



PRESIDIO®

Future. Built.

**MANAGED SERVICES CONTRACT
SELECT SERVICES
CAREERSOURCE CENTRAL FLORIDA**

January 19, 2021 (revision 1.5)

REVISION HISTORY

Revision	Revision Date	Name	Notes
1.0	07-01-2020	Paul Goldy	Initial Proposal for Select Managed Services
1.1	07-07-2020	Meredith Kirkwood	Updated Terms and Conditions, Reference MMSA
1.2	09-08-2020	Meredith Kirkwood	Updated Covered Equipment List, Pricing
1.3	10-14-2020	Meredith Kirkwood	Updated LoA Effective Date, STM Fee
1.4	01-05-2021	Lauren Wright	Removed Auto Renewal Clause
1.5	01-19-2021	Ken Boord	Updates per contract review with customer (email comments)

Lauren N Wright
1/27/2021

Notices: © 2021 Presidio. All Rights Reserved. This document and its contents are the confidential and proprietary intellectual property of PRESIDIO and may not be duplicated, redistributed or displayed to any third party without the express written consent of PRESIDIO.

Other product and company names mentioned herein may be the trademarks of their respective owners.

TABLE OF CONTENTS

1. SERVICE SUMMARY	4
2. SERVICE DELIVERY CENTER	5
3. MONITORING.....	10
4. CLIENT PORTAL & STANDARD REPORTS	13
5. CHANGE MANAGEMENT	14
6. PROBLEM MANAGEMENT	17
7. PATCH MANAGEMENT	18
8. CARRIER MANAGEMENT.....	19
9. DISPATCH SERVICES	20
10. VENDOR MANAGEMENT	21
11. SERVICE DELIVERY MANAGEMENT	22
12. SERVICE TRANSITION MANAGEMENT	23
13. CLIENT RESPONSIBILITIES.....	25
14. PRICING & CONTRACT TERM	27
15. COVERED EQUIPMENT LIST.....	29
TERMS AND CONDITIONS.....	30
APPENDIX A: NETWORK SERVICES	35
GENERAL DEFINITIONS.....	37

1. SERVICE SUMMARY

This Managed Services Contract is designed to provide a thorough understanding of Managed Services activities and deliverables. The main body of this proposal outlines the service deliverables for Presidio Managed Services. The Service Appendices provide details on Client-selected services, including any custom offerings.

Select Service is built on the Presidio Managed Services Delivery Framework, which combines industry-leading technologies, proven processes and highly certified personnel. The service includes all of the integrated Service Elements, identified in the table below. Presidio also provides the option of adding Custom Elements to supplement the Select offering. These elements are scoped separately.

Service Elements drive the level of service for each of the Presidio Managed Services offerings and are defined in the sections that follow. Details for the specific service deliverables are outlined in the Service Appendices. Your Managed Services Support Solution will include the following:

Service Elements

Select Service
<ul style="list-style-type: none">• Service Delivery Center• 7 x 24 x 365 Monitoring• Client Portal• Standard Reports• Change Management<ul style="list-style-type: none">◦ 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) is the central point-of-contact to Presidio Managed Services for daily support activity and is also generally referred to as the Network Operations Center (NOC). It is the main point of contact for reporting incidents (disruptions or potential disruptions in service availability and/or quality) and for Clients making service requests (routine requests for services). Presidio's Service Delivery Center team is staffed 24 hours a day, 7 days a week, 365 days a year in three primary locations including Orlando, FL, Dallas, TX, and Minneapolis, MN.

The SDC will deliver Tier 1 through Tier 3 technical support using Presidio's Information Technology Infrastructure Library (ITIL)-based processes. Presidio defines technical support levels as follows:

Tier 1: Technician Support

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

Tier 2: Engineering Support

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

Tier 3: Advanced Technical Support

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

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

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

Client personnel contacting the Presidio SDC must be authorized to do so as defined in the 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 and handled as a normal Change, if required.
 - Interact with third-party support providers (e.g., Cisco Technical Assistance Center [TAC]). This requires a Client-signed Letter of Agency (LOA) processed during the Service Transition Management phase. Carrier Case Management is only included in the Select tier of services.

2.1.1. Incident Prioritization Classification and Prioritization

Incidents need proper classification and prioritization. Classification and prioritization are described as follows:

- Classification - Determined by choosing the correct service offering, category and subcategory as it pertains to the incident.
- Prioritization - Assigning impact and urgency calculates the appropriate priority.

2.1.2. Determining Classification and Prioritization

Based on the information placed in the incident during its creation, the incident is reviewed and the correct classification, urgency and impact are selected.

Priority is based on the combined Impact and Urgency assignments, reflecting the level of adverse impact to the Client systems.

2.1.3. Impact Definition

Impact refers to the business impact of the system impacted. The initial impact is pre-defined from the alerting tool based on the type of alarm received or Client request.

There are three categories of impact:

1. **High:** Incident affecting an entire site or multiple sites.

2. **Medium:** Incident affecting multiple users.
3. **Low:** Incident affecting one or few users.

2.1.4. Urgency Definition

Urgency is the extent to which the incident's resolution can bear delay. The initial urgency is pre-defined from the alerting tool based on the type of alarm received or Client request.

Presidio Incident and Problem urgency and corresponding priority levels are defined as follows:

1. **High:** Full service outage of a critical system or VIP is affected, requires urgent response.
2. **Medium:** Client's ability to function is partially impacted, requires the SDC to respond as soon as possible.
3. **Low:** No impact on the Client's ability to function; is more informational in nature and a response is not critical.

Presidio retains the case priority even if there is a reduced severity of impact until incident resolution. The case may be left open for a prescribed period while operational stability is being assessed.

The incident shall be closed by Presidio or Client upon validation of issue remediation and the CI's return to operational stability.

Complete detail for open and closed tickets resides on the Client Portal and is used to support incident management and problem management processes.

2.1.5. Priorities for Tools Generated Incidents

Presidio monitoring tools apply the following priorities for auto-generated incidents, generally indicating the condition shown (the actual condition is determined by a number of factors as defined in the thresholds).

Incident Priorities

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

2.1.6. Incident Escalation

Incidents are escalated according to a defined process. At any point in the incident management process, the Client may request escalation via the Presidio SDC Supervisor to address concerns about the handling of the incident. If service restoration requires activities by a third-party provider, Presidio initiates and manages the process.

For a High Severity (P1 or P2), Clients are asked to call Presidio Managed Services. The SDC will initiate a live handoff to an engineer. If further escalation of an existing ticket or after business hours escalation is required, the Client should request to speak to the SDC Supervisor or

Manager. The Client is provided with a list of five escalation levels in case needed, including the SDC Supervisor at Level 1.

Upon resolution, the Client is notified the incident is resolved and provided with the opportunity to verify services have been restored satisfactorily. Following incident resolution and Client notification, the incident is closed by Presidio. Reports regarding incident management are available on the Client Portal.





2.2. Service Level Objectives

Service Level Objectives (SLO) are specifically aligned to incident priorities and response times for service requests. Presidio categorizes each issue by priority reflecting the level of adverse impact to Client systems. Priority provides a reasonable and accurate reflection of the number and complexity and business impact of systems affected. Clients have the ability to set or change the priority level of an incident at any time, based on the impact to their specific business.

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 Level Objectives

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%	30 minutes >90%	4 hours >80%	8 hours NA
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%	1 hour >90%	8 hours >80%	3 days 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 NA			

* Requires customer user subscription to notifications.

Acknowledgement Response Time achievement percentage is calculated as follows:

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

First Access Response Time achievement percentage is calculated as follows:

Total Incidents within First Access Response Time Service Level Target / Total Incidents (for each priority).

3. MONITORING

Presidio's monitoring is implemented through an extensive set of integrated tools that work in unison to manage a customer's environment. These tools provide device health monitoring and reporting, enable event consolidation, provide an interface for remote diagnostics and exchange information with the IT Service Management (ITSM) platform to support advanced capabilities such as automated incident creation.

The Presidio Data Collection Agent (DCA) comes pre-configured with all Presidio monitoring tools. Once installed, Presidio's experienced team configures the customer DCA to communicate back to Presidio's primary collection point where all Customer data is collected and automatically analyzed.

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

Presidio will monitor the health and performance via multiple avenues including SNMP polling at set intervals, SNMP traps for critical alerts, and when viable, other methods as determined by the technology being monitored.

3.1. Service Details

- Tool Setup and Deployment
- User Orientation
- 24X7 Collection of Monitored Component Data
- Technical Support on Tool and Collection Process
- Real-time Threshold Monitoring and Exception Notification Event management

Presidio provides monitoring and instrumentation problem resolution services with best-practice processes supported by a state-of-the-art toolset. The service starts with a component, and then performs polling for events. Alarms are consolidated and efficiency is optimized for root cause analysis. Presidio provides full console services and incident workflow. The components of the service include:

- Surveillance
 - The instrumentation mechanism is present and active for devices that are monitored and filtering of conditions is established to provide preventive, early warning of out-of-normal conditions.
- Detection
 - Out-of-normal conditions are identified by the surveillance mechanism and conditions are forwarded to collection engines for automated analysis.
- Consolidation
 - The condition is compared to other active conditions to establish relationships and the condition is identified from many as actual, or most probable, common cause of all related conditions and an alert is forwarded to the ITSM system.
- Isolation
 - The operator validates the isolated incident using automated alert data, available documentation, skill and judgment. The operator then identifies the absence or presence of a known error condition.

- **Respond and Inform**
 - The incident and resolution data are reviewed and the instrumentation problem management process begins. The problem management team identifies appropriate systemic action and advises surveillance if filtering requires an adjustment.
- **Learn**
 - The incident and resolution information are reviewed and the instrumentation problem management process begins. The problem management team identifies appropriate systemic action and advises surveillance if the filtering requires adjustment.

3.2. Performance Management

Performance planning includes information collection, forecasting, analysis, decision-making, and decision support. Performance planning is a strategic part of capacity management. Through capacity planning, future requirements are forecasted, and plans are prepared to ensure that resource capacity will be available when needed. Presidio's Monitoring solutions will detect conditions as capacity approaches predetermined thresholds, alert operations staff to these conditions via the operations console and initiate escalation and incident investigation automatically.

3.3. Monitoring Framework

This section describes the design of the monitoring solution including the various components of the solution and the infrastructure to support those components.

3.4. Presidio Data Centers

Presidio's Managed Services data center space includes two separate facilities. Each facility features dual home connectivity to two network carriers and a data center infrastructure consisting of independent compute, storage, security and network infrastructure. Each infrastructure component has multiple levels of redundancy to avoid a service outage with a single failure of a component.

3.5. 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.

3.6. Presidio Monitoring Solution(s)

The Presidio Monitoring Solution provides continuous monitoring of the health and availability of heterogeneous systems and networks. The service provides an extensive range of servers, voice applications, routers and wireless access points for monitoring. Certain server and application

settings can also be changed to provide as much information that is available from SNMP and other native system or application utilities that can alert support teams when failures or events occur. Powerful event management capabilities correlate information and pinpoint the root cause of a problem. The service uses the following techniques to find infrastructure problems:

- **Mapping** – The Presidio monitoring solutions walk the devices mapping the topology and stores in a model of the environment and all the devices
- **Polling** - Actively reach out to every intelligent device every 5 minutes and ask it about its state of health
- **Log Reading** - Scanning the logs of every device for symptoms (where available and by request)
- **Trap Listening** - Filtering for those which are warning alarms sent by intelligent devices or other element management systems when they detect a problem (where available and by request)
- **Consolidation** - Use expert rules to relate symptoms to the known topology, the devices known to be there, and other symptoms recently obtained

3.7. Monitoring Notification and Escalation

Incident notification informs Presidio and the Client that an Incident has been recorded.

Notification and Escalation

- Automated, policy-based actions used to further customize event notifications
- Typically used to create unique notification timing based on business
- operational requirements (i.e. suppress memory alarms on certain servers if they are less than 30 minutes in duration during application peaks)
- Grouping policies can be based on customer, component type, description, etc.

Dynamic Modeling

- Ability to give individual devices unique attributes which can be used for workflow or business unit needs (through the ITSM System)
- Identify critical devices which may need higher priority action or lower priority action (i.e. only needs escalation during prime time)
- Ability to set platform type used on operations, ticketing, workflow, troubleshooting

Console Configurations

- Operations console configurations to alter views of accounts, devices, classes of events, events requiring action, etc.

4. CLIENT PORTAL & 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 three categories:

1. Standard Changes
2. Normal Changes
3. Emergency 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. Presidio reviews the contract for each device-level request and determines if it falls outside of the scope as defined below:

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

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

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

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

5.5.2. User Changes

A User Change is change for Collaboration services impacting any single user-based configuration, including moves, additions, changes or deletions; e.g., a request to add/delete a user profile. Details are provided in the MACD section of the Unified Communications Service Appendix.

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

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

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.

Problem Management has two major categories:

1. Problem Identification
2. Problem Diagnosis

6.1. Problem Identification

The process starts with analyzing available data, identifying and recording problems, and classifying problems according to impact, urgency, and status.

6.2. Problem Diagnosis

The Problem is assessed to determine potential resolutions, which can include both temporary workarounds as well as permanent fixes. If a permanent fix is possible and cost-justifiable, a recommendation is made to the Client to correct the error by initiating a change via Change Management.

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.

Patch management for incidents is applied when a vendor support case directs Presidio to apply a version consistent with a fix for a known error. Vulnerabilities are defined as a defect reported by a manufacturer that has the potential to affect the overall security of a client device or devices. These vulnerabilities are typically resolved with a software workaround or a patch issued by the manufacturer. Vulnerability patches are applied when there is a CVSS score that is a 9.0 or higher (Critical) as defined by the CVSS specifications listed at <https://www.first.org/cvss/specification-document>. Due to the unknown nature of the number of releases during any given year, Presidio will provide up to two vulnerability patches per device per year beginning on the Start of Service date of the contract. Additional vulnerability patches are not considered MACD activity and are billed as a separately negotiated addendum to the original SOW as applicable. Vulnerability patches are not proactively applied as part of any other service level.

Patch application to remediate incidents and mitigate known security vulnerabilities is a cooperative decision between the customer and Presidio. Patches are evaluated to ensure that current environmental stability is maintained. Patches to remediate an incident, vulnerability or problem identified by Presidio are handled as a Change Request.

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

- For incident remediation patches, Presidio will review manufacturer field notices to determine impact and urgency to the Client system and existing software levels.
- For vulnerabilities classified as Critical per the Common Vulnerability Scoring System, CVSSv3, with a score of 9.0 – 10.0, Presidio will assess impacts to the Client and provide recommendations for remediation as applicable.
- For critical security vulnerabilities and incident remediation as defined above, Presidio remotely applies updates to affected CIs following the approved Change Management process.

If the Patch application necessitates a full upgrade in version level, requires a physical change to the existing hardware configuration or impacts dependent technologies, the effort is evaluated and may be subject to a separate project agreement. Covered equipment with software where the software maintenance has reached end of support or has lapsed, is not covered by the Patch Management element.

Client-requested patches for obtaining additional features or functions are out of scope of this section and must be handled as a separate agreement as referenced in "Device Level Changes" under the Change Management section of this document.

8. CARRIER MANAGEMENT

Presidio provides operational handling of carrier cases with third-party data and voice carriers for incident remediation. For most Clients under management by Presidio, there is a strong telecommunication vendor dependency. This service element enables Presidio to open tickets, for Clients who have provided a signed Letter of Agency (LOA) and the requisite circuit information, on behalf of the Client for any circuits directly connected to devices under Presidio management. Presidio manages the case throughout the incident resolution process.

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

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:
 - Installing the DCA in a suitable equipment rack and connecting to network.
 - Power connection to Uninterruptible Power System (UPS) or other facility with continuous uninterrupted power.
 - Power-up.
 - Notification to Presidio that installation is complete.
- Provide suitable commercial power, and recommends UPS or other acceptable power back-up facilities providing a minimum of 1kVA dedicated to each appliance.

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:

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

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:
 - DCA monitoring of Managed CIs.
 - Proper operation or network connectivity of Managed CIs.
- Maintain responsibility for informing Presidio of Client employee status changes.
- Provide and maintain a list of Client employees authorized to request changes.
- Provide and maintain an escalation path within the Client's employee base.

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	1 Year	Estimated Coverage Period	Start: 4/1/2021	End: 3/31/2022
Billing Frequency			Amount (\$) per Period	
Monthly			\$1,163.30	
Base Managed Services			Base Annual Service Fees	
	Network Services		\$13,959.60	
Subtotal			\$13,959.60	
Non-Recurring Fees				
Service Transition Management (see pages 23-24 of contract)			\$10,000.00	
Subtotal			\$10,000.00	
Total Fees				
Year 1			\$23,959.60	
Total Contract			\$23,959.60	

14.1. 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 for the initial 12-month period but may be cancelled (subject to termination fees as set forth below, and not to include any non-cancellable third-party offerings) after the initial 12-month period with 60-days' written notice. However, to avoid interruption in service, Client reserves the right to renew or terminate this Service Order after the initial term, for up to two additional annual terms with a 60-days' written notice to Presidio. Further, unless the quantities of equipment listed in Section 15 – Covered Equipment List (see Page 29) is increased by the Client, Presidio agrees not to increase the Network Services price during these additional renewal periods. In cases where third-party offerings (including but not limited to Cisco maintenance, NetApp ASP, EMC VSPP, LogRhythm, and Intel ISCC) are included as part of the services being provided by Presidio, the portion of this SOW representing such third-party offerings shall be strictly non-cancelable. The Client will not, under any circumstances, be entitled to receive any refund for any prepaid third-party offerings that are included as part of the services being provided by Presidio. In the event of an early termination of this SOW for any reason, 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.

In the event the term of this SOW expires without a Client termination or renewal, services and billing outlined within this SOW will continue on a month-to-month basis until a termination or renewal is received from the customer.

15. COVERED EQUIPMENT LIST

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

Device Type	Manufacturer	Model	Quantity
Vendor Managed Firewall	Sophos	Sophos XG	2
Router (Branch)	Cisco	CISCO3825	1
Router (Branch)	Cisco	CISCO2921	3
Switch (Access Branch)	Cisco	WS-C29xx	6
Switch (Access Branch)	Cisco	WS-C9300	9
Switch (Access Branch)	Cisco	WS-C3850	1
Switch (Datacenter, Core)	Cisco	WS-C4500E	2

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

TERMS AND CONDITIONS

This Master Managed Services Agreement ("Agreement") is effective as of the date last signed below, and is made by and between Presidio Networked Solutions LLC, with principal offices at 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:	CareerSource Central Florida	POC:	Paul Worrell
Billing Address:	390 N Orange Ave, Suite 700 Orlando, FL 32801	POC Phone #:	407-531-1222 x2019
		POC E-mail:	pworrell@careersourcecf.com

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 be modified accordingly. Presidio will advise Client of any condition which would render the Equipment ineligible for the Services hereunder. Client shall be responsible for correcting, at its expense, any such condition prior to or during the term of Presidio Services being provided.

6. Term

The initial term of this Master Managed Services Agreement ("Term") shall be three (3) years from the effective date. The Term of this Master Managed Services Agreement will automatically renew for additional one (1) year periods unless Client terminates the Agreement by giving prior written notice to Presidio (as specified in Section 8, below) at least sixty (60) days before the then-current Term expiration date. Notwithstanding anything to the contrary, any such notice of non-renewal shall not take effect, and this Agreement shall remain in force, until the end of the term of any and all outstanding SOWs. **The term of Services under each SOW shall be as specified therein.**

7. Client Responsibilities

Subject to reasonable confidentiality/security obligations as accepted by Presidio in writing, Client shall grant Presidio full and free remote and/or physical access to the Equipment at all times during the Term of each SOW, including all required access credentials (e.g. IP addresses, SNMP community strings, passwords, etc.). For monitoring tiers of service, Client shall provide Presidio with at least one publicly-routable IP address for monitoring VPN connectivity and one IP address for the Presidio monitoring collection station. Client will provide all pertinent network diagrams and documentation. Client shall provide and maintain an up-to-date list of authorized contacts and escalation information, including third-party vendor contact information, letters of authority, maintenance schedules and device configurations. Client shall ensure that the Equipment meets, at all times, the manufacturer-approved configuration specifications and is covered by a then-current vendor maintenance and support program. **Client acknowledges and agrees that the foregoing factors are critical for Presidio to perform the Services, and Presidio's performance hereunder or under any SOW may be delayed or suspended if Client does not comply with its obligations in this Section.**

8. Notices

Day-to-day notices, authorizations and other official communications under this Agreement shall be transmitted in writing by email to Presidio's assigned Account Manager or Service Delivery Manager and to the Client at the POC address specified above, or as otherwise specified in a SOW. Legal and termination notices shall be sent by nationally-recognized overnight courier (signature required), to Presidio Networked Solutions LLC, Attn: General Counsel, One Penn Plaza, Suite 2832, New York, NY 10119, and to Client at the address and POC set forth in Section 1 above. Email notices are effective upon actual receipt; overnight courier notices are deemed given upon delivery as determined by signature, or refusal to accept delivery.

9. Assignment

Neither party may assign or transfer this Agreement or any rights or obligations hereunder without the written consent of the other party. Any required consent shall not be unreasonably withheld, conditioned or delayed. Notwithstanding the foregoing, Presidio may assign this Agreement without Client's consent in connection with a merger or other sale of Presidio's business as a going concern.

10. Warranties, Remedies and Limitations

Presidio warrants that the Services will be performed in a good and workmanlike manner, in accordance with all applicable laws and regulations. In the event this warranty is breached, Presidio shall promptly render/re-perform conforming Services. **THE FOREGOING WARRANTY IS MADE IN LIEU OF ALL OTHER WARRANTIES, GUARANTEES OR CONDITIONS PERTAINING TO THE SERVICES, WHETHER WRITTEN OR ORAL, STATUTORY, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY AS TO MERCHANTABILITY, NONINFRINGEMENT OR FITNESS FOR ANY PARTICULAR PURPOSE. ALL SUCH OTHER WARRANTIES ARE HEREBY EXPRESSLY DISCLAIMED. PRESIDIO IS NOT RESPONSIBLE FOR ANY WARRANTY OFFERED TO CLIENT BY ANY OTHER PARTY. THE FOREGOING WARRANTY AND REMEDY SHALL CONSTITUTE PRESIDIO'S SOLE AND EXCLUSIVE OBLIGATION, AND CLIENT'S SOLE AND EXCLUSIVE REMEDY FOR BREACH OF WARRANTY HEREUNDER, NOTWITHSTANDING ANY FAILURE OF THE FOREGOING REMEDY TO FULFILL ITS ESSENTIAL PURPOSE.**

11. Non-Solicitation

During the term of this Agreement and for a period of twelve (12) months thereafter, Client will not, without the prior written consent of Presidio, solicit for employment any Presidio employee who was directly involved in the performance of this Agreement or any SOW. Notwithstanding the foregoing, Client shall not be restricted from engaging in normal recruiting and hiring practices, including the placement of ads directed toward the general public and/or the use of recruiters, so long as such recruiting efforts are not specifically targeted at Presidio employees with whom Client became acquainted through this Agreement.

12. Confidentiality

Both parties recognize that during the course of this Agreement, one party ("Receiving Party") may acquire knowledge, confidential or proprietary business information or trade secrets from the other party ("Disclosing Party") which: (a) has been marked as confidential, (b) whose confidential nature has been made known to the Receiving Party, or (c) that due to the nature of the information, should be reasonably understood to be confidential (collectively, "Confidential Information"). Confidential Information, whether marked or not, shall specifically include, but not be limited to: (1) technical information such as methods, processes, formulae, compositions, systems, techniques, inventions, machines, computer programs and research projects; (2) business information such as client lists, pricing data, supply sources, financial and marketing data, production, or merchandising systems or plans, business policies or practices, and (3) any non-public personal information, including but not limited to personally identifiable financial, credit card or medical information. The Receiving Party agrees to keep all Confidential Information in a secure place and further agrees not to publish, communicate, divulge, use, or disclose, directly or indirectly, for his, her or its own benefit or for the benefit of another, any Confidential Information except as specifically required in accordance with performing its duties under this Agreement and as allowed by applicable law. The obligations of confidentiality contained herein shall apply during the Term of this Agreement and for a period of three (3) years thereafter. As applicable, upon termination or expiration of this Agreement, the Receiving Party shall deliver all confidential records, data, information, and other computer media or documents produced or acquired during the performance of this Agreement and all copies thereof to the Disclosing Party, provided that either party may, subject to the confidentiality provisions hereof, keep such copies as may be required of it by applicable law. Confidential Information shall remain the property of its owner/original discloser and nothing herein should be construed as granting a license, title, or any other rights to that information. This obligation of confidentiality shall not apply with respect to information that 1) was in the public domain prior to disclosure, 2) is available to the Receiving Party from third parties having the legal right to disclose the same on an unrestricted basis, 3) is disclosed by Disclosing Party to others on an unrestricted basis, or 4) is developed by Receiving Party independently without reference to any Confidential Information of the Disclosing Party. Either party may disclose Confidential Information to a court or government body having competent jurisdiction pursuant to an order therefrom, provided that the Receiving Party provides any legally permissible prior written notice of disclosure to the Disclosing Party and takes reasonable actions to avoid and/or minimize the extent of such disclosure.

13. Limitation of Damages

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW: (A) EACH PARTY'S ENTIRE LIABILITY UNDER THIS AGREEMENT AND ALL SOWS, WHETHER ARISING OUT OF THE SERVICES OR FROM SUCH PARTY'S NEGLIGENT OR OTHER ACTS OR OMISSIONS, SHALL BE LIMITED TO THE CHARGES AND FEES ACTUALLY PAID FOR THE SERVICES GIVING RISE TO THE CLAIM, AND (B) REGARDLESS OF THE LEGAL OR EQUITABLE BASIS OF ANY CLAIM OR OF ACTUAL NOTICE, NEITHER PARTY SHALL BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL LOSSES OR DAMAGES, INCLUDING, WITHOUT LIMITATION, DATA LOSS, EVEN IF THE PARTY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

14. Default

Except as otherwise provided herein, in the event of any material breach of this Agreement by either party which continues for more than thirty (30) days after receipt of reasonable written notice of the breach, the aggrieved party may at its option: (a) if Client, suspend payments for so long as the breach continues uncorrected; and/or (b) if Presidio, suspend performance hereunder for so long as the breach continues uncorrected; and/or (c) to avail itself of any and all remedies available to it at law or equity, whether or not it elects to suspend its performance as permitted hereby.

15. Subcontracting:

Presidio reserves the right to subcontract such portions of the Services to subcontractors of Presidio's choosing as it deems appropriate, provided that no such subcontract shall relieve Presidio of primary responsibility for performance of such Services.

16. Indemnification

Each party shall indemnify the other with respect to any third-party claim alleging: (a) bodily injury (including death) or damage to tangible property, to the extent such injury or damage is caused by the negligence or willful misconduct of the indemnifying party, (b) breach of any representations, warranties or obligations under this Agreement; or (c) violation of any applicable law or regulation. Each party will promptly advise the indemnifying party of the claim and turn over its defense. The party being indemnified must cooperate in the defense or settlement of the claim, but if properly and timely tendered to the indemnifying party, then the indemnifying party must pay all litigation costs, reasonable attorney's fees, settlement payments and any damages awarded; provided, however, the indemnifying party shall not be required to reimburse attorney's fees or related costs that the indemnified party incurs either to fulfill its obligation to cooperate, or to monitor litigation being defended by the indemnifying party.

17. Publicity

Unless required by law, neither party shall disclose the existence of, or any term or condition of, this Agreement to any third party (other than its parent or an affiliate) without the prior written consent of the other party. Neither party shall publish any advertising, sales promotion, press releases or publicity matters relating to this Agreement without the prior written approval of the other party.

18. Miscellaneous

The failure by either party to enforce any provision of this Agreement will not constitute a present or future waiver of such provision, nor limit such party's right to enforce such provision 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.

CareerSource Central Florida	Presidio Networked Solutions LLC
By: <u>Pamela Nabors</u>	By: <u>SPH</u>
Name: <u>Pamela Nabors</u>	Name: <u>Steven Palmese</u>
Title: <u>President & CEO</u>	Title: <u>CIO</u>
Date: <u>2/3/2021</u>	Date: <u>Feb 5, 2021</u>

Letter of Agency

April 1, 2021

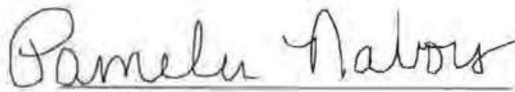
To Whom It May Concern,

Subject: Letter of Agency

The undersigned, CareerSource Central Florida, 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 CareerSource Central Florida 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 CareerSource Central Florida 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

Pamela Nabors - President & CEO

Client Name/Title (Please Print)

APPENDIX A: NETWORK SERVICES

The Presidio Network Services Portfolio includes both Network Management and Security Device Management.

Network Management

Network Management service provides monitoring and management of a Client's network infrastructure. The Service Offering covers and supports Core Switches, Routers, WAN Accelerators, Data Center Networks, LAN Switches, and Wireless Access Points and Controllers.

Security Device Management

The Security Device Management service manages a variety of security devices, including firewalls and Intrusion Prevention and Detections Systems (IPS/IDS).

A key aspect to Security Device Management is administration and monitoring at the device level to ensure availability and functionality. Inclusive in the service is the administration of critical security parameters, including firewall rule set administration, IDS/IPS signature management, and VPN tunnel management.

This service covers and supports Firewalls, Intrusion Prevention Appliances, Access Control Appliances, and Identity Services Engines.

Network Services Monitoring

The Network Management and Security Device Management Services include standard device-level monitoring.

The following are examples of the standard monitoring elements for the Network and Security Device Management Managed Services. Further content can be provided upon request.

Operational Status\System Uptime

- CPU Statistics
- Memory Statistics
- Hardware Environmental Status
- Interface Statistics
- SNMP Down

Standard Reports

The Client Portal allows Standard reports to be viewed online. The Standard Reports include four pre-configured reports, and data is retained for 6 months.

Client Portal for Network and Security Device Management Services Reports

Title	Description
Device Availability	Availability is based on uptime. Lists each managed CI, IP address, availability percentage, and actual downtime if applicable
CPU Utilization	Measures the average and the maximum CPU utilization for each CI in the report period. A graphical representation of the top CI is also included.
Interface Bandwidth Utilization	Measures the average and maximum bandwidth utilization by interface on each of the applicable managed CIs. The report ranks each interface. A graphical representation of the top interfaces is also included.

Memory Utilization	Measures the average and maximum memory utilization percentage for each managed CIs during the report period. A graphical representation of the top CIs is also included in the report.
---------------------------	---

NETWORK AND SECURITY SERVICES MANAGEMENT

Network Management and Security Device Management Services

Title	Description
System Backups	Presidio shall perform back-up processes for Cisco routers, switches, and other supported Command Line Interface (CLI) based CIs. This includes definition and execution of service restoration process for Managed CIs. The configuration back-ups are stored on the Presidio Monitoring Framework and available for use by Presidio in bringing current or replacement Managed CI to service. Device-based backups are not performed for Monitored-Only or Vendor Managed devices.
Moves, Adds, Changes, and Deletions (MACDs)	<p>With the Select Service level, Presidio offers device-level changes. The MACD section within this Statement of work defines the scope of these changes, along with any associated volume limitations.</p> <p>The following are examples of typical device-level changes:</p> <ul style="list-style-type: none"> • Router interface changes • Firewall ACL modifications • Switch port configurations • Wireless access-point definition (lightweight)

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.

Vendor Management: Presidio provides monitoring only (if monitoring framework is deployed), first-level support (triage only), alert and notification of monitored faults, and coordination of the supporting vendor/support teams on the Client's behalf throughout the troubleshooting process. Presidio does not provide second- and third-level troubleshooting and support for these devices. This support can only be provided on equipment with an existing manufacturer's warranty or current maintenance support contract.

Addendum to Agreement between CSCF and Presidio, dated 1/19/2021

CareerSource Central Florida Contractor General Provisions, Certifications and Assurances

CareerSource Central Florida will not award a contract where the contractor has failed to accept the General Provisions, Certifications and Assurances contained in this section. This contract addendum ensures the inclusion and acknowledgement of the required Federal and State contracting and purchasing requirements which must be included in Workforce Board of Central Florida, d/b/a CareerSource Central Florida's (CareerSource) vendor agreements. This addendum will not extend the contract period or increase the contract amount described in the original agreement. CareerSource Central Florida is required to provide its vendors with the GENERAL PROVISIONS, CERTIFICATIONS AND ASSURANCES contained.

This Addendum is part of the attached Agreement by and between CareerSource Central Florida (CareerSource) and Presidio (Contractor), for services described in **Managed Services Contract Select Services (V1.5)**, dated January 19, 2021 attached hereto. In consideration of the mutual covenant and stipulations set forth in the contract and Addendum herein, the parties hereby agree as follows:

1. COMPLIANCE WITH POLICIES AND LAWS

The warranty of this Section specifically includes compliance by Contractor and its subcontractors with the provisions of the Immigration Reform and Compliance Act of 1986 (P. L. 99-603), the Workforce Innovation and Opportunity Act (WIOA), the Workforce Innovation Act of 2000, 45 CFR 98, the Temporary Assistance for Needy Families Program (TANF), 45 CFR parts 260-265, and other applicable federal regulations and policies promulgated thereunder and other applicable State, Federal, criminal and civil law with respect to the alteration or falsification of records created in connection with this Agreement. Office of Management and Budget (OMB) Circulars: Contractor agrees that, if applicable, it shall comply with all applicable OMB circulars, such as 2 CFR 200 Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards. Contractor will comply, as applicable, with the provisions of the Davis-Bacon Act (40 U.S.C. 276a to 276a7, the Copeland Act (40 U.S.C. 276c and 18 U.S.C. 874, and the Contract Work Hours and Safety Standards Act (40 U.S.C. 327-333), regarding labor standards for federally assisted construction sub-agreements.

2. CERTIFICATION REGARDING DEBARMENT, SUSPENSION AND OTHER MATTERS

Contractor certifies that it is not currently debarred, suspended, or excluded from or for participation in Federal assistance programs, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal department or agency within a three-year period preceding the effective date of the Agreement, in accordance with 29 CFR Part 98. No contract shall be awarded to parties listed on the GSA List of Parties Excluded from Federal Procurement or Non-Procurement Programs.

3. NON-DISCRIMINATION, EQUAL OPPORTUNITY ASSURANCES, CERTIFICATIONS, OTHER PROVISIONS

As a condition of funding from CareerSource under Title I of the WIOA, Contractor assures that it will comply fully with the following:

- 1) Title VI of the Civil Rights Act of 1964 as amended, 42 U.S.C. 2000d et seq., which prohibits discrimination on the basis of race, color or national origin.
- 2) Section 504 of the Rehabilitation Act of 1973 as amended, 29 U.S.C. 794, which prohibits discrimination on the basis of disability.
- 3) Title IX of the Education Amendments of 1972 as amended, 20 U.S.C. 1681 et. Seq. which prohibits discrimination on the basis of sex in educational programs.
- 4) The Age Discrimination Act of 1975 as amended, 42 U.S.C. 6101 et seq., which prohibits discrimination on the basis of age.
- 5) Section 654 of the Omnibus Budget Reconciliation Act of 1981 as amended, 42 U.S.C. 9849, which prohibits discrimination on the basis of race, creed, color, national origin, sex, handicap, political affiliation or beliefs.
- 6) Section 188 of the Workforce Innovation and Opportunity Act (WIOA), which prohibits discrimination against all individuals in the United States on the basis of race, color, religion, sex, national origin, age, disability, political affiliation, or belief, and against beneficiaries on the basis of either citizenship/status as a lawfully admitted

Addendum to Agreement between CSCF and Presidio, dated 1/19/2021

immigrant authorized to work in the United States or Participation in any WIOA Title I financially assisted program or activity.

- 7) The American with Disabilities Act of 1990, P.L. 101-336, which prohibits discrimination on the basis of disability and requires reasonable accommodation for persons with disabilities.
- 8) Equal Employment Opportunity (EEO): The Contractor agrees that it shall comply with Executive Order (EO) No. 11246, Equal Employment Opportunity, as amended by EO No. 11375, requires that Federal Contractors and subcontractors not discriminate against any employee or applicant for employment because of race, color, religion, sex, or national origin. It also requires the Contractor/subcontractor to take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, or national origin and as supplemented in Department of Labor regulation 29 CFR Parts 33 and 37 as well as 41 CFR Part 60 and 45 CFR Part 80 if applicable.
- 9) Contractor also assures that it will comply with 29 CFR Part 38 and all other regulations implementing the laws listed above. This assurance applies to the grant applicant's operation of the WIOA Title I-financially assisted program or activity, and to all agreements Contractor makes to carry out the WIOA Title I-financially assisted program or activity. Contractor understands that the United States has the right to seek judicial enforcement of this assurance.

4. CERTIFICATION REGARDING CLEAN AIR ACT, WATER ACT, ENERGY EFFICIENCY AND ENVIRONMENTAL STANDARDS

Clean Air and Water Act: When applicable, if this Contract is in excess of \$100,000, Contractor shall comply with all applicable standards, orders or regulations issued under the Clean Air Act as amended (42 U.S.C. 7401), Section 508 of the Clean Water Act as amended (33 U.S.C. 1368 et seq.), Executive Order 11738 and Environmental Protection Agency regulations (40 CFR Part 15). The Contractor shall report any violation of the above to the contract manager. Energy Efficiency: The Contractor shall comply with mandatory standards and policies relating to energy efficiency which are contained in the State of Florida's Energy Conservation Plan issued in compliance with the Energy Policy and Conservation Act (Public Law 94-163).

Contractor will comply with environmental standards which may be prescribed pursuant to the following: (a) institution of environmental quality control measures under the National Environmental Policy Act of 1969 (P.L. 91-190) and Executive Order (EO) 11514; (b) notification of violating facilities pursuant to EO 11738; (c) protection of wetlands pursuant to EO 11990; (d) evaluation of flood hazards in flood plains in accordance with EO 11988; (e) assurance of project consistency with the approved State management program developed under the Coastal Zone Management Act of 1972 (16 U.S.C. 1451 et seq.); (f) conformity of Federal actions to State (Clean Air) Implementation Plans under Section 176(c) of the Clean Air Act of 1955, as amended (42 U.S.C. 7401 et seq.); (g) protection of underground sources of drinking water under the Safe Drinking Water Act of 1974, as amended, (P.L. 93-523); and (h) protection of endangered species under the Endangered Species Act of 1973, as amended, (P.L. 93-205). The Contractor will comply with the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act (42 U.S.C 6962).

5. CERTIFICATION REGARDING LOBBYING AND INTEGRITY

Contractor shall comply with the provisions of the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352) 29 CFR Part 93. When applicable, if this Agreement is in excess of \$100,000, Contractor must, prior to contract execution, complete the Certification Regarding Lobbying Form.

6. CONFIDENTIALITY

It is understood that the Contractor shall maintain the confidentiality of any information, regarding CareerSource customers and the immediate family of any applicant or customer, that identifies or may be used to identify them and which may be obtained through application forms, interviews, tests, reports from public agencies or counselors, or any other source. Contractor shall not divulge such information without the written permission of the customer, except that such information which is necessary as determined by CareerSource for purposes related to the performance or evaluation of the Agreement may be divulged to CareerSource or such other parties as they may designate having responsibilities under the Agreement for monitoring or evaluating the services and performances under the Agreement, or to governmental authorities to the extent necessary for the proper administration of the law. All release of information shall be in accordance with applicable State laws, and policies of CareerSource. No release of information by Contractor, if such release is required by Federal or State law, shall be construed as a breach of this Section.

Addendum to Agreement between CSCF and Presidio, dated 1/19/2021

7. RIGHTS TO DATA/COPYRIGHTS AND PATENTS

The Board, State of Florida and the U.S. Department of Labor shall have unlimited rights to inventions made under contract or agreement for the performance of experimental, developmental, or research work shall provide for the rights of the Federal Government and the recipient in any resulting invention in accordance with 37 CFR part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements" and any implementing regulations issued by the awarding agency.

8. MONITORING

At any time and as often as CareerSource, the State of Florida, United States Department of Labor, Comptroller General of the United States, the Inspector Generals of the United States and the State of Florida, or their designated agency or representative may deem necessary, Contractor shall make available all appropriate personnel for interviews and all financial, applicant, or participant books, documents, papers and records or other data relating to matters covered by this contract, for examination and/or audit, and/or for the making of excerpts or copies of such records for the purpose of auditing and monitoring activities and determining compliance with all applicable rules and regulations, and the provisions of this Agreement. The above referenced records shall be made available at the Contractor's expense, at reasonable locations as determined by CareerSource. Contractor shall respond in writing to monitoring reports and requests for corrective action plans within 10 working days after the receipt of such request from CareerSource.

9. PUBLIC ANNOUNCEMENTS AND ADVERTISING

Contractor agrees that when issuing statements, press releases, request for proposals, bid solicitation, and other documents describing the project or programs funded in whole or in part under this Agreement, Contractor shall clearly state: (1) the percentage of the total cost of the program or project which will be financed with Federal money under this Agreement and (2) the dollar amount of Federal funds for the project or program.

10. PUBLIC ENTITY CRIMES

Contractor shall comply with subsection 287.133(2)(a), F.S., whereby a person or affiliate who has been placed on the convicted vendor list following a conviction for a public entity crime may not submit a bid, proposal, or reply on a contract to provide any goods or services to a public entity; may not submit a bid, proposal, or reply on a contract with a public entity for the construction or repair of a public building or public work; may not submit bids, proposals, or replies on leases of real property to a public entity; may not be awarded or perform work as a contractor, supplier, subcontractor or consultant under a contract with any public entity; and may not transact business with any public entity in excess of the threshold amount provided in section 287.017, F.S., for Category Two for a period of thirty-six (36) months from the date of being placed on the convicted vendor list.

11. THE PRO-CHILDREN ACT

Contractor agrees to comply with the Pro-Children Act of 1994, 20 U.S.C. 6083. Failure to comply with the provisions of the law may result in the imposition of civil monetary penalty up to \$1,000 for each violation and/or the imposition of an administrative compliance order on the responsible entity. This clause is applicable to all approved sub-contracts. In compliance with Public Law (Pub. L.) 103-277, the Contract shall not permit smoking in any portion of any indoor facility used for the provision of federally funded services including health, day care, early childhood development, education or library services on a routine or regular basis, to children up to age 18.

12. TERMINATION FOR DEFAULT/CONVENIENCE

This modified agreement may be terminated as follows:

1. Either party may request termination of modified agreement upon 60 days prior written notice to the other party.
2. The Board may unilaterally terminate or modify this modified agreement, if for any reason either the U.S. Department of Labor or the State of Florida reduces funding through the grants under which this modified agreement is funded.
3. The Board may unilaterally terminate this modified agreement at any time that it is determined that:
 - a. Contractor fails to provide any of the services it has contracted to provide; or
 - b. Contractor fails to comply with the provisions of this modified agreement; or
 - c. Such termination is in the best interest of the BOARD.
4. Written notification of termination must be by registered mail, return receipt requested.

Addendum to Agreement between CSCF and Presidio, dated 1/19/2021

If Contractor disagrees with the reasons for termination, they may file a grievance in writing within ten days of notice of termination to the CareerSource Central Florida Consortium of Elected Officials, who will conduct a grievance hearing and decide, from evidence presented by both parties, the validity of termination.

In the event this modified agreement is terminated for cause, Contractor shall be liable to the Board for damages sustained for any breach of this modified agreement by the Contractor, including court costs and attorney fees, when cause is attributable to the Contractor, in accordance with the Agreement terms.

In instances where Contractors/sub-grantees violate or breach modified agreement terms, the Board will use all administrative, contractual or legal remedies that are allowed by law to provide for such sanctions and penalties as may be appropriate.

IN WITNESS WHEREOF, Contractor and Client have caused this Agreement to be duly executed as of the date set forth below.

APPROVED BY: CAREERSOURCE CENTRAL FLORIDA

BY: Pamela Nabors

Pamela Nabors, President & CEO
Printed Name of Client Representative

Duly authorized for and on behalf of
CareerSource Central Florida

APPROVED BY: PRESIDIO NETWORKED SOLUTIONS

BY: Jackie Arnett 1/27/2021

Jackie Arnett, Director Contract Administration
Printed Name of Contractor Authorized Representative

Duly authorized for and on behalf of
Presidio Networked Solutions, LLC

Steven Palmese
Steven Palmese (Feb 5, 2021 08:02 EST)

Steven Palmese

CIO

Feb 5, 2021