW)

- Quote requests

- Automated quote approval workflows

- Maintenance contract information

- Contract and device adjustment requests

- Insight into Cisco bugs, TAC cases, and RMAs

- Self-service reporting

- Report subscriptions via email

- Punchout via cXML-compatible procurement platforms such as Ariba and Coupa

- B2B and API connections with OEMs
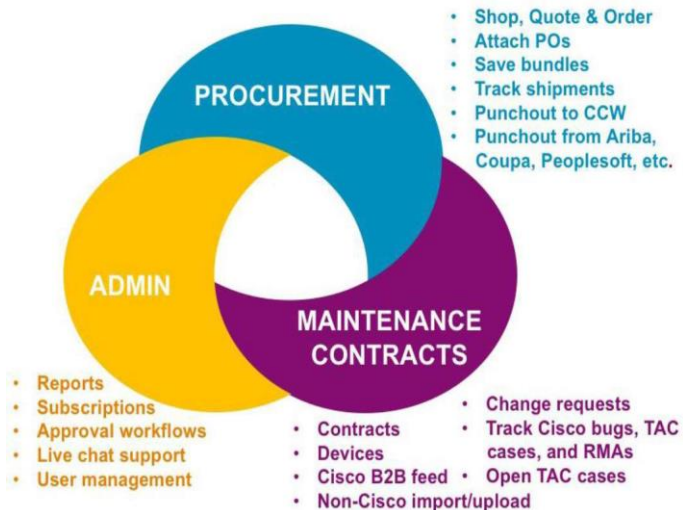
After the State's MyPresidio account is created, accessing the portal is easy at https://mypresidio.com/mypresidio.com.

Attachment E3:
**STATE OF OKLAHOMA CONTRACT WITH PRESIDIO NETWORKED SOLUTIONS
LLC RESULTING FROM SOLICITATION NO. EV00000168**
ADDITIONAL BIDDER TERMS

"Intentionally Left Blank"

Attachment E4:

STATE OF OKLAHOMA CONTRACT WITH PRESIDIO NETWORKED SOLUTIONS LLC RESULTING FROM SOLICITATION NO. EV00000168

MASTER TERMS BETWEEN BIDDER & STATE

"Intentionally Left Blank"

Attachment E5:
STATE OF OKLAHOMA CONTRACT WITH PRESIDIO NETWORKED SOLUTIONS LLC RESULTING FROM SOLICITATION NO. EV00000168
THIRD PARTY INFORMATION

"Intentionally Left Blank"

MANAGED SERVICES CONTRACT

SELECT SERVICES

INSERT CLIENT NAME

Month Day, 2021

REVISION HISTORY

Revision	Revision Date	Name	Notes
1.0	xx-xx-2021		Initial Proposal for Select Managed Services

TABLE OF CONTENTS

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
• Service Delivery Center • 7 x 24 x 365 Monitoring • Client Portal • Standard Reports • Change Management   ○ MACD (Move, Add, Change, Delete) • Problem Management • Patch Management • Dispatch Services • Vendor Management • Carrier Case Management

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. Carrier Case Management is only included in the Select tier of services

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

Service Credits

Service Credits shall be awarded beginning with the first full month following thirty (30) days of Service based on the criteria outlined below.

The service level table with credits identifies a credit equal to a percentage of MRC if the Acknowledgement, First Access Response Time and Resolution Time service levels are not met for P1s and P2s. A percentage is assigned to each category for a maximum credit of 10% of MRC per month.

Credits apply if the number of incidents allow for measurement per month.

Service Level Objectives with Service Credits

Service Level Objective	P1 🔴	P2 🟠	P3 🟡	P4 🟢
Acknowledgement Response Time* 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% (20 Incidents required)	30 minutes >90% (10 Incidents required)	4 hours >80% (5 Incidents required)	8 hours NA
SLA Penalty - Acknowledgement (% of Monthly Recurring Charge).	1% of MRC	1% of MRC	NA	NA

Service Level Objective	P1 🔴	P2 🟠	P3 🟡	P4 🟢
First Access Response Time 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% (20 Incidents required)	1 hour >90% (10 Incidents required)	8 hours >80% (5 Incidents required)	3 days NA
SLA Penalty – First Access Response (% of Monthly Recurring Charge)	2% of MRC	2% of MRC	NA	NA
Resolution Time 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% (20 Incidents required)	24 hours >90% (10 Incidents required)	3 days >80% (5 Incidents required)	14 days NA
SLA Penalty – Resolution (% of Monthly Recurring Charge)	2% of MRC	2% of MRC	NA	NA
MACD Request Completion Time 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 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, Presidio Monitoring and Operation teams 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 of Presidio's ITIL compliant Service Desk system, every component managed is defined as a configuration item in the Configuration Management Database.

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.

Inside of Presidio's ITIL compliant Service Desk system, every component managed is defined as a configuration item in the Configuration Management Database (CMDB) and all events and data are tracked back to the individual Configuration Items.

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 whether Presidio Professional Services, internal client or 3rd 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 Project 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 oversite at 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. CARRIER CASE MANAGEMENT

Presidio provides incident identification of transport issues with third-party data and voice carriers for incident remediation. This service element enables Presidio to identify and communicate carrier issues to Client for Client to provide case management with their carrier. When contracted, Presidio can manage these cases throughout the incident resolution process at an additional fee based on the number of circuits deployed; a circuit is defined as any circuit carrying data or voice into a customer premise device (Data, Voice, or Cellular). Client must provide a signed Letter of Agency (LOA) and the requisite circuit information for Presidio to manage carrier cases.

9. 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.

10. 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.

11. SERVICE DELIVERY MANAGEMENT

If ACV > $75K, include the following:

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)

If ACV between $20K and $75K, include the following :

The assigned Service Delivery Coordinator (SDC) manages client satisfaction in the delivery of IT services and provides the client a primary point of contact within Presidio Managed Services. The SDC also ensures that the team understands the various technology services that Presidio delivers to the client.

The Service Delivery Coordinator assumes responsibility for all aspects of account performance (technical, contractual, and administrative). The following are standard SDC 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
- Maintain active communication internally and externally
- Deliver remote Quarterly Business Review (QBR) to the client

If ACV < $20K, include the following:

NOC Service Delivery will manage client satisfaction in the delivery of IT services and provide client escalation within Presidio's NOC management team. The following are standard responsibilities:

- Manage Customer satisfaction
- Maintain active communication and coordinate with the client and other internal/external groups as needed for effective incident handling and change requests

- Maintain configuration management database, support documentation and any agreed upon special procedures

12. 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.

12.1. Kickoff Meeting

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

This Service Transition Management phase includes the following activities:

- Coordinating, scheduling, and executing the Kickoff Meeting.

- Reviewing deliverables included in this Managed Service Contract.

- Reviewing services purchased 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).

12.2. 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 PM develops a Project Plan for subsequent steps with distribution to project contacts. The required information must be uploaded into the Monitoring Framework. The Client is responsible for providing the information included in the Capture Template, which is provided as part of Service Transition process.

12.3. Presidio Monitoring Framework

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

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

Implementing the Monitoring Framework includes the following:

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

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

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

12.4. 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.

12.5. 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.

12.6. Remote Training Session

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

The objectives of the training session are reviews of:

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

12.7. 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 PM and the Client execute a Certificate of Acceptance, concluding the Service Transition Management phase, and the Service Delivery phase commences.

13. CLIENT RESPONSIBILITIES

13.1. 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 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:

  o Installing the DCA in a suitable equipment rack and connecting to network.

  o Power connection to Uninterruptible Power System (UPS) or other facility with continuous uninterrupted power.

  o Power-up.

  o Notification to Presidio that installation is complete.

- Provide suitable commercial power and recommends UPS or other acceptable power back-up facilities providing a minimum of 1kVA dedicated to each appliance.

13.2. Training

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

13.3. 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.

13.4. 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:

- o Points of contact and profile data
- o Change management procedures
- o Notification policy
- o 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).

13.5. 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 to 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.

13.6. 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:

  - o DCA monitoring of Managed CIs.

  - o 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.

14. 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. Pricing included in this Agreement is valid for 30 days from the date issued.

Coverage Period				
Term		Estimated Coverage Period	Start:	End:

	Billing Frequency	Amount ($) per Period

Base Managed Services	Base Annual Service Fees
Collaboration Services	$0.00
Data Center Services	$0.00
Network Services	$0.00
Service Management	$0.00
Security Services	$0.00
Workplace Services (x# of Hours @ $X/ea)	$0.00
Subtotal	$0.00

Non-Recurring Fees		
Service Transition Management	*(billed upon execution of contract)*	$0.00
	Subtotal	$0.00

Total Fees	
Year 1	$0.00
Year 2	$0.00
Year 3	$0.00
Total Contract	$

14.1. 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 Term of this SOW will automatically renew for additional one (1)-year periods unless Client terminates the SOW by providing at least 30 days' written notice before the then-current Term expiration date.

15. COVERED EQUIPMENT LIST

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

Device Type	Manufacturer	Model	Serial Number	Quantity

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") applies to only Managed Services and is wholly unrelated to and independent of any Master Product and/or Professional Services Agreement. This Agreement 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**

Client Company:		POC:	
Billing Address:		POC Phone #:	
		POC E-mail:	

2. **Scope; Coverage Period and Fees**

Presidio shall provide the services ("Services") as defined in each attached Statement of Work (each, an "SOW") and the associated Service Appendix, with respect to the software ("Software") and/or related hardware ("Hardware") (collectively, the "Equipment") referenced in the Covered Equipment List ("CEL"), and subject to Presidio's acceptance of such Equipment as eligible for Services coverage pursuant to Section 5 below. The Equipment covered by this Agreement includes only the items on the CEL. The Start of Service ("SOS") date will be specified in the SOW, provided that for service management offerings, including Presidio Support Services ("PSS") for Cisco and other vendors, the SOS begins on the date that Presidio submits a purchase order to its vendor for the underlying support contract. A PSS agreement is independent from other Presidio Managed Services, and does not necessarily co-terminate with other managed services agreements.

3. **Billing**

Immediately upon (or prior to) execution of each SOW, Client shall issue a purchase order to Presidio for the Services requested therein. Presidio will have the right to withhold performance of the Services until such time as a purchase order, issued in conformance with this Agreement, is provided by Client. Presidio will reference the purchase order number on all invoices submitted to Client. Any preprinted terms and conditions on Client's purchase order (or other forms) which are in addition to or in conflict with this Agreement shall be null and void, even if purportedly acknowledged in writing by Presidio. Presidio will bill Client as specified in each SOW. Unless otherwise specified in an SOW, recurring Services will begin billing on the earlier of: (a) forty-five (45) business days from full execution of the SOW, or (b) the SOS, as determined by Presidio and communicated to Client. Service transition management fees, as specified in the SOW, shall be billed upon full execution of this Agreement and the applicable SOW. Client shall be invoiced thirty (30) days in advance of the current Service period. Cisco Partner Shared Support(PSS) offerings will be billed in advance for the duration of that agreement, for all years of the agreement. All invoices issued under this Agreement are due thirty (30) days from the date received by Client. All past due amounts shall bear interest at the rate of one percent (1.0%) per month or, if less, the maximum permissible rate under applicable law. In addition to the charges due for the Services or otherwise hereunder, Client shall pay or reimburse Presidio for any taxes, duties, fees and/or charges resulting from Presidio's performance of this Agreement which are levied by any taxing or other governing authority, except for taxes based upon Presidio's net income. Quotes provided by Presidio are valid for 30 days from the date issued.

4. **Additional Services and Fees**

The parties recognize that from time to time, Client may request maintenance and support or other Presidio services that fall outside the scope of this Agreement. The parties will discuss any requested out-of-scope services and negotiate the terms therefor in good faith. Services specifically considered outside the scope of this Agreement include, without limitation, the following: (a) correction of errors not attributable to Presidio or the manufacturer; (b) electrical work external to the Equipment; (c) installation, de-installation, reinstallation, or relocation; (d) supplies, accessories, or attachments; (e) "no fault found" (problem with equipment not provided by Presidio and/or not covered under this Agreement): and (f) MACD volumes or other managed services in excess of the terms per the Statement of Work and associated appendices. Additionally, material services requiring more than 2 hours will be treated as billable engagements. The threshold for services considered to be "material" is based on the time required for resolution. Client will be notified before billable work is performed, and such work will not begin until authorized by Client.

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 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 termof Presidio Services being provided.

6. **Master Managed Services Agreement 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 later. 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.

REPLACE WITH CLIENT   **PRESIDIO NETWORKED SOLUTIONS LLC**

BY: _____   BY: _____

NAME: _____   NAME: _____

TITLE: _____   TITLE: _____

DATE: _____   DATE: _____

Letter of Agency

<mark>"Effective Date"</mark>

To Whom It May Concern,

Subject: Letter of Agency

The undersigned, <mark><Customer Name></mark>, 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 <mark><Customer Name></mark> 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 <mark><Customer Name></mark> 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	**Calls attempted** - A call attempt is a request from a phone/device to a PBX to initiate a call, whether that call is successful or not. Calls attempted = Calls completed + Calls rejected + other failures. **Calls completed** - A call completed is a call successfully processed by a PBX and terminated with a disconnect cause code that indicates graceful termination. Calls rejected - A rejected call is either a call attempt that is received but not processed by a PBX due to throttling when the PBX is under high load, or a call that failed due to resource limitations. **Call failures** - A failed call is a call attempt that is processed by a PBX but the call terminated abnormally with a disconnect cause code indicating that the call failed. Call failure ratio - The call failure ratio is the percentage of processed calls that failed. **Calls processed** - A processed call is a call attempt that is processed by a PBX regardless whether the call completed successfully or not. **Disconnect cause code** - The disconnect cause code indicates why a call terminated abnormally. It may be attributed to either the origination or destination device. **Report data** - 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
	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 CI's to service. Device-based backups are not performed for Monitored-Only CI's.

Presidio provides best practice recommendations to the Client in support of their Unified Communications applications backups. The Client is responsible for the configuration and storage of the backup jobs. Presidio monitors the backup services utilizing Cisco RTMT and 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
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

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 data base and Client Portal.

Management Services: Service that provides Monitoring, Incident Resolution, Reactive Problem Management, Service Level management and Standard Changes to resolve all Incidents.

Manual Cases: Cases that a system user manually opens on the Client Portal or via phone.

Manufacturer Field Notice: Electronic notification from the manufacturer about product-related issues.

Manufacturer Maintenance and Support Contract: Contractual agreement between Client and Managed Components manufacturer that grants access to manufacturer-provided services, such as Managed Element hardware replacement, software patches, and technical support, necessary to maintain good working order.

Message Bus: Connects data collected from Probes with the Management Hub**.**

Monitoring: Detecting events on Managed CIs or Monitored-Only CIs.

Monitoring Framework: Presidio's integrated technology and tools required for delivering monitoring and managed services.

Monitored-Only CI: CI monitored by Monitoring Framework but not fully managed by Presidio Managed Services.

Patch: Small fix to a problem using a piece of software code.

Problem: Underlying cause of one or more Incidents.

Problem Analysis: Investigating problems to determine root cause.

Problem Management: Process to find and resolve the root cause of a Problem and prevention of Incidents.

Service Addendum: Bilaterally agreed to document modifying scope of agreement.

Service 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) is 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**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 data base and Client Portal.

Management Services: Service that provides Monitoring, Incident Resolution, Reactive Problem Management, Service Level management and Standard Changes to resolve all Incidents.

Manual Cases: Cases that a system user manually opens on the Client Portal or via phone.

Manufacturer Field Notice: Electronic notification from the manufacturer about product-related issues.

Manufacturer Maintenance and Support Contract: Contractual agreement between Client and Managed Components manufacturer that grants access to manufacturer-provided services, such as Managed Element hardware replacement, software patches, and technical support, necessary to maintain good working order.

Message Bus: Connects data collected from Probes with the Management Hub**.**

Monitoring: Detecting events on Managed CIs or Monitored-Only CIs.

Monitoring Framework: Presidio's integrated technology and tools required for delivering monitoring and managed services.

Monitored-Only CI: CI monitored by Monitoring Framework but not fully managed by Presidio Managed Services.

Patch: Small fix to a problem using a piece of software code.

Problem: Underlying cause of one or more Incidents.

Problem Analysis: Investigating problems to determine root cause.

Problem Management: Process to find and resolve the root cause of a Problem and prevention of Incidents.

Service Addendum: Bilaterally agreed to document modifying scope of agreement.

Service 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) is 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.

Attachment F to
STATE OF OKLAHOMA CONTRACT WITH PRESIDIO NETWORKED SOLUTIONS
LLC. RESULTING FROM SOLICITATION NO. EV00000168
Negotiated Exceptions and Additional Terms to the Contract

The Contract is hereby amended to include the terms as set forth below and supersedes all prior terms and exceptions submitted by **PRESIDIO NETWORKED SOLUTIONS LLC.** or discussed by the parties.

Requested Exceptions and Additional Terms not addressed below are declined by the State of Oklahoma.

Section	Exception
Attachment B, Section 2.2 Contract Effectiveness and Order of Priority	**The originally placed paragraph shall be modified and replaced with the following:** A. any Addendum; B. any applicable Solicitation as shown in Attachment A; C. any Contract-specific terms contained in a Contract Document including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract; D. the terms contained in this Contract Document; E. any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation as shown in Attachment A or applicable law; F. any statement of work, work order, or other similar ordering document as applicable; and G. other mutually agreed Contract Documents.
Attachment B, Section 6.2 Ordering, Inspection, and Acceptance	**The originally placed paragraph shall be modified and replaced with the following:** Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. The services will have a warranty period of 90 days from acceptance. Notwithstanding any other provision in the Contract,

Section	Exception
	deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service. Supplier warrants and represents that a product or deliverable furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, be substantially uninterrupted and error-free in operation and guaranteed against faulty material and workmanship for the warranty period maximum allowed by the manufacturer. A defect in a product or deliverable furnished by or through the Supplier shall be repaired or replaced by Supplier at no additional cost or expense to the Customer if such defect occurs during the warranty period. To the extent Supplier provides a third party product, the warranties given by the manufacturer will be provided, Supplier makes no independent warranties. Except as expressly provided in this agreement, Supplier makes no warranties express or implied and specifically disclaims any warranty or merchantability, fitness for a particular purpose, or any warranty arising by usage or trade course of dealings or course of performance.
Attachment B, Section 16.5 Limitation of Liability	**The originally placed paragraph shall be modified and replaced with the following:** A. With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier, and Supplier shall not be liable to the State or any Customer, for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages. Except for Supplier's liability for Data Security Incidents addressed in Section 16.5(B), Supplier's liability for damages of any kind to the State or any Customer shall be limited to the total amount paid to Supplier under this Contract during the twelve months immediately preceding accrual of the claim or cause of action or $20,000,000 whichever is lesser B. Supplier's liability for unauthorized access to, unauthorized disclosure, transfer, or processing of, damage to, or loss, destruction, alteration, or corruption of any data arising from any act or omission of Supplier including but not limited to Supplier breach of data security obligations (collectively, "Data Security Incidents") shall not exceed $20,000,000. For avoidance of doubt, Section 16.5(C) shall not be construed to negate or otherwise render unenforceable the damages limitations applicable to Data Security Incidents set forth in this Section 16.5(B). C. Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to

Section	Exception
	property damage, bodily injury or death caused by Supplier or its employees, agents or subcontractors; indemnity, security or confidentiality obligations under the Contract; the bad faith, negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors. D. The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.
12.1 Intellectual Property Ownership	**The originally placed paragraph shall be modified and replaced with the following:** As between Supplier and Customer, the Work Product and Intellectual Property Rights therein are and shall be owned exclusively by Customer, excluding Supplier's Background IP, and not Supplier. Supplier specifically agrees that the Work Product shall be considered "works made for hire" and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier hereby agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is hereby effectively transferred, granted, conveyed, assigned and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third-Party Intellectual Property, except as may be incorporated in the Work Product by Supplier. Notwithstanding the foregoing Supplier or it's third-party manufacturer as applicable, retains all ownership and intellectual property rights in its Background IP. Background IP means all object code, Third Party Software, technology, systems, strategies, processes, methods, techniques, ideas, experience, information, know-how, patents, trademarks, copyrights, designs, development, or other proprietary rights that are used or delivered by Supplier hereunder, whether pre-existing or conceived, created, or developed by Supplier outside the scope of this

Section	Exception
	Agreement, whether embodied or otherwise encompassed in the Work Product and including all improvements or derivatives thereof.
12.7 Intellectual Property Ownership	**The originally placed paragraph shall be modified and replaced with the following:** Customer hereby grants to Supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any Work Product solely as necessary to provide services to Customer. Supplier shall not use any of the Customer's intellectual property rights or confidential information in connection with the provision of services to its other customers.
Appendix 1 - B.4 Data Security	**The originally placed paragraph shall be modified and replaced with the following:** Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier, may allow its personnel, or contractors to store Customer Data on portable devices, including personal computers, including for devices that are used and kept only in the United States provided that Supplier accepts responsibility for security of said Data . Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.
Appendix 2 to the State of Oklahoma Information Technology Terms CJIS Security Policy Requirements Generally	**The following paragraph shall be added to the beginning of the pertinent section:** Both parties acknowledge that PRESIDIO NETWORKED SOLUTIONS, LLC will not take possession or control of CJIS (Criminal Justice Information) data in performance of this contract. However, the following language will be applicable if PRESIDIO NETWORKED SOLUTIONS, LLC agrees to take possession or control of CJIS data in performance of this contract in the future and only with an updated Master Service Agreement or Statement of Work agreed to by both parties.

ATTACHMENT A
EVENT NO. EV00000168

This Solicitation is a Contract Document and is a request for proposal in connection with the Contract awarded by the Office of Management and Enterprise Services as more particularly described below. Any defined term used herein but not defined herein shall have the meaning ascribed in the General Terms or other Contract Document.

PURPOSE

The Contract is awarded as a statewide contract for solutions for Local Area Network (LAN) Managed Services and Phone System Support.

1.   Contract Term and Renewal Options
        The initial Contract term, which begins on the effective date of the Contract, is one year and there are three one-year options to renew the Contract.

2. Certain Contract requirements and terms are attached hereto as Exhibit 1 and Exhibit 2 and incorporated herein.

   Exhibit 1: Contract Requirements

   Exhibit 2: Pricing Sheet

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

This State of Oklahoma General Terms ("General Terms") is a Contract Document in connection with a Contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma.

In addition to other terms contained in an applicable Contract Document, Supplier and State agree to the following General Terms:

1   Scope and Contract Renewal

1.1   Supplier may not add products or services to its offerings under the Contract without the State's prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.

1.2   At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.

1.3   If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier's performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract Documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by Supplier; and c) current products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an Addendum. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request.

1.4   The State may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period. If the State exercises such option to extend ninety (90) days, the State shall notify the

Supplier in writing prior to Contract end date. The State, at its sole option and to the extent allowable by law, may choose to exercise subsequent ninety (90) day extensions at the Contract pricing rate, to facilitate the finalization of related terms and conditions of a new award or as needed for transition to a new Supplier.

1.5   Supplier understands that supplier registration expires annually and, pursuant to OAC 260:115-3-3, Supplier shall maintain its supplier registration with the State as a precondition to a renewal of the Contract.

2   Contract Effectiveness and Order of Priority

2.1   Unless specifically agreed in writing otherwise, the Contract is effective upon the date last signed by the parties. Supplier shall not commence work, commit funds, incur costs, or in any way act to obligate the State until the Contract is effective.

2.2   Contract Documents shall be read to be consistent and complementary. Any conflict among the Contract Documents shall be resolved by giving priority to Contract Documents in the following order of precedence:

A.   any Addendum;

B.   any applicable Solicitation;

C.   any Contract-specific terms contained in a Contract Document including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;

D.   the terms contained in this Contract Document;

E.   any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law;

F.   any statement of work, work order, or other similar ordering document as applicable; and

G.   other mutually agreed Contract Documents.

2.3   If there is a conflict between the terms contained in this Contract Document or in Contract-specific terms and an agreement provided by or on behalf of Supplier including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms provided by Supplier shall not take priority over this Contract Document or

Acquisition-specific terms. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Addendum.

2.4   Any Contract Document shall be legibly written in ink or typed. All Contract transactions, and any Contract Document related thereto, may be conducted by electronic means pursuant to the Oklahoma Uniform Electronic Transactions Act.

3   **Modification of Contract Terms and Contract Documents**

3.1   The Contract may only be modified, amended, or expanded by an Addendum. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Supplier, is a material breach of the Contract. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the Supplier shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.

3.2   Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a Customer other than OMES in connection with an Acquisition.

4   **Definitions**

In addition to any defined terms set forth elsewhere in the Contract, the Oklahoma Central Purchasing Act and the Oklahoma Administrative Code, Title 260, the parties agree that, when used in the Contract, the following terms are defined as set forth below and may be used in the singular or plural form:

4.1   **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.

4.2   **Addendum** means a mutually executed, written modification to a Contract Document.

4.3   **Amendment** means a written change, addition, correction or revision to the Solicitation.

4.4   **Bid** means an offer a Bidder submits in response to the Solicitation.

4.5 **Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.

4.6 **Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract Documents and an appropriate encumbering document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.

4.7 **Contract Document** means this document; any master or enterprise agreement terms entered into between the parties that are mutually agreed to be applicable to the Contract; any Solicitation; any Contract-specific terms; any Supplier's Bid as may be negotiated; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents and any Addendum.

4.8 **Customer** means the entity receiving goods or services contemplated by the Contract.

4.9 **Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.

4.10 **Destination** means delivered to the receiving dock or other point specified in the applicable Contract Document.

4.11 **Indemnified Parties** means the State and Customer and/or its officers, directors, agents, employees, representatives, contractors, assignees and designees thereof.

4.12 **Inspection** means examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.

4.13 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.

4.14 **OAC** means the Oklahoma Administrative Code.

4.15 **OMES** means the Office of Management and Enterprise Services.

4.16 **Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.

4.17 **State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.

4.18 **Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State.

4.19 **Suspension** means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act.

4.20 **Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.

4.21 **Work Product** means any and all deliverables produced by Supplier under a statement of work or similar Contract Document issued pursuant to this Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (vii) all Intellectual Property Rights in any of the foregoing, and which are or were created,

prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

5   Pricing

5.1   Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.

5.2   Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.

5.3   The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6   Ordering, Inspection, and Acceptance

6.1   Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.

6.2   Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service.

Supplier warrants and represents that a product or deliverable furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, be substantially uninterrupted and error-free in operation and guaranteed against faulty material and workmanship for a warranty period of the greater of ninety (90) days from the date of acceptance or the maximum allowed by the manufacturer. A defect in a product or deliverable furnished by or through the Supplier shall be repaired or replaced by Supplier at no additional cost or expense to the Customer if such defect occurs during the warranty period.

Any product to be delivered pursuant to the Contract shall be subject to final inspection and acceptance by the Customer at Destination. The Customer assumes no responsibility for a product until accepted by the Customer. Title and risk of loss or damage to a product shall be the responsibility of the Supplier until accepted. The Supplier shall be responsible for filing, processing, and collecting any and all damage claims accruing prior to acceptance.

Pursuant to OAC 260:115-9-5, payment for an Acquisition does not constitute final acceptance of the Acquisition. If subsequent inspection affirms that the Acquisition does not meet or exceed the specifications of the order or that the Acquisition has a latent defect, the Supplier shall be notified as soon as is reasonably practicable. The Supplier shall retrieve and replace the Acquisition at Supplier's expense or, if unable to replace, shall issue a refund to Customer. Refund under this section shall not be an exclusive remedy.

6.3   Supplier shall deliver products and services on or before the required date specified in a Contract Document. Failure to deliver timely may result in liquidated damages as set forth in the applicable Contract Document. Deviations, substitutions, or changes in a product or service, including changes of personnel directly providing services, shall not be made unless expressly authorized in writing by the Customer. Any substitution of personnel directly providing services shall be a person of comparable or greater skills, education and experience for performing the services as the person being replaced. Additionally, Supplier shall provide staff sufficiently experienced and able to perform with respect to any transitional services provided by Supplier in connection with termination or expiration of the Contract.

6.4   Product warranty and return policies and terms provided under any Contract Document will not be more restrictive or more costly than warranty and return policies and terms for other similarly situated customers for a like product.

7   Invoices and Payment

7.1   Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted.

The following terms additionally apply:

A.   An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.

B.   Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment.   Proper invoice is defined at OAC 260:10-1-2.

C.   Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.

D.   The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.

E.   If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.

F.   Supplier shall have no right of setoff.

G.   Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.

H.   The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

8   Maintenance of Insurance, Payment of Taxes, and Workers' Compensation

8.1   As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set

forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.

Such proof of coverage shall additionally be provided to the Customer if services will be provided by any of Supplier's employees, agents or subcontractors at any Customer premises and/or employer vehicles will be used in connection with performance of Supplier's obligations under the Contract. Supplier may not commence performance hereunder until such proof has been provided. Additionally, Supplier shall ensure each insurance policy includes a thirty (30) day notice of cancellation and name the State and its agencies as certificate holder and shall promptly provide proof to the State of any renewals, additions, or changes to such insurance coverage. Supplier's obligation to maintain insurance coverage under the Contract is a continuing obligation until Supplier has no further obligation under the Contract. Any combination of primary and excess or umbrella insurance may be used to satisfy the limits of coverage for Commercial General Liability, Auto Liability and Employers' Liability. Unless agreed between the parties and approved by the State Purchasing Director, the minimum acceptable insurance limits of liability are as follows:

A. Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;

B. Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than $5,000,000 per occurrence;

C. Automobile Liability Insurance with limits of liability of not less than $5,000,000 combined single limit each accident;

D. Directors and Officers Insurance which shall include Employment Practices Liability as well as Consultant's Computer Errors and Omissions Coverage, if information technology services are provided under the Contract, with limits not less than $5,000,000 per occurrence;

E. Security and Privacy Liability insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits $5,000,000 per occurrence; and

F. Additional coverage required in writing in connection with a particular Acquisition.

8.2 Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.

8.3 Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) relating to tax liability, unemployment insurance and/or Workers' Compensation in connection with its performance under the Contract.

9   Compliance with Applicable Laws

9.1 As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:

A.   Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.

B.   Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;

C.   Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters;

D.   1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;

E.   Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;

F. Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein);

G. Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity;

H. Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at **www.dhs.gov/E-Verify**;

I. Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and

J. Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.

9.2 The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at https://omes.ok.gov/sites/g/files/gmc316/f/InfoSecPPG_0.pdf. Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.

9.3 At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.

9.4 In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory

contract provisions required in connection with the receipt of federal funds or other funding source.

9.5 The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.

9.6 As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.

9.7 The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.

9.8 Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or appointment of a receiver, liquidator or trustee.

9.9 Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.

9.10 If services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents are compliant with Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents be non-compliant, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non-electronic format, Supplier shall promptly provide such communication and any associated support documents in an alternate format

usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

10   Audits and Records Clause

10.1   As used in this clause and pursuant to 67 O.S. §203, "record" includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.

10.2   The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.

10.3   Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director.

11   Confidentiality

11.1   The Supplier shall maintain strict security of all State and citizen data and records entrusted to it or to which the Supplier gains access, in accordance with and subject to applicable federal and State laws, rules, regulations, and policies and shall use any such data and records only as necessary for Supplier to perform its obligations under the Contract. The Supplier further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. The Supplier warrants and represents that such information shall not be sold, assigned, conveyed, provided, released, disseminated or otherwise disclosed by Supplier, its employees, officers, directors, subsidiaries, affiliates, agents, representatives, assigns, subcontractors, independent contractors, successor or any other persons or entities without Customer's prior express written

permission. Supplier shall instruct all such persons and entities that the confidential information shall not be disclosed or used without the Customer's prior express written approval except as necessary for Supplier to render services under the Contract. The Supplier further warrants that it has a tested and proven system in effect designed to protect all confidential information.

11.2 Supplier shall establish, maintain and enforce agreements with all such persons and entities that have access to State and citizen data and records to fulfill Supplier's duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the Customer.

11.3 Supplier shall immediately report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonable should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.

11.4 Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.

11.5 Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents,

representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

11.6 The Supplier shall immediately forward to the State Purchasing Director, and any other applicable person listed in the Notices section(s) of the Contract, any request by a third party for data or records in the possession of the Supplier or any subcontractor or to which the Supplier or subcontractor has access and Supplier shall fully cooperate with all efforts to protect the security and confidentiality of such data or records in response to a third party request.

11.7 Customer may be provided access to Supplier Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this section. Nothing herein is intended to waive the State Purchasing Director's authority under OAC 260:115-3-9 in connection with Bid information requested to be held confidential by a Bidder. Notwithstanding the foregoing, Supplier Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use or otherwise and is not in contravention of this Contract; (ii) is known and has been reduced to tangible form by the receiving party before the time of disclosure for the first time under this Contract and without other obligations of confidentiality; (iii) is independently developed without the use of any of Supplier Confidential Information; (iv) is lawfully obtained from a third party (without any confidentiality obligation) who has the right to make such disclosure or (v) résumé, pricing or marketing materials provided to the State. In addition, the obligations in this section shall not apply to the extent that the applicable law or regulation requires disclosure of Supplier Confidential Information, provided that the Customer provides reasonable written notice, pursuant to Contract notice provisions, to the Supplier so that the Supplier may promptly seek a protective order or other appropriate remedy.

12   Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Prompt disclosure is required under this section if the activity or interest is

related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an obligation under the Contract, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

13   Assignment and Permitted Subcontractors

13.1   Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.

13.2   Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.

13.3   If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Prior to a subcontractor being utilized by the Supplier, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Such approval is within the sole discretion of the State. Any proposed subcontractor shall be identified by entity name, and by employee name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to

the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract Documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

13.4 All payments under the Contract shall be made directly to the Supplier, except as provided in subsection A above regarding the Supplier's assignment of payment. No payment shall be made to the Supplier for performance by unapproved or disapproved employees of the Supplier or a subcontractor.

13.5 Rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred, at no additional cost, to other Customer entities.

14 Background Checks and Criminal History Investigations

Prior to the commencement of any services, background checks and criminal history investigations of the Supplier's employees and subcontractors who will be providing services may be required and, if so, the required information shall be provided to the State in a timely manner. Supplier's access to facilities, data and information may be withheld prior to completion of background verification acceptable to the State. The costs of additional background checks beyond Supplier's normal hiring practices shall be the responsibility of the Customer unless such additional background checks are required solely because Supplier will not provide results of its otherwise acceptable normal background checks; in such an instance, Supplier shall pay for the additional background checks. Supplier will coordinate with the State and its employees to complete the necessary background checks and criminal history investigations. Should any employee or subcontractor of the Supplier who will be providing services under the Contract not be acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or services.

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third party threaten or make a claim that any portion of a product or service provided by Supplier under the Contract infringes that party's patent, intellectual property,

copyright or other property right, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of a service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier.

16   Indemnification

16.1   Acts or Omissions

A.   Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising out of, or resulting from any action or claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the execution or performance of the Contract.

B.   To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer due to negligence, misconduct, wrongful act, or omission on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such amount shall be invoiced to, and is payable by, Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

16.2   Infringement

Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from or in connection with Supplier's breach of its representations and warranties in the Contract or alleged infringement of any patent, intellectual property, copyright or other property right in connection with a product or service provided under the Contract. Supplier's duty under this section is reduced to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or third party to a product delivered under the Contract or combinations of the product with any non-Supplier-provided services or products unless Supplier recommended or participated in such modification or combination; (c) use of a product or service by Customer in violation of the Contract unless done so at the direction of Supplier, or (d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system.

16.3   Notice and Cooperation

In connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim. Any Customer affected by the claim will reasonably cooperate with Supplier and defense of the claim to the extent its interests are aligned with Supplier. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim against Indemnified Parties that are not a State agency, where relief against the Indemnified Parties is limited to monetary damages that are paid by the defending party under indemnification provisions of the Contract.

16.4   Coordination of Defense

In connection with indemnification obligations under the Contract, when a State agency is a named defendant in any filed or threatened lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally

participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

16.5   Limitation of Liability

A.   With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.

B.   Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to property damage, bodily injury or death caused by Supplier or its employees, agents or subcontractors; indemnity, security or confidentiality obligations under the Contract; the bad faith, negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors.

C.   The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

17   Termination for Funding Insufficiency

17.1   Notwithstanding anything to the contrary in any Contract Document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

17.2   Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contractor certain obligations are terminated shall be refunded.

17.3   The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

18   Termination for Cause

18.1   Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.

18.2   The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract; (ii) Supplier's material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.

18.3   Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence

of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

18.4 The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual or anticipated failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-9 is an example.

19   Termination for Convenience

19.1 The State may terminate the Contract, in whole or in part, for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days' written notice of termination. Any partial termination of the Contract shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that remain in effect.

19.2 Upon receipt of notice of such termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but

there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

20 Suspension of Supplier

20.1 Supplier may be subject to Suspension without advance notice and may additionally be suspended from activities under the Contract if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract.

20.2 Upon receipt of a notice pursuant to this section, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to receipt of notice by Supplier, the Suspension does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract during a period of Suspension or suspended activity or for any damages or other amounts caused by or associated with such Suspension or suspended activity. A right exercised under this section shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.

20.3 Such Suspension may be removed, or suspended activity may resume, at the earlier of such time as a formal notice is issued that authorizes the resumption of performance under the Contract or at such time as a purchase order or other appropriate encumbrance document is issued. This subsection is not intended to operate as an affirmative statement that such resumption will occur.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract.

A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22   Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Supplier certifies that no person involved in any manner in development of the Contract employed by the State shall be employed to fulfill any services provided under the Contract.

23   Force Majeure

23.1   Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other similar casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.

23.2   Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. However, a purchase order or other payment mechanism may be terminated if Supplier cannot cause delivery of a product or service in a timely manner to meet the business needs of Customer. Supplier is not entitled to payment for products or services not received and, therefore, amounts payable to Supplier during the force majeure event shall be equitably adjusted downward.

23.3   Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay

or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

24   Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession, regardless of cause. If Supplier fails to comply with Customer's security requirements, Supplier is subject to immediate suspension of work as well as termination of the associated purchase order or other payment mechanism.

25   Notices

All notices, approvals or requests allowed or required by the terms of any Contract Document shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the physical address set forth below. Notice information may be updated in writing to the other party as necessary. Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall not be delivered solely via e-mail.

If sent to the State:
State Purchasing Director
2401 N. Lincoln Blvd., Suite 116
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:
Purchasing Division Deputy General Counsel
2401 N. Lincoln Blvd., Suite 116
Oklahoma City, Oklahoma 73105

26   Miscellaneous

26.1   Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract Documents, in the singular or in the aggregate, shall be governed by the laws of the State without regard to application of choice of law principles. Pursuant to 74 O.S. §85.14, where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma.

26.2 No Guarantee of Products or Services Required

The State shall not guarantee any minimum or maximum amount of Supplier products or services required under the Contract.

26.3 Employment Relationship

The Contract does not create an employment relationship. Individuals providing products or performing services pursuant to the Contract are not employees of the State or Customer and, accordingly are not eligible for any rights or benefits whatsoever accruing to such employees.

26.4 Transition Services

If transition services are needed at the time of Contract expiration or termination, Supplier shall provide such services on a month-to-month basis, at the contract rate or other mutually agreed rate. Supplier shall provide a proposed transition plan, upon request, and cooperate with any successor supplier and with establishing a mutually agreeable transition plan. Failure to cooperate may be documented as poor performance of Supplier.

26.5 Publicity

The existence of the Contract or any Acquisition is in no way an endorsement of Supplier, the products or services and shall not be so construed by Supplier in any advertising or publicity materials. Supplier agrees to submit to the State all advertising, sales, promotion, and other publicity matters relating to the Contract wherein the name of the State or any Customer is mentioned or language used from which, in the State's judgment, an endorsement may be inferred or implied. Supplier further agrees not to publish or use such advertising, sales promotion, or publicity matter or release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the Contract or any Acquisition hereunder without obtaining the prior written approval of the State.

26.6 Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 *et seq*. Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required.

26.7 Failure to Enforce

Failure by the State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract Document, or any part thereof, or the right of the State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract Document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.

26.8 Mutual Responsibilities

A.   No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.

B.   The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.

C.   The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved.

D.   The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract.

E.   Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

26.9 Invalid Term or Condition

To the extent any term or condition in the Contract conflicts with a compulsory applicable State or United States law or regulation, such Contract term or

condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable State or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.

26.10 Severability

If any provision of a Contract Document, or the application of any term or condition to any party or circumstances, is held invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable and the application of such provision to other parties or circumstances shall remain valid and in full force and effect. If a court finds that any provision of this contract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

26.11 Section Headings

The headings used in any Contract Document are for convenience only and do not constitute terms of the Contract.

26.12 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State.

26.13 Survival

As applicable, performance under all license, subscription, service agreements, statements of work, transition plans and other similar Contract Documents entered into between the parties under the terms of the Contract shall survive Contract expiration. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.

26.14 Entire Agreement

The Contract Documents taken together as a whole constitute the entire agreement between the parties. No statement, promise, condition,

understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract Document shall be binding or valid. The Supplier's representations and certifications, including any completed electronically, are incorporated by reference into the Contract.

26.15 Gratuities

The Contract may be immediately terminated, in whole or in part, by written notice if it is determined that the Supplier, its employee, agent, or another representative violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.

26.16 Import/Export Controls

Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under the Contract (even if incorporated into other products) except in compliance with all applicable import and export laws, conventions and regulations.

ATTACHMENT C

OKLAHOMA STATEWIDE CONTRACT TERMS

1. **Statewide Contract Type**

   1.1   The Contract is a non-mandatory statewide contract for use by State agencies. Additionally, the Contract may be used by any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claims Act including any associated institution, instrumentality, board, commission, committee, department or other entity designated to act on behalf of the political subdivision; a state, county or local governmental entity in its state of origin; and entities authorized to utilize contracts by the State via a multistate or multigovernmental contract.

   1.2   The Contract is a firm, fixed price contract for indefinite delivery and quantity for the Acquisitions available under the Contract.

2. **Orders and Addendums**

   2.1   Unless mutually agreed in writing otherwise, orders shall be placed directly with the Supplier by issuance of written purchase orders or by Purchase Card by state agencies and other authorized entities. All orders are subject to the Contract terms and any order dated prior to Contract expiration shall be performed. Delivery to multiple destinations may be required.

   2.2   Any ordering document shall be effective between Supplier and the Customer only and shall not be an Addendum to the Contract in its entirety or apply to any Acquisition by another Customer.

   2.3   Additional terms added to a Contract Document by a Customer shall be effective if the additional terms do not conflict with the General Terms and are acceptable to Supplier. However, an Addendum to the Contract shall be signed by the State Purchasing Director or designee. Regarding information technology and telecommunications contracts, pursuant to 62 O.S., §34.11.1, the Chief Information Officer acts as the Information Technology and Telecommunications Purchasing Director.

3. **Termination for Funding Insufficiency**

In addition to Contract terms relating to termination due to insufficient funding, a Customer may terminate any purchase order or other payment mechanism if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. The determination by the Customer of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

4. **Termination for Cause**

In addition to Contract terms relating to termination for cause, a customer may terminate its obligations, in whole or in part, to Supplier if it has provided Supplier with written notice of material breach and Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. The Customer may also terminate a purchase order or other payment mechanism or Supplier's activities under the Contract immediately without a thirty (30) day written notice to Supplier, if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements if such non-compliance relates or may relate to Supplier provision of products or services to the Customer or if Supplier's material breach is reasonably determined (i) to be an impediment to the function of the Customer and detrimental to the Customer, or (ii) when conditions preclude the thirty (30) day notice.

5. **Termination for Convenience**

In addition to any termination for convenience provisions in the Contract, a Customer may terminate a purchase order or other payment mechanism for convenience if it is determined that termination is in the Customer's best interest. Supplier will be provided at least thirty (30) days' written notice of termination.

6. **Contract Management Fee and Usage Report**

6.1 Pursuant to 74 O.S. § 85.33A, the State assesses a contract management fee on all transactions under a statewide contract. The payment of such fee will be calculated for all transactions, net of returns and the Supplier has no right of setoff against such fee regardless of the payment status of any Customer or any aggregate accounts receivable percentage. Supplier acknowledges and agrees that all prices quoted under any statewide contract shall include the contract management fee and the contract

management fee shall not be reflected as a separate line item in Supplier's billing. The State reserves the right to change this fee upward or downward upon sixty (60) calendar days' written notice to Supplier without further requirement for an Addendum.

6.2 While Supplier is the awardee of a statewide contract, transactions that occur under the terms of the statewide contract are subject to a one percent (1%) contract management fee to be paid by Supplier. Supplier shall submit a Contract Usage Report on a quarterly basis for each contract using a form provided by the State and such report shall include applicable information for each transaction. Reports shall include usage of the statewide contract by every Customer during the applicable quarter. A singular report provided late will not be considered a breach of the statewide contract; provided, however, repeated failure to submit accurate quarterly usage reports and submit timely payments may result in suspension or termination, in whole or in part, of the Contract.

6.3 All Contract Usage Reports shall meet the following criteria:

i. Electronic submission in Microsoft Excel format to **strategic.sourcing@omes.ok.gov**;

ii. Quarterly submission regardless of whether there were transactions under the Contract during the applicable quarterly reporting period;

iii. Submission no later than forty-five (45) days following the end of each calendar quarter;

iv. Contract quarterly reporting periods shall be as follows:

a. January 01 through March 31;

b. April 01 through June 30;

c. July 01 through September 30; and

d. October 01 through December 31.

v. Reports must include the following information:

a.	Procuring entity;
b.	Order date;
c.	Purchase Order number or note that the transaction was paid by Purchase Card;
d.	City in which products or services were received or specific office or subdivision title;
e.	Product manufacturer or type of service;
f.	Manufacturer item number, if applicable;
g.	Product description;
h.	General product category, if applicable;
i.	Quantity;
j.	Unit list price or MSRP, as applicable;
k.	Unit price charged to the purchasing entity; and
l.	Other Contract usage information requested by the State.

6.4 Payment of the contract management fee shall be delivered to the following address within forty-five (45) calendar days after the end of each quarterly reporting period:

State of Oklahoma
Office of Management and Enterprise Services, Central Purchasing
2401 North Lincoln Boulevard, Suite 118
Oklahoma City, Oklahoma 73105

To ensure payment is properly accounted for, Supplier shall provide the following information with payment: (i) reference to the applicable Contract Usage Report and quarterly reporting period and (ii) the applicable statewide contract number(s) and the amount of the contract management fee being paid for each contract number.

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

The parties further agree to the following terms ("Information Technology Terms"), as applicable, for any Acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, OMES-Information Services ("OMES-IS") is designated to purchase information technology and telecommunication products and services on behalf of the State. The Act directs OMES-IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the owner of information technology and telecommunication assets and contracts on behalf of the State, allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier. OMES-IS is the data custodian for State agency data; however, such data is owned by the respective State agency.

1 Definitions

1.1 **COTS** means software that is commercial off the shelf.

1.2 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier.

1.3 **Data Breach** means the unauthorized access by an unauthorized person that results in the use, disclosure or theft of Customer Data.

1.4 **Host** includes the terms **Hosted** or **Hosting** and means the accessing, processing or storing of Customer Data.

1.5 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, Moral Rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.

1.6 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.

1.7 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential

by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

1.8   **Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) data subject to protection under a federal, state or local law, rule, regulation or ordinance.

1.9   **Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the Hosted environment used to perform the services.

1.10   **State CIO** means the State Chief Information Officer or authorized designee.

1.11   **Supplier Intellectual Property** means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier and identified in writing as such (a) prior to providing any services or Work Product to Customer and prior to receiving any documents, materials, information or funding from or on behalf of a Customer relating to the services or Work Product, or (b) after the effective date of the Contract if such tangible or intangible items or things were independently developed by Supplier outside Supplier's provision of services or Work Product for Customer under the Contract and were not created, prepared, developed, invented or conceived by any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

1.12   **Third Party Intellectual Property** means the Intellectual Property Rights of any third party that is not a party to the Contract, and that is not directly or indirectly providing any goods or services to a Customer under the Contract.

1.13   **Work Product** means any and all deliverables produced by Supplier for Customer under a statement of work issued pursuant to the Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the effective date of the Contract, including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (i) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts,

personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided to Customer under the Contract or statement of work, and (vii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or a statement of work, or with funds appropriated by or for Customer or Customer's benefit: (a) by any Supplier personnel or Customer personnel, or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to- practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

2   Termination of Maintenance and Support Services

Customer may terminate maintenance or support services without an adjustment charge, provided any of the following circumstances occur:

2.1   Customer removes the product for which the services are provided, from productive use or;

2.2   The location at which the services are provided is no longer controlled by Customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).

If Customer chooses to renew maintenance or support after maintenance has lapsed, Customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Any amount paid to Supplier in the form of prepaid fees that are unused when services under the Contract or purchase order are terminated shall be refunded to Customer.

3   Compliance and Electronic and Information Technology Accessibility

State procurement of information technology is subject to certain federal and State laws, rules and regulations related to information technology accessibility, including but not limited to Oklahoma Information Technology Accessibility Standards ("Standards") set forth at https://oklahoma.gov/omes/services/information-services/is/policies-and-standards/accessibility-standards.html. Supplier shall provide a Voluntary Product Accessibility Template ("VPAT") describing accessibility compliance via a URL linking to the VPAT and shall update the VPAT as necessary in order to allow a Customer to obtain current VPAT information as required by State law. If products require development or customization, additional requirements and documentation may be required, and compliance shall be necessary by Supplier. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, purchase order or Addendum.

All representations contained in the VPAT provided will be relied upon by the State or a Customer, as applicable, for accessibility compliance purposes.

4 Media Ownership (Disk Drive and/or Memory Chip Ownership)

4.1 Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the property of the Customer.

4.2 Personal information may be retained within electronic media devices and components; therefore, electronic media shall not be released either between Customers or for the resale, of refurbished equipment that has been in use by a Customer, by the Supplier to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied by Supplier, its agents or subcontractors during the downtime (repair) of products purchased or leased through the Contract. If a device is removed from a location for repairs, the Customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information that may be stored within the hard drive or memory of the device.

5 Offshore Services

No offshore services are provided for under the Contract. State data shall not be used or accessed internationally for troubleshooting or any other use not specifically provided for herein without the prior written permission, which may be withheld in the State's sole discretion, from the appropriate authorized representative of the State. Notwithstanding the above, back office administrative functions of the Supplier may be located offshore and the follow-the-sun support model may be used by the Supplier to the extent allowed by law applicable to any Customer data being accessed or used.

6 Compliance with Technology Policies

6.1 The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf.

Supplier's employees and subcontractors shall adhere to the applicable State IT Standard Methodologies and Templates including but not limited to Project Management, Business Analysis, System Analysis, Enterprise and IT Architecture, Quality, Application and Security Methodologies and Templates as set forth at https://oklahoma.gov/omes/services/information-services/is/policies-and-standards.html

6.2 Supplier shall comply with applicable Federal Information Processing Standards including, without limitation, FIPS 200, FIPS 140-2 or successor standards and all recommendations from the National Institute of Standards and Technology. The confidentiality of Customer Data shall be protected and maintained in accordance with these standards as well as other

applicable Customer standards.

6.3 Supplier shall comply with the CJIS Security Policy as more particularly described at Appendix 2 attached hereto and incorporated herein.

7 **Emerging Technologies**

The State of Oklahoma reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

8 **Extension Right**

In addition to extension rights of the State set forth in the Contract, the State CIO reserves the right to extend any Contract if the State CIO determines such extension to be in the best interest of the State.

9 **Source Code Escrow**

Pursuant to 62 O.S. § 34.31, if customized computer software is developed or modified exclusively for a State agency, the Supplier has a continuing obligation to comply with such law and place the source code for such software and any modifications thereto into escrow with an independent third-party escrow agent. Supplier shall pay all fees charged by the escrow agent and enter into an escrow agreement, the terms of which are subject to the prior written approval of the State, including terms that provide the State receives ownership of all escrowed source code upon the occurrence of any of the following:

9.1 A bona fide material default of the obligations of the Supplier under the agreement with the applicable Customer;

9.2 An assignment by the Supplier for the benefit of its creditors;

9.3 A failure by the Supplier to pay, or an admission by the Supplier of its inability to pay, its debts as they mature;

9.4 The filing of a petition in bankruptcy by or against the Supplier when such petition is not dismissed within sixty (60) days of the filing date;

9.5 The appointment of a receiver, liquidator or trustee appointed for any substantial part of the Supplier's property;

9.6 The inability or unwillingness of the Supplier to provide the maintenance and support services in accordance with the agreement with the agency;

9.7 Supplier's ceasing of maintenance and support of the software; or

9.8 Such other condition as may be statutorily imposed by the future amendment or enactment of applicable Oklahoma law.

10   Commercial Off The Shelf Software

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement that conflict with the terms of this Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail.

11   Ownership Rights

Any software developed by the Supplier under the terms of the Contract is for the sole and exclusive use of the State including but not limited to the right to use, reproduce, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. Moreover, except with regard to any deliverable based on Supplier Intellectual Property, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy, modify, display, perform, transmit and prepare derivative works of Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Except for any Supplier Intellectual Property, all work performed by the Supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as Work for Hire (as defined under the U.S. copyright laws) and, as such, shall be owned by and for the benefit of State.

In the event that it should be determined that any portion of such software or related supporting documentation does not qualify as "Work for Hire", Supplier hereby irrevocably grants to the State, for no additional consideration, a non-exclusive, irrevocable, royalty-free license to use, copy, modify, display, perform, transmit and prepare derivative works of any such software and any Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Supplier shall assist the State and its agents, upon request, in preparing U.S. and foreign copyright, trademark, and/or patent applications covering software developed, modified or customized for the State. Supplier shall sign any such applications, upon request, and deliver them to the State. The State shall bear all expenses that incurred in connection with such copyright, trademark, and/or patent applications.

If any Acquisition pursuant to this Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation owned by the State may be

shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier.

12   Intellectual Property Ownership

The following terms apply to ownership and rights related to Intellectual Property:

12.1   As between Supplier and Customer, the Work Product and Intellectual Property Rights therein are and shall be owned exclusively by Customer, and not Supplier. Supplier specifically agrees that the Work Product shall be considered "works made for hire" and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier hereby agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is hereby effectively transferred, granted, conveyed, assigned and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third-Party Intellectual Property, except as may be incorporated in the Work Product by Supplier.

12.2   Supplier, upon request and without further consideration, shall perform any acts that may be deemed reasonably necessary or desirable by Customer to evidence more fully the transfer of ownership and/or registration of all Intellectual Property Rights in all Work Product to Customer to the fullest extent possible including, but not limited to, the execution, acknowledgement and delivery of such further documents in a form determined by Customer. In the event Customer shall be unable to obtain Supplier's signature due to the dissolution of Supplier or Supplier's failure to respond to Customer's repeated requests for such signature on any document reasonably necessary for any purpose set forth in the foregoing sentence, Supplier hereby irrevocably designates and appoints Customer and its duly authorized officers and agents as Supplier's agent and Supplier's attorney-in-fact to act for and in Supplier's behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by Supplier, provided however that no such grant of right to Customer is applicable if Supplier fails to execute any document due to a good faith dispute by Supplier with respect to such document. It is understood that such power is coupled with an interest and is therefore irrevocable. Customer shall have the full and sole power to prosecute such applications and to take all other action concerning the Work Product, and Supplier shall cooperate, at Customer's sole expense, in the preparation and

prosecution of all such applications and in any legal actions and proceedings concerning the Work Product.

12.3 Supplier hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the Work Product which Supplier may now have or which may accrue to Supplier's benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. Supplier acknowledges the receipt of equitable compensation for its assignment and waiver of such Moral Rights.

12.4 All documents, information and materials forwarded to Supplier by Customer for use in and preparation of the Work Product shall be deemed the confidential information of Customer, subject to the license granted by Customer to Supplier hereunder. Supplier shall not otherwise use, disclose, or permit any third party to use or obtain the Work Product, or any portion thereof, in any manner without the prior written approval of Customer.

12.5 These provisions are intended to protect Customer's proprietary rights pertaining to the Work Product and the Intellectual Property Rights therein and any misuse of such rights would cause substantial and irreparable harm to Customer's business. Therefore, Supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the Supplier's obligations with respect to confidentiality provisions of the Contract and the Work Product and a Customer's Intellectual Property Rights, upon a request by Customer, without requiring proof of irreparable injury, as same is presumed.

12.6 Upon the request of Customer, but in any event upon termination or expiration of this Contract or a statement of work, Supplier shall surrender to Customer all documents and things pertaining to the Work Product, generated or developed by Supplier or furnished by Customer to Supplier, including all materials embodying the Work Product, any Customer confidential information and Intellectual Property Rights in such Work Product, regardless of whether complete or incomplete. This section is intended to apply to all Work Product as well as to all documents and things furnished to Supplier by Customer or by anyone else that pertains to the Work Product.

12.7 Customer hereby grants to Supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any Work Product solely as necessary to provide services to Customer. Except as provided in this section, neither Supplier nor any subcontractor shall have the right to use the Work Product in connection with the provision of services to its other customers without the prior written consent of Customer, which consent may be withheld in Customer's sole discretion.

12.8 To the extent that any Third-Party Intellectual Property is embodied or reflected in the Work Product or is necessary to provide services, Supplier shall obtain from the applicable third party for the Customer's benefit, an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for Customer's internal business purposes; likewise, with respect to any Supplier Intellectual Property embodied or reflected in the Work Product or

necessary to provide services, Supplier grants to Customer an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for the Customer's internal business purposes. Each such license shall allow the applicable Customer to (i) use, copy, modify, display, perform (by any means), transmit and prepare derivative works of any Third-Party Intellectual Property or Supplier Intellectual Property embodied in or delivered to Customer in conjunction with the Work Product and (ii) authorize others to do any or all of the foregoing. Supplier agrees to notify Customer on delivery of the Work Product or services if such materials include any Third-Party Intellectual Property. The foregoing license includes the right to sublicense third parties, solely for the purpose of engaging such third parties to assist or carry out Customer's internal business use of the Work Product. Except for the preceding license, all rights in Supplier Intellectual Property remain in Supplier. On request, Supplier shall provide Customer with documentation indicating a third party's written approval for Supplier to use any Third-Party Intellectual Property that may be embodied or reflected in the Work Product.

12.9   Supplier agrees that it shall have written agreement(s) that are consistent with the provisions hereof related to Work Product and Intellectual Property Rights with any employees, agents, consultants, contractors or subcontractors providing services or Work Product pursuant to the Contract, prior to the provision of such services or Work Product and that it shall maintain such written agreements at all times during performance of this Contract which are sufficient to support all performance and grants of rights by Supplier. Copies of such agreements shall be provided to the Customer promptly upon request.

12.10   To the extent not inconsistent with Customer's rights in the Work Product or other provisions, nothing in this Contract shall preclude Supplier from developing for itself, or for others, materials which are competitive with those produced as a result of the services provided under the Contract, provided that no Work Product is utilized, and no Intellectual Property Rights of Customer therein are infringed by such competitive materials. To the extent that Supplier wishes to use the Work Product or acquire licensed rights in certain Intellectual Property Rights of Customer therein in order to offer competitive goods or services to third parties, Supplier and Customer agree to negotiate in good faith regarding an appropriate license and royalty agreement to allow for such.

12.11   If any Acquisition pursuant to the Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation and materials owned by a Customer may be shared with other publicly funded agencies at the discretion of such Customer without permission from or additional compensation to the Supplier.

13   Hosting Services

13.1   If Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract Hosts Customer Data in connection with an Acquisition, the provisions of Appendix 1, attached hereto and incorporated herein, apply to such Acquisition.

13.2   If the Hosting of Customer Data by Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract contributes to or directly causes a Data Breach, Supplier shall be responsible for the obligations set forth in Appendix 1 related to breach reporting requirements and associated costs. Likewise if such Hosting contributes to or directly causes a Security Incident, Supplier shall be responsible for the obligations set forth in Appendix 1, as applicable.

14   **Change Management**

When a scheduled change is made to products or services provided to a Customer that impacts the Customer's system related to such product or service, Supplier shall provide two (2) weeks' prior written notice of such change. When the change is an emergency change, Supplier shall provide twenty-four (24) hours' prior written notice of the change. Repeated failure to provide such notice may be an evaluation factor (as indicative of Supplier's past performance) upon renewal or if future bids submitted by Supplier are evaluated by the State.

15   **Service Level Deficiency**

In addition to other terms of the Contract, in instances of the Supplier's repeated failure to provide an acceptable level of service or meet service level agreement metrics, service credits shall be provided by Supplier and may be used as an offset to payment due.

16   **Notices**

In addition to notice requirements under the terms of the Contract otherwise, the following individuals shall also be provided the request, approval or notice, as applicable:

Chief Information Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

With a copy, which shall not constitute notice, to:
Information Services Deputy Counsel
3115 North Lincoln Boulevard
Oklahoma City, Oklahoma 73105

The parties agree to the following provisions in connection with any Customer Data accessed, processed or stored by or on behalf of the Supplier and the obligations, representations and warranties set forth below shall continue as long as the Supplier has an obligation under the Contract

A.   Customer Data

 1. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of all Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).

 2. Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal request related to Customer without first notifying the Customer and obtaining the Customer's prior approval, which shall not be unreasonably withheld, of Supplier's proposed responses. Supplier agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.

 3. Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

B.   Data Security

 1. Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the Hosted environment and Customer Data and to protect against both unauthorized access to the Hosting environment, and unauthorized communications between the Hosting environment and the Customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public

Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

2. All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data.

3. Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus.

4. Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.

5. Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.

6. Supplier shall perform an independent audit of its data centers at least annually at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

7. Any remedies provided in this Appendix are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

C. **Security Assessment**

1. The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum security standards at time the Contract was executed. Failure to maintain the State's minimum security standards

during the term of the contract, including renewals, constitutes a material breach. Upon request, the Supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes, Supplier shall promptly notify the State and include in such notification the updated information; provided, however, Supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the Contract constitutes a material breach by Supplier and may result in a whole or partial termination of the Contract.

2. Any Hosting entity change must be approved in writing prior to such change. To the extent Supplier requests a different sub-contractor than the third-party Hosting Supplier already approved by the State, the different sub-contractor is subject to the State's approval. Supplier agrees not to migrate State's data or otherwise utilize the different third-party Hosting Supplier in connection with key business functions that are Supplier's obligations under the contract until the State approves the third-party Hosting Supplier's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party Hosting Supplier does not meet the State's requirements under the State Certification and Accreditation Review, Supplier acknowledges and agrees it will not utilize the third-party Supplier in connection with key business functions that are Supplier's obligations under the contract, until such third party meets such requirements.

D. **Security Incident or Data Breach Notification:** Supplier shall inform Customer of any Security Incident or Data Breach.

1. Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication.

2. Supplier shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation (i.e. HIPAA requires notice to be provided within 24 hours).

3. Supplier shall:

   a. Maintain processes and procedures to identify, respond to and analyze Security Incidents;

   b. Make summary information regarding such procedures available to Customer at Customer's request;

   c. Mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Supplier; and

> **d.** Document all Security Incidents and their outcomes.

4. If Supplier has reasonable belief or actual knowledge of a Data Breach, Supplier shall (1) promptly notify the appropriate Customer identified contact set forth herein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

E. **Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Supplier.

1. Supplier shall (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

2. Unless otherwise stipulated, if a Data Breach is a direct result of Supplier's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – all not to exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Supplier based on root cause.

3. If a Data Breach is a direct result of Supplier's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

F. **Notices**

In addition to notice requirements under the terms of the Contract and those set forth above, a request, an approval or a notice in connection with this Appendix provided by Supplier shall be provided to:

Chief Information Security Officer

3115 N. Lincoln Blvd

Oklahoma City, OK 73105

and

servicedesk@omes.ok.gov.

G. **Supplier Representations and Warranties**

Supplier represents and warrants the following:

1.   The product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.

2.   Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.

3.   The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.

4.   Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or though the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

H. **Indemnity**

Supplier agrees to defend, indemnify and hold the State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification), excluding damages that are the sole fault of Customer, arising from or in connection with Supplier's breach of its express representations and warranties in these Information Technology Terms and the Contract. If a third party claims that any portion of the products or services provided by Supplier under the terms of another Contract Document or these Information Technology Terms infringes that party's patent or copyright, Supplier shall defend, indemnify and hold harmless the State and Customer against the claim at Supplier's expense and pay all related costs, damages, and attorney's fees incurred by or assessed to, the State and/or Customer. The State and/or Customer shall promptly notify Supplier of any third party claims and to the extent authorized by the Attorney General of the State, allow Supplier to control the defense and any related settlement negotiations. If the Attorney General of the State does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall be granted authorization to equally participate in any proceeding related to this section but Supplier shall remain responsible to indemnify Customer and the State for all associated costs, damages and fees incurred by or assessed to the State and/or Customer. Should the software become, or in Supplier's

opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with Hosting services, Supplier may, at its option (i) procure for the State the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes non-infringing.

I.   Termination, Expiration and Suspension of Service

1.   During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data.

2.   In the event of a termination or expiration of the Contract, the parties further agree:

Supplier shall implement an orderly return of Customer Data in a format specified by the Customer and, as determined by the Customer:

a.   return the Customer Data to Customer at no additional cost, at a time agreed to by the parties and the subsequent secure disposal of State Data;

b.   transitioned to a different Supplier at a mutually agreed cost and in accordance with a mutually agreed data transition plan and the subsequent secure disposal of State Data or

c.   a combination of the two immediately preceding options.

3.   Supplier shall not take any action to intentionally erase any Customer Data for a period of:

a.   10 days after the effective date of termination, if the termination is in accordance with the contract period;

b.   30 days after the effective date of termination, if the termination is for convenience; or

c.   60 days after the effective date of termination, if the termination is for cause.

After such period, Supplier shall, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control.

4.   The State shall be entitled to any post termination or expiration assistance generally made available with respect to the services.

5.   Disposal by Supplier of Customer Data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer, shall be performed in a secure manner. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to Customer within thirty (30) calendar day of its request for disposal of data.

INTRODUCTION

The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff.

CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information ("CJI"). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency ("CJA") and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. **Per Appendix "A" to said Security Policy, "access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI."**

DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION
AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI
and CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy **plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System ("OLETS") which is operated by DPS.**

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:
   1.   the Definitions and Acronyms in §3 & Appendices "A" & "B";

2.   the general policies in §4;
3.   the Policies in §5;
4.   the appropriate forms in Appendices "D", "E", "F" & "H"; and
5.   the Supplemental Guidance in Appendices "J" & "K".

This FBI Security Policy is located and may be downloaded at: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

Policy Requirement Checklist	Compliance checklist –

Policy Area 1   Information Exchange Agreements

Policy Area 2   Security Awareness Training

Policy Area 3   Incident Response

Policy Area 4   Auditing and Accountability

Policy Area 5   Access Control

Policy Area 6   Identification and Authentication

Policy Area 7   Configuration Management

Policy Area 8   Media Protection

Policy Area 9   Physical Protection

Policy Area 10   Systems and Communications
                     Protection and Information
                     Integrity

Policy Area 11 Formal Audits Policy

Area 12 Personnel Security