APPENDIX A

Customer Name:	City of Aurora
Street Address:	44 E. Downer Place
City, State, Zip:	Aurora, IL, 60505

The Agreement referenced below by and between Sentinel Technologies, Inc., (Contractor) with principal offices at 2550 Warrenville Road, Downers Grove, Illinois 60515, and City of Aurora, an Illinois municipal corporation, (Customer) with principal offices at 44 E. Downer Place, Aurora, IL, 60505 is hereby amended to include the following:

Commencement Date	Agreement No.	Addendum No. 2021-01911-R4

1.0 Service Transition - Setup and Onboarding Scope of Work

The following describes the Services and Scope of Work for the transition process to utilize the contracted services.

A Sentinel Onboarding Coordinator will create a "MySentinel®" account for you. "MySentinel®" is the portal in which you will be able to access ServiceNow CSM, the Sentinel ticketing system, as well as, Enterprise Insight, the monitoring portal. There will be a welcome email from Sentinel's InfoSENter with temporary credentials.

The typical timeframe for onboarding, from kickoff to "go live", is approximately 30-45 days. Throughout the project, there will be reoccurring weekly meetings which will cover progress and updates. Depending on services purchased, additional meetings may be scheduled.

1.1 Discovery

Kickoff and MySentinel® Account Creation
During the kickoff meeting, Sentinel will review the contract and discuss the onboarding timeline at a high level. The items below are requirements that Sentinel will need from the Customer throughout this project to ensure successful onboarding. Sentinel will review and discuss these documents during the kickoff call, and they will be provided on the project SharePoint page, which is accessed through the MySentinel® portal. Please note that timely completion of these requirements will be essential to an efficient onboarding process and meeting the targeted "go live" date.

- Device List – **Required in first week**
- Credentials List – **Required in first week**
- Customer Notification Procedure – **Required one (1) week prior to go live**
- Letter of Agency – **Required in first three (3) weeks**
- Circuit ID Information – **Required in first three (3) weeks**
- Vendor List – **Required in first three (3) weeks**

IPSEC VPN Tunnel Building Session
The Tunnel Building Session is a live meeting that's scheduled during the kickoff meeting between Sentinel onboarding engineers and your point of contact for VPN connectivity and tunnel build.

Below lists the information that will need to be provided to the Sentinel onboarding engineers in order to build the IPsec VPN Tunnel used for always-on monitoring:

- Firewall vendor (Cisco ASA, Sophos, Palo Alto, Sonic Wall, etc.)
- Firewall's outside IP Address (A Public IP the tunnel will terminate to)
- Outside interface's name (WAN/outside/public/etc.)
- Name of existing crypto map (Cisco only - if applicable)

- Pre-shared key (This can be generated when building tunnel)
- Monitored Networks to allow over the tunnel (e.g. 192.168.0.0/24)

If increased encryption methods are preferred, please ensure the Sentinel team is made aware of this desire and it will use best efforts to accommodate if practicable.

Complete Onboarding Device Template
This list must provide all devices that Sentinel is to monitor and/or manage. Sentinel will review all systems, devices, and/or components to determine which candidates are to be: (i) onboarded per schedule, (ii) added to onboarding schedule, or (iii) out of scope. Any additions or subtractions to this list may result in changes to monthly billing and invoices.

Provide Sentinel Service Accounts (Credentials)
Sentinel will need access to in-scope devices via service account credentials both to configure the devices for the monitoring system as well as for ongoing troubleshooting and support.

Verify Device Access
Confirmation that we have access to monitor all devices listed in the contract.

1.2 Device Configuration

Sentinel will require Customer permission or change management, proper credentials, and access to the devices to proceed within the first two (2) weeks.

The following are configuration changes Sentinel onboarding engineers will execute on in-scope devices and systems:

- Configure Network Address Translation (NAT) statements.
- Configure Simple Network Management Protocol (SNMP) strings.
- Configure logging and traps.
- Configure firewall rules.
- Configure static routes.
- Identify and resolve any remaining connectivity issues.

Configure NAT Statements
In order to accommodate multiple customers that use the same private IP address spacing within their networks, Sentinel will assign each monitored device a unique polling IP address to be used within the Sentinel network. In order to accomplish this, Sentinel will configure a static 1-to-1 NAT statement on the Sentinel router for each monitored device. No IP address assignment or IP changes will occur on Customer's devices.

Configure SNMP Strings
In order to properly monitor devices within Enterprise Insight, Sentinel will enable/install SNMP on each device we are to monitor and manage. Sentinel will then configure an SNMP community string in order to communicate and poll information from each device.

Configure Logging and Traps
As a part of ensuring that all events are tracked and monitored within Enterprise Insight, Sentinel will configure each monitored device to send Syslog and SNMP trap information to Sentinel. These Syslog and trap messages will be used to generate alerts within the system when received.

Configure Firewall Rules
In order to establish connectivity to in-scope devices and systems, it may be necessary to configure firewall rules within Customer's network to allow Sentinel connections to pass through the environment. These changes would take place on firewall appliances, and in some cases, end point devices.

Configure Routing
The site-to-site VPN tunnel used to connect the Sentinel network to the Customer's network provides a means for IP connectivity to Enterprise Insight. As Enterprise Insight uses its own range of public IP address space, in some cases, it may be necessary to make adjustments to routing for these networks within your environment. This is done to resolve issues with return traffic, destined for the Sentinel networks, taking the wrong path back.

Identify and Resolve Any Remaining Connectivity Issues
Over the course of the Service Transition process, it is likely that the Sentinel team will uncover issues that may not have presented themselves prior. These issues may include anything from connectivity issues to devices or lost passwords, to hung services or devices. Depending on the issue, the remediation efforts could result in minor service disruption and/or additional service charges. Before any remediation is done, Sentinel will contact the Customer in writing, explain the problem, the recommended method to resolve the issue, and obtain written approval before making any changes.

At this time, all agreed upon systems are added to the remote monitoring and other management tools.

1.3 Access Verification, Troubleshooting, and Forms

Additional documents and forms to complete onboarding process:

- Customer Notification Procedure (CNP): This document will be used for Sentinel personnel to reference who to contact and when within the organization for certain monitoring alerts. This is what Sentinel NOC engineers will use to know who to contact during certain time periods and for differing levels of priority alerts. Sentinel reserves the right to limit the quantity of CNPs.
- Letter of Agency – Upon execution of this document, this will be used by Sentinel personnel as permission to act on the Customer's behalf during carrier incident handling with the ISP/circuit provider.
- Circuit Information – Any circuits that terminate to devices that require monitoring and/or management. Sentinel will need circuit ID information so troubleshooting can occur carrier related incidents.
- Vendor List – Contact information and devices for other vendors that may need to be contacted so that we can troubleshoot related incidents.

1.4 Enterprise Insight Tutorial and Pre-Go Live

Pre-go live activities include a web based Enterprise Insight tutorial of Customer's customized portal. Customer will have the ability to log in, see in-scope devices, and Sentinel will train Customer to navigate the site and answer any questions. Sentinel will have a representative of the Customer Service department provide a thorough tutorial of ServiceNow CSM and execute a pre-go live audit.

1.5 Go Live

System monitoring and alerts are active and monthly invoicing will begin.

1.6 Service Exclusions and Limitations

During the Discovery and Device Configuration phases, Sentinel requires information of a time sensitive nature for proper Service Transition. Should this information not be received in a timely manner, Sentinel reserves the right to increase the Service Transition fee to account for the additional efforts required. Customer will be notified prior to any service increases or changes.

2.0 Monitoring and Alerting

"Monitoring and alerting" are the systems and processes that monitor events that occur throughout the IT infrastructure and sends notifications to identified stakeholders when thresholds are reached or failures are detected.

2.1 Service Features and Inclusions

- 24X7X365 Monitoring System access.
- Up/Down Monitoring and Alerting for in-scope devices and systems.
- Device Monitoring and Analysis.
    - ICMP and SNMP polling.
    - Device availability statistics.
    - CPU, memory and disk space capacity and utilization.
    - Interface status, capacity and utilization.
    - Interface traffic, errors and discards.
    - Device response time and latency.

Historical Reporting
All data monitored and collected will be stored for a period up to one year. Reports can be run on a real-time basis via the NOC portal or e-mailed based on predetermined intervals. Reports such as Inventory, Performance Utilization, Availability and Past Events can be run at any point in time.

Syslog and Trap Collection
Sentinel will collect Syslog and/or Trap messages and will correlate with information gathered via polling so that the single best and timeliest alert is generated without duplicates, and with minimal delay.

Server and Application Monitoring
Sentinel will monitor critical applications that are running on the supported servers. Sentinel has 'templates' for most standard applications but is also available to provide custom application monitoring which may incur additional costs based on scope. Sentinel is able to leverage numerous protocols and methods. Examples include: SNMP, WMI, RPC, DB Queries, http gets, and others.

Monitored Elements

- Each device or system is allowed up to ten (10) elements to be monitored, as averaged over the total number of devices (i.e., some individual devices may have more than 10 elements, as long as the average number of elements per device over all devices is not greater than 10). If more elements are required, a Monitoring Change Request will be initiated and submitted. An “element” is an interface, memory, or disk drive.
- Elements and components to be monitored will vary based on criteria such as make and model of hardware or device, software version, service pack level, firmware version etc.
- When devices are removed from monitoring, they will be permanently removed from the web console, and historical data will not be available. Additionally, no alerts will be triggered.
- For hardware health reporting, Sentinel will poll server hardware directly from the Vendor Hardware Monitoring Agents. Supported vendors are: VMware, HP, Dell, IBM, and Cisco.
- Virtualization monitoring is at the hypervisor host level. The only data that will be provided are performance statistics that include CPU, memory, and network traffic for the host or virtual machines themselves.
- Windows Event Log Monitoring requires an agent to be deployed on Windows servers where the event logs will be monitored. This agent will forward Windows events to Sentinel’s monitoring infrastructure as a Syslog message.

2.2. Sentinel Responsibilities

- Provide a VPN or other secure network endpoint to enable Sentinel’s remote connectivity to in-scope devices and systems.
- Remotely assist customer with installing and configuring any data or asset collecting tools, if required.
- Abide by the Customer Notification Procedures (CNP) provided by the Customer during Service Transition.

2.3 Customer Responsibilities

- Provide an end point network device capable of supporting an IPSec site-to-site VPN.
- Provide Sentinel access to Customer devices documented in this contract. Access shall include, but is not limited to, device network reachability into and through Customer's network, proper device configuration to allow monitoring using any necessary protocols (including but not limited to ICMP, SNMP, HTTP, Telnet, RPC, SMB, and Syslog), and device credentials with sufficient rights to allow Sentinel to properly diagnose, troubleshoot, and resolve issues, depending on the contracted service. Sentinel shall not be responsible for any delays in discovering, alerting on, responding to, or resolving any issues on Customer devices due to Customer's failure to provide sufficient access to Customer devices. Further, Sentinel shall not be responsible for any delays in restoring any of Customer's device configurations due to any failure to provide sufficient device credentials or any changes to device credentials which impact the ability of Sentinel to back up the configuration of any Customer devices which Customer has contracted for Sentinel to back up.
- Promptly complete and provide any necessary documents, information, feedback, etc., reasonably required for the establishment of the service.
- Provide the environment necessary for any technical requirements needed by data and asset collection tools.
- Provide point(s) of contact accountable for information gathering, request response, onsite testing, or other activities in support of the Service Transition scope of work.
- Review and approve any documentation required by Sentinel to complete the Service Transition.

2.4 Service Exclusions and Limitations

The Monitoring and Alerting service does not include any support services on its own. Remediation of issues discovered through monitoring or an alert would be the responsibility of the Customer for all devices and systems that do not include support Managed Services. Customer may also utilize time and materials (T&M) or project services from Sentinel for issue resolution.

3.0 Incident Management

An “Incident” is defined as an event that could lead to loss of, or disruption to, an organization's operations, services or functions. Sentinel will identify, troubleshoot, and restore service to a normal functioning state when an incident is detected through Enterprise Insight or a service ticket to the Sentinel Customer Service Desk.

3.1 Service Features and Inclusions

- 24X7X365 Sentinel Customer Service Desk (CSD)
  - Acts as a single point of contact for all incident reports, service requests, updates, and notifications
- MySentinel® Customer Portal
  - Access for incident ticket submission, tracking, and reporting
- Event Management – Alerts from the monitoring system automatically submitted as Incidents
  - Utilizing Enterprise Insight to automatically create service tickets on impacted devices or systems when alerts are generated
- 3rd Party Liaison Support
  - Sentinel will provide management services and, if requested, will act as the Customer’s agent in attempting to resolve issues with other vendors or suppliers (e.g. maintenance outside of Sentinel’s preferred partners, circuit carriers, and software developers).
  - Carrier Incident Handling - Sentinel will work with circuit carriers on the Customer’s behalf if there is a circuit outage or degradation in service, if applicable. Sentinel will act as the liaison while providing continuous communication and troubleshooting updates.

3.2 Sentinel Responsibilities

- Incident ticket creation from detected events through Enterprise Insight or reported through the Customer Service Desk.
- Allocate a unique ticket number for tracking, follow-up, reporting, and closure.
- Consult with Customer to confirm the priority of the Incident.
- Notify relevant stakeholders about incident and keeping all parties updated through incident closure.
- Ensure incident tickets are routed to an appropriately skilled engineer for troubleshooting.
- Work ticket until incident is resolved and normal operation has been restored.

3.3 Customer Responsibilities

- Provide details about 3rd party support contracts and other documentation or authorization required for incident resolution.
- Immediately contact Sentinel via Customer Service Desk or through the MySentinel® Customer Portal if Customer believes an incident is actively occurring or has occurred.
- Raise or escalate any incidents to a higher priority via the Customer Service Desk only.

3.4 Service Exclusions and Limitations

- "Emergency Incidents" are excluded from this service. Emergency Incidents are categorized as events that are influenced by elements outside of standard operating conditions and/or procedures that require an urgent and immediate response beyond the scope of routine Incident Management. Examples of these elements include but are not limited to: facilities or building failures, security incidents such as malware or ransomware, or formal declaration of a disaster.
- Detection and/or remediation of security attacks, breaches, or issues on infrastructure are excluded from this service. Sentinel can provide security coverage through numerous additional options including, SECaaS, SOC, Managed SIEM and products within our SecuritySelect™ product portfolio.
- In the event that the Customer, or a third party hired by the Customer, incorrectly configures or otherwise makes a change to the environment resulting in an alert or service issue for which Sentinel's services are required for remediation, all remediation efforts will be billed on a time and materials (T&M) basis. T&M billing will commence only after exhausting the initial two-hour Move, Add, Change and Delete (MACD) limitation. A separate T&M agreement is required.
- In the event that the Customer, or a third party hired by the Customer, causes excessive false-positive monitoring alerts though interactions with systems covered by the Contractor, and without notifying Contractor of these interactions for proper alert management, then Contractor reserves the right to bill T&M for its response efforts. Customer will be notified in advance before any changes or additions to the invoice.

4.0 Problem Management

A "Problem" is defined as the unknown cause of one or more corresponding Incidents.

4.1 Service Features and Inclusions

Problem detection, logging, and prioritization.

4.2 Sentinel Responsibilities

- Correlate and organize Incident tickets related to the Problem.
- Characterize and prioritize the Problem and determine appropriate actions.
- Provide recommended actions or action plan to the Customer for review and/or approval.
- Deploy a permanent fix utilizing the Change Management process, when applicable.
- Review Problems and analyses during the periodic review meetings determined during Service Transition.

4.3 Customer Responsibilities

- Provide any additional information regarding the in-scope device or system related to the Problem, as needed.
- Coordinate with third party vendors and organizations to address issues where a third party device or system is the cause of the Problem.

4.4 Service Exclusions and Limitations

Not applicable.

5.0 Change Management and System Administration

A "Change," is defined as an event that is an approved request by the Customer (tracked via ticket), implemented with a minimum and accepted risk to IT infrastructure, and results in a new configuration or status of one or more in-scope devices or systems. Sentinel will manage the deployment of technical changes to in-scope devices or systems as a result of Service Requests.

5.1 Service Features and Inclusions

Service Request and Device Administration
Routine, day-to-day administrative tasks will be performed on Customer's systems on a 24x7x365 basis. All Service and MACD (Move, Add, Change, Delete) Requests will be performed remotely by the engineering team. Unlimited Service and MACD Requests are included that are capable of being performed within a two (2) hour time frame.

Patch Management
Sentinel will perform preventative maintenance while adhering to the Customer's change control window and approval process. A schedule for minor release updates will be determined during the Service Transition process. Otherwise, server patches will be reviewed and applied monthly. Any other device may be reviewed upon request and within Sentinel's sole discretion. Sentinel will adhere to the following policies regarding device software and updates:

- Sentinel may require agents to be installed onto servers for automated patching.
- Sentinel will install minor software releases when requested by Customer or recommended by Sentinel. A minor software release is defined as an incremental release of Software that provides maintenance fixes, that, within Sentinel's sole discretion, is capable of being performed within a two (2) hour time window.
- Sentinel reserves the right to update Customer's device software revision level if the installed revision level is no longer supported by the device manufacturer.
- Sentinel reserves the right to update the Customer device software to fix software bugs in the existing version.
- When adding new devices to the Customer's existing network, Sentinel follows industry best practices and, therefore, reserves the right to install the new devices with the same version of software running on other similar or interconnected devices in order to avoid creating incompatibility issues across the environment.
- Sentinel will install operating system patches as reasonably necessary to ensure the security of the Customer's infrastructure.

5.2 Sentinel Responsibilities

- Manage the lifecycle of Service Requests.
- Coordinate and execute changes to in-scope devices and systems using commercially reasonable efforts to minimize any adverse impacts to Customer's environment.
- Validate and prioritize Service Requests, where applicable.
- Provide notifications of change request start and completion for Customer impacting changes.

5.3 Customer Responsibilities

- Faithfully execute Customer's change management process prior to submitting any Service Requests, where applicable.
- Notify Sentinel of any informational changes (e.g. new vendor or renewed warranty contract).
- Submit Service Requests through the Customer Portal or the Customer Service Desk.
- Confirm and maintain scheduled maintenance windows for change activities.
- Review, discuss, and make decisions on any changes requested or required by Sentinel.

5.4 Service Exclusions and Limitations

- Customer has a current manufacturer's product-support and/or warranty contract that grants rights to use and access updates and patches. Sentinel reserves the right to refuse to patch or update any systems not covered under a current product-support and/or warranty contract.
- Service Requests are defined as an activity that can be completed remotely within a **maximum of two (2) hours per request** on current covered inventory. If, at Sentinel's sole discretion, it is determined that a Service Request will extend beyond the two-hour maximum, the Customer will be notified and will be offered at least one of the following options:
    - Sentinel will provide a non-binding estimate of the effort necessary to complete the work on a time and materials (T&M) basis. T&M billing will commence only after exhausting the initial two hour Service Request limitation.
    - Sentinel will provide a quote to perform the work as a fixed-fee project under a separate SOW.
- If Customer opts out of patch management, Sentinel requires this request in writing and Customer acknowledges that by opting out of the aforementioned patching being recommended by Sentinel, it may expose its network and systems to security vulnerabilities, and Customer elects to opt out of patching with Sentinel despite such security risks. Customer understands that Sentinel shall not be liable for any damages of any kind to arise from any security breach or system outage to result directly or indirectly from the unpatched software, and Customer agrees to indemnify and hold Sentinel harmless from any claims or damages that may arise out of such.
- If Customer has Windows or Linux servers, which are still supported by the manufacturer, that are behind patching schedule by six-months or longer, the first round of patching must be completed as a project or T&M engagement.
- Sentinel will not be required to install minor software updates until they are validated by Sentinel and the parties agree there is a business need for the update.
- Sentinel will not be required to install updates, such as firmware, onto physical devices, such as routers or switches, until they are validated by Sentinel and the parties agree there is a business need for the update.

6.0 Configuration Management

Sentinel will backup and manage the configurations of supported devices with a command line interface (CLI).

6.1 Service Features and Inclusions

Configuration Backups
Device configurations with a CLI will be backed up nightly from Sentinel's network configuration management tool and stored when a change has occurred.

Configuration Restoration
In the event of a critical failure or outage, in-scope systems or devices that have a backed up configuration will be restored with that configuration to restore service functionality. The following restoration methods will be used:

- Sentinel will restore the most recent configuration stored from the automated configuration management tool, or a version requested by the Customer.
- Sentinel will be unable to provide system restoration on Unified Communication (UC) servers that Sentinel is not permitted to backup. Sentinel will not monitor or control any UC backups, unless otherwise determined by mutual agreement between the parties.

6.2 Sentinel Responsibilities

- Implement and manage a configuration management system that will backup and archive the configurations of in-scope devices.
- Backup the configuration of supported in-scope devices.
- Restore the configurations to those devices as needed.

6.3 Customer Responsibilities

Provide access to in-scope devices to backup current configurations.

6.4 Service Exclusions and Limitations

- In the event that configuration data needs to be restored, Sentinel will only be responsible for restoring to the last validated restore point, and there is no guarantee that Sentinel will be able to restore all Customer configuration data.
- Limited to configuration data only on supported CLI devices. All operational data such as document files, virtual server data are not in scope.

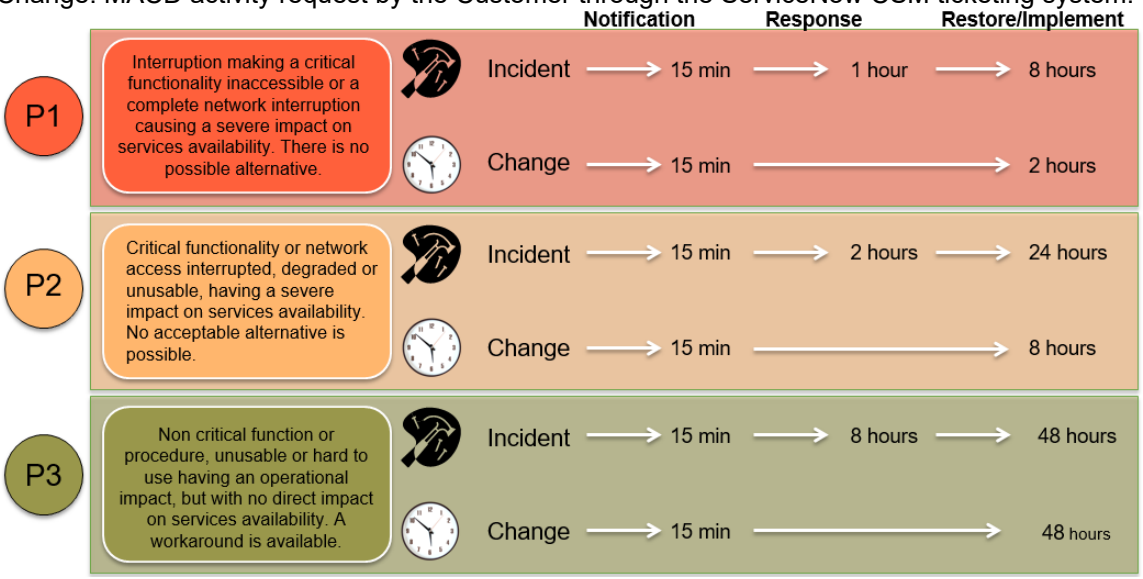
7.0 Service Level Agreements and Quality Assurance

7.1 Sentinel's NOC Monitoring Server Infrastructure

- 99% detection and alerting of network events and incidents.
- 99% availability of all network monitoring and management systems.
- 99% active SNMP (Simple Network Management Protocol) and/or ICMP (Internet Control Message Protocol) polls to all available monitored devices completed within each devices polling cycle.

7.2 Sentinel Managed Services Customer SLAs

- 99.5% Commitment on SLAs.
- Incident: an alert generated by the Sentinel NOC, such as an outage or any other unplanned interruption to service.
- Change: MACD activity request by the Customer through the ServiceNow CSM ticketing system.



Definitions

- **P1** – Interruption making a critical functionality inaccessible or a complete network interruption causing a severe impact on services availability. There is no workaround or alternative.
- **P2** – Critical functionality or network access interrupted, degraded, or unusable, having a severe impact on services availability. No acceptable alternative is possible.
- **P3** – Non-critical function or procedure unusable or hard to use having an operational impact, but with no direct impact on services availability. A workaround is available.
- **Notification** – An opened Incident or Change request ticket is acknowledged by the Sentinel Service Desk. This includes monitoring and alert system generated Incidents.
- **Response** – Communication to the proper stakeholder(s) of an estimated resolution time
- **Mean Time to Restore** – Time in hours taken to restore the interrupted service. Measurement begins at the time of Notification.

7.3 Uptime and Maintenance Windows

Sentinel NOC system is built for 99.999% redundancy. Enterprise Insight guarantees the NOC environment uptime shall be 99%. The system will be updated/patched by Sentinel on the third Saturday to Sunday of each month from 10:00 p.m. to 6:00 a.m., on a monthly basis. This will include the server infrastructure, as well as network infrastructure. This plan will consist of the following information:

- Device being updated.
- Updates being installed.
- Impact to the environment.
- Process for removing update that was installed.
- Criteria for a successful update.
- Process for testing the environment when back online.
- Person performing the update.

7.4 Quality Assurance and Customer Experience

Sentinel's Quality Assurance (QA) team may host QA meetings and/or provide periodic reports to review trends and performance of monitored data, as well as business and project planning and forecasting. The exact meeting frequency will be determined mutually during Service Transition.

8.0 General Provisions, Limitations, and Exclusions

    - Upon the execution of a separate Time & Materials (T&M) Agreement between the Parties, Contractor may perform Support Services outside of the scope of this Agreement.
- If, within 30 days of Service Transition kick off, the Customer environment is determined by Sentinel to be in an unsupportable and/or unstable state, Sentinel may require that the Customer undergo additional services to remediate, at its current T&M rates. For that avoidance of doubt, all pre-existing issues/conditions are out of the scope of this contract.
- Specific elements to be monitored and alerted on are determined during the Service Transition process. These elements are variable based on device types, software versions and other factors.
- Sentinel configures event types and thresholds in accordance with best practices, which are available on request. Any custom event types or thresholds may be included at an additional charge.
- Unless otherwise included in this or a separate contract, Sentinel will provide all services remotely only. Unless otherwise stated within this contract, no on-site support is included in the base fees.
- Customer acknowledges that the Services do not provide a guarantee or warranty of complete protection against security breaches or attacks.
- The recording and/or monitoring of incoming and outgoing telephone calls between Contractor and Customer will be undertaken by Contractor, subject to the consent of all parties to such calls, for the purpose of providing constructive performance feedback, pursuing complaints, taking corrective action, measuring satisfaction or for any other purpose Contractor deems relevant to improving customer service.
- Sentinel is not responsible for outages due to acts of God or nature.

- Sentinel is not responsible for third-party telecommunications carrier outages that cause the system to become offline or outages of third-party utilities providers.
- The Customer is responsible for all licensing of third-party products used by Customer.
- All managed devices and systems will have a current manufacturer's product-support and/or warranty contract in place. At Sentinel's sole discretion, systems not covered by a manufacturer's product-support and/or warranty contract will be managed on a "best effort," basis and will not be included in SLA commitments.
- Customer is responsible for informing Contractor as to whether Contractor may process, store, or transmit any credit card holder data in its performance of these services.
- Sentinel's participation in any Customer scheduled recurring meetings is not in scope.

8.1 Hardware Upgrades

As part of the Services provided under this statement of work Sentinel will track and analyze performance statistics to ensure the Customer's network is operating optimally. If Sentinel determines a network device is experiencing a performance issue, Sentinel will recommend appropriate action. Customer will be responsible for any and all charges incurred to upgrade the hardware, including charges for installation services. In addition, if any of Customer's network devices are deemed to be "end of life" (i.e., is no longer supported), as determined by the equipment manufacturer, Sentinel shall promptly notify Customer, and it will be the Customer's responsibility to remove the device from the network or replace it with a supported device. In such case, Customer will be responsible for any and all charges incurred to upgrade the hardware, including charges for installation services. In this scenario, Sentinel will provide support on a best-effort basis.

8.2 Software Upgrades

Major software upgrades are not included in this contract. A major software release is defined as a release of software that provides additional software functions.

- If Customer directs or approves the implementation of any manufacturer software upgrades, Sentinel will perform such implementation for additional charges (at Sentinel's then-current rates).
- In the event that an upgrade has been deemed critical or mandatory by the Manufacturer or Sentinel, it is expected the Customer will comply and will upgrade the environment to the new software. Sentinel will apply a reasonable standard to the process of determining whether an upgrade is critical or mandatory, and only those upgrades required to remedy a potentially serious system performance or security issue will be considered. If the Customer refuses to make a recommended upgrade, Sentinel will no longer be held responsible for the performance or security of the network, and Sentinel will provide support on a best-effort basis and those devices will not be covered under SLA commitments.

8.3 Supported Applications

The Pricing Summary, attached hereto, lists the services and applications that will be supported under this contract. Exhibit 1, attached hereto, lists examples of additional services and applications that may be supported under this contract, if requested to be added by Customer. Any service or application outside of Exhibit 1 that Customer requests to be included must be approved by Sentinel in writing, in Sentinel's sole discretion.

Solution-Specific Terms & Assumptions

Terms & Assumptions

- Any additions or deletions to the covered inventory during the term of this Agreement will be adjusted monthly, as required, and reflected in the subsequent monthly invoice provided to the Customer. These changes may incur an additional NRC for onboarding or offboarding. If any such deletions result in a decrease of 10% or greater of the initial MRC, Contractor reserves the right to reassess any discount applied to the ongoing MRC, within its sole discretion.

Pricing Summary

The provisions of this Appendix A shall commence on the date of signature below and shall continue for a Term of 36 months, and shall automatically renew for subsequent periods of the same length as the initial Term unless either party gives the other written notice of termination at least thirty (30) days prior to expiration of the then-current Term.

SUMMARY

One Time Setup Fee:	$3,979.00
Monthly Sub-Total:	$9,142.00
Customer Discount:	8.26 %
Monthly Total:	**$8,420.11**

SENTINEL MANAGED SERVICES

INFRASTRUCTURE

Product	*Location*	*Quantity*	*Comments*
WAN Routers-Voice Gateway		4	2900 Series Voice Gateways

SERVERS & VIRTUALIZATION

Product	*Location*	*Quantity*	*Comments*
Hypervisor		2	ESXi 6.7

SUPPORT SERVICES

Product	*Location*	*Quantity*	*Comments*
Service Fee		1	

VOICE & COLLABORATION

Product	*Location*	*Quantity*	*Comments*
Call Manager-Publisher		1	
Call Manager-Subscriber		2	
Call Manager-Voice Users/Handsets		1050	estimated including ATAs
Call Manager-Voice Users/Handsets		16	TP Units / Codec
Call Manager - UC BaaS		1	
Unity		1	
Unity-Redundant		1	
Unity - UC BaaS		1	
IM & Presence		1	
IM & Presence-Redundant		1	
IM & Presence - UC BaaS		1	
E911-Emergency Responder		1	CER
E911-Emergency Responder-Redundant		1	CER
E911 - UC BaaS		1	
UCCX		1	
UCCX-Redundant		1	
UCCX - Contact Center Agents		21	
UCCX - UC BaaS		1	
Telepresence		1	Telepresence Conductor
Other UC Server		1	Webex Meeting Server
Other UC Server		2	Expressway - Core
Other UC-Redundant		2	Expressway - Edge

General Terms and Assumptions

- With regard to any software licenses installed by Contractor as necessary to effectuate the provision of services under this Agreement, thus not within the scope of the deliverables, Customer is hereby prohibited from duplicating said software in any form or fashion and is further restricted from using the software beyond the intended scope set forth herein. Moreover, Customer is restricted from licensing, sublicensing or transferring said software to any third party (except to a related party) without the express permission of Contractor, under which circumstance the software shall stay under the control and auspices of the Contractor. In the event Customer loses or damages the software, a copy may be provided at a nominal charge. Contractor may, at its discretion, remove said software upon the completion of its provision of services. Alternatively, at the end of this engagement or the license period, whichever occurs first, Customer is required to either destroy or return all copies of said software to Contractor, as expressly directed by Contractor.
- The manufacturer/support provider has the right to inspect any products that have either never had support coverage or have not had support coverage for an extended period to determine their eligibility for maintenance/support. Devices subject to inspection will be flagged as such and are subject to a non-refundable inspection fee, which shall be the responsibility of Customer. Sentinel will work with the manufacturer/support provider on Customer's behalf until device eligibility is determined. Devices that do not pass the inspection will be ineligible for support.
- For products purchased pursuant to this agreement, Contractor agrees to provide storage at no additional charge for up to 90 days. If the storage period exceeds 90 days, Customer agrees to the following: a.) Customer will be responsible to pay a fee of 2% per month for storage of purchased products from that point forward, b.) Customer will be invoiced and will be responsible to pay the unpaid balance for any products purchased from Contractor that have not been paid in full and, c.) Ownership will transfer from Contractor to Customer.
- For all products purchased, it is assumed that prior to order execution with Contractor, Customer has reviewed, understood, and agreed to each manufacturer's respective terms and conditions governing the purchase of products, including, but not limited to, applicable warranties, order cancellation, and return policies. In the event of a return request, Sentinel may assist Customer by facilitating the request between Customer and the manufacturer. In addition, product return requests will be subject to Sentinel's own return policies, which may include restocking fees and/or shipping and handling costs.
- The Contractor shall provide an invoice to the City for services rendered and the City shall approve and thereafter pay any undisputed portions thereof in accordance with the Illinois Local Government Prompt Payment Act, 50 ILCS 505/1 et. seq. Approved, but unpaid invoiced amounts shall accrue interest in the manner and to the extent authorized by the Act.
- Sentinel makes no guarantees with respect to this product's compliance with any local, state, or federal privacy laws, including, but not limited to, the Biometric Information Privacy Act (BIPA) and the California Consumer Privacy Act (CCPA), and Customer shall maintain all responsibility and bear all liability with regard to its compliance with such in relation to its use of this product. Customer shall indemnify and hold harmless Sentinel from any third party claims to arise out of any privacy violations with regard to this product.

Payment Terms

All Invoices: Net 30

The provisions of this Appendix A's Pricing Summary replace, govern, and control over any conflicting terms in the Master Service Agreement, and these terms shall commence on the date of signature below and shall continue for a Term of 36 months.

This quote is valid for 30 days from 1/6/2023

*Regarding the resale of any products, pricing may be subject to a manufacturer price increase before the expiration date of the quote.

CUSTOMER:
City of Aurora

Signature: _____

Printed Name: _____

Title: _____

Date: _____

P.O. #:_____

CONTRACTOR:
Sentinel Technologies, Inc.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Exhibit 1

Vendor	Product
AlienVault	USM sensor
AlienVault	USM server
AMI	MegaRAC (BMC)
Apache Foundation	Apache Web Server
APC	PowerNet (UPS)
APC	PowerNet (PDU)
BlackBerry	Enterprise Server
Check Point	Connectra
Cisco	ACS
Cisco	Calabrio Workforce Management
Cisco	CallManager
Cisco	CallManager
Cisco	CallManager
Cisco	Customer Voice Portal Server
Cisco	DMP
Cisco	Duo Security Authentication Proxy
Cisco	Cisco Enterprise License Manager
Cisco	Emergency Responder
Cisco	Unified Contact Center Enterprise Intelligent Contact Manager Server
Cisco	IP Contact Center
Cisco	Unified Contact Center IP Interactive Voice Response
Cisco	IM & Presence
Cisco	Unified Contact Center Enterprise Server
Cisco	Unified Call Center Express
Cisco	Umbrella Connector
Cisco	Unity
Cisco	Unity Connection
Cisco	Voice Gateway Utilization
Citrix	Virtual Apps and Desktops
Dell	EqualLogic Storage
EMC	Celera AntiVirus Agent (CAVA)
EMC	ScaleIO Metadata Manager (MDM)
EMC	ScaleIO Data Server (SDS)
EMC	ScaleIO Tie-Breaker (TB)
EMC	ScaleIO Utilization
Generic	DHCP server
Generic	DNS server
Generic	Pound
Generic	RADIUS server
Generic	SMTP server
Generic	SSH
Generic	SSL/TLS Certificate
Generic	tinyproxy
Generic	Varnish
Generic	Web server
Genesys	Contact Center
Hyland	Onbase
InnerApps	IDSync
Legato	DiskXtender
Legato	EmailXtender
Liebert	DS Heating/Cooling Unit
Microsoft	Active Directory

Vendor	Product
Microsoft	Azure Site Recovery Configuration Server
Microsoft	Azure Site Recovery Windows Master Target
Microsoft	Communications Server
Microsoft	Dynamics CRM 2016
Microsoft	Exchange 2003
Microsoft	Exchange CAS 2007
Microsoft	Exchange Edge 2007
Microsoft	Exchange Hub 2007
Microsoft	Exchange Mailbox 2007
Microsoft	Exchange Unified Messaging 2007
Microsoft	Exchange CAS 2010
Microsoft	Exchange DAG 2010
Microsoft	Exchange Edge 2010
Microsoft	Exchange Hub 2010
Microsoft	Exchange Mailbox 2010
Microsoft	Exchange CAS 2013
Microsoft	Exchange DAG 2013
Microsoft	Exchange Mailbox 2013
Microsoft	Exchange CAS 2016
Microsoft	Exchange DAG 2016
Microsoft	Exchange Mailbox 2016
Microsoft	Windows Hyper-V
Microsoft	IIS
Microsoft	Remote Desktop Services Broker
Microsoft	Remote Desktop Services Session Host
Microsoft	SharePoint 2010
Microsoft	SharePoint 2016
Microsoft	Skype for Business 2015 Edge
Microsoft	Skype for Business 2015 Front End
Microsoft	Skype for Business 2015 Mediation
Microsoft	Skype for Business 2015 Persistent Chat
Microsoft	SQL Server 2005
Microsoft	SQL Server 2008
Microsoft	SQL Server 2012
Microsoft	SQL Server 2014
Microsoft	SQL Server 2016
Microsoft	SQL Server - Legacy
Microsoft	Windows
Microsoft	Windows Domain Controller
Microsoft	Windows Print Server
Microsoft	Windows DHCP server
Microsoft	Windows DNS server
Microsoft	Windows
MySQL	MySQL server
Open Source	Linux
PostgreSQL	PostgreSQL server
Pure Storage	FlashArray//M
Safari	Montage
Sagemcom	XMediusFAX
SAP	BPC
Schneider Electric/Sinetica	Eagle-i Rack Monitoring Unit (PDU)
SolarWinds	Orion NetFlow Traffic Analyzer back-end
SolarWinds	Orion (polling engine)
Symantec	Backup Exec Agent for Windows
Symantec	Backup Exec Server

Vendor	Product
Symantec	Backup Exec Agent for Windows
Symantec	Backup Exec Server
Symantec	NetBackup
Titan	FTP server
Trend Micro	OfficeScan server
Tripp Light	Power Distribution Unit
Veeam	Agent for Windows
Veeam 7	Backup
Veeam 8	Backup
Veeam 9	Backup
Veeam ONE	ONE
Verint	Verba
VMware	vCenter