DATA SHIELD® MANAGED SECURITY SERVICES ORDER FORM

This "**Order Form**" is between Data Defenders, LLC ("**Data Defenders**") and the City of Aurora, Illinois ("**Customer**"), together the "**Parties**", and incorporates by reference and is governed by the terms and conditions of the Master Security Services Terms and Conditions Agreement MSSTC No.: 20190213-01-DS. Capitalized terms used and not otherwise defined in the Order Form or Services Catalogue have the meaning set forth in the Master Security Services Terms and Conditions Agreement.

Customer acknowledges and agrees to all terms of this Order Form, the Master Security Services Terms and Conditions Agreement, and the service particulars outlined herein (together, the "**Agreement**"). Customer and Data Defenders have executed this Order Form on the date of the last signature (the "**Effective Date**").

1. **TERM AND TERMINATION.** The initial term and renewal terms of this Order Form are as set out herein:

   a. The term of the Services shall begin on January 1, 2021 and will be referred to as the "**Service Commencement Date**" and will continue for thirty-six (36) calendar months ("**Initial Term**");

   b. Prior to the expiration of the Initial Term, the Customer must submit a Renewal Request to Data Defenders no less than one-hundred and twenty (120) days prior to the expiration of the Initial Term or the Renewal Term to renew this Order Form. Customer shall be granted two (2) optional twelve (12) consecutive calendar months period extensions each (each a "**Renewal Term**") at the then prevailing rates. The Initial Term and any Renewal Term may be referred to collectively in this Order Form as the "**Term".**

   c. If Customer wishes to terminate this Order Form at the end of the then-current Term, Customer may do so by providing Data Defenders with written notice at least one hundred and twenty (120) days prior to the end of the current Term of its intention not to enter the Renewal Term;

   d. The expiration of any thirty-six (36) consecutive calendar month period beginning from the Service Commencement Date shall be known as an "**Anniversary Date**", and any twelve (12) consecutive calendar month period from the Service Commencement Date or any Anniversary Date shall be known as a "**Contract Year**";

   e. Suspension of Services. Data Defenders reserves the right to suspend performance of the Services with immediate effect in the event Customer is more than forty-five (45) days overdue in payments that have not been disputed in good faith by Customer; and

   f. This Order Form will continue for the Term set out herein.

2. **SERVICE FEES**. All Fees are in USD. Customer confirms the below scope and acknowledges that pricing is based on the below scope. Customer agrees to place additional orders for any material increase to such scope and acknowledges that additional Fees shall apply for any increases in scope.

3. **RENEWAL TERM PRICING.** Upon expiry of the Initial Term, then-current prices for the Services will apply and will be payable on an annual basis. Notice of increase in pricing for Renewal Terms

will be provided by Data Defenders to Customer not less than ninety (90) days before commencement of each Renewal Term.

4. **PAYMENT TERMS.** Fees are exclusive of all taxes and other applicable services fees. Payment for services will be billed to Customer according to the cycle indicated in the "Billing" column of the Order Form Pricing table. For Service components that are marked with the indicator of "Pro. Serv." in the Category column of the Order Form Pricing table, services will be billed on an "As Incurred" basis. For Service components that are marked with the indicator of "License" in the Category column of the Order Form Pricing table, Services will be billed on an "Annual" basis at the beginning of each Contract Year. Payment for Services billed on an annual basis for each Contract Year will be billed to Customer no more than thirty (30) days before the commencement of each Contract year and payment for Services for each Contract Year will be due fifteen (15) days before the commencement of each Contract Year. Payment for services billed on an "As Incurred" basis will be due no more than thirty (30) days from the date of the invoice submission. Payment for Services for each Renewal Term will be billed no more than thirty (30) days before the commencement of each Renewal Term and will be due fifteen (15) days before the commencement of each Renewal Term. The first payment is due upon the Effective Date.

5. **PROFESSIONAL SERVICE TASK HOURS.** Professional service task hours are pre-allocated, annually allotted units of hours assigned to specific professional services tasks as shown in the Order Form Pricing table below. These units of hours are indicated by the marking of "Pro. Serv." in the "Category" column of the Order Form Pricing table. Customer may use these annual allotment of hours at any time within the current Contract Year but may not carry over unused hours within any professional services task allotment to a new Contract Year unless otherwise indicated in section 5ii of this Order Form. The following additional stipulations for usage of hours will apply to professional service task hours allocated on this Order Form.

   i. **REDISTRIBUTION OF PROFESSIONAL SERVICE TASK HOURS.** During any current Contract Year, Customer may redistribute unused professional service task hours from one professional services task to any other professional services task within the same Contract Year.

   ii. **ROLLOVER OF PROFESSIONAL SERVICE TASK HOURS.** Customer may not rollover unused professional services task hours from the current Contract Year to the next Contract Year. However, a rollover exception will be made for the following professional services tasks as long as they are included in the Scope of Services and pre-paid on an annual billing cycle by the Customer as indicated in the Order Form Pricing table below.

   - Incident Response Professional Services Task
   - Network Management Professional Services Task

   Pre-allocated and unused hours for the professional services tasks indicated in this section 5ii may be rolled-over to the next Contract Year. Rollover of hours will be allowed one-time during the Initial Term; unused hours that are rolled over from the current Contract Year to the next Contract Year can only be assigned to the same professional services task in the next Contract Year.

iii. **REALLOCATION OF PROFESSIONAL SERVICE TASK HOURS.** It is understood by all Parties to this Order Form that the allocation of hours as shown for each professional services task indicated in the Scope of Services for this Order Form may not accurately represent the appropriate amount of time required to complete service delivery within a Contract Year for each professional services task. Per the MSSTC Agreement, all Parties to this Order Form understand that Customer, being the benefactor of the professional services tasks provided in this Order Form, maintains the final decision-making control and flexibility to determine how these hours will be used within each Contract Year. It is additionally understood and agreed upon by all Parties to this Order Form, that upon the complete exhaustion of the annual allocation of hours for any in-scope professional services task as indicated in the Order Form Pricing table below, Data Defenders will immediately terminate all work activities for those active tasks. It is understood that Data Defenders will resume work activities upon the reallocation of the required hours by Customer to complete any active work task where a work stoppage has occurred. Therefore, to provide Customer with the opportunity to avert any potential work stoppage by Data Defenders, Data Defenders agrees to provide notice to Customer's Authorized Contact when 85% of the annual allocation of hours for any in-scope professional services task defined under this Order Form has been exhausted.

6. SERVICES

iv. **STANDARD MAINTENANCE AND SUPPORT**: Customer acknowledges and agrees to the following standard maintenance and support terms and conditions found in the Services Catalogue at https://contracts.Data-Defenders.com/Data-Defenders-services-catalogue/

v. **MDR SERVICES:** Customer acknowledges and agrees to the General MDR Services Responsibilities found in the Services Catalogue at https://contracts.eSentire.com/eSentire-services-catalogue/managed-detection-and-response-mdr-services/

a. **esENDPOINT Detect and Respond Powered by CrowdStrike Services:** Customer agrees to the esENDPOINT provisions as described in Schedule A and to the service particulars as described in the Services Catalogue at https://contracts.eSentire.com/eSentire-services-catalogue/managed-detection-and-response-mdr-services/esendpoint-powered-by-crowdstrike-inc-services/

b. **esNETWORK Services:** Customer agrees to the esNETWORK service particulars found in the Services Catalogue at https://contracts.eSentire.com/eSentire-services-catalogue/managed-detection-and-response-mdr-services/esnetwork-services/

c. **Data Shield Sentinel Security Event Information and Device Management:** Customer agrees to the Data Shield Sentinel SEIM and Device Management service particulars found in the Services Catalogue at https://contracts.data-defenders.com/data-defenders-services-catalogue/data-shield-sentinel-SEIM/

d. **Data Shield Vulnerability Management:** Customer agrees to the Data Shield Vulnerability Management service particulars found in the Services Catalogue at https://contracts.data-defenders.com/data-defenders-services-catalogue/data-shield-vulnerability-management/

e. **Data Shield Professional Services:** Customer agrees to the Data Shield Professional Services service particulars found in the Services Catalogue at https://contracts.data-defenders.com/data-defenders-services-catalogue/data-shield-professional-services/

7. **SERVICE LEVEL AGREEMENTS (SLA).** This SLA defines the Service Levels provided in relation to Data Defenders' Data Shield Managed Security Service and is subject to our Managed Security Services Master Terms and Conditions (MSSTC). This SLA must be agreed upon by both Data Defenders and the Customer. This SLA defines which services the SLA includes, performance and other requirements of Service provisioning and delivery, and how reporting of the delivery must be performed. Remedies for Data Defenders not meeting the requirements are defined in this SLA. Customer must at all times cooperate with Data Defenders in determining and verifying that a qualifying Service outage has occurred.

a. **Responsibility and formal organization for Data Shield MSS Service Delivery**. Individuals assigned to this engagement can perform more than one of the following roles when required. The following roles need to be appointed within the Customer and Data Defenders to serve as the basis of fulfilling the Scope of Services and the mutually agreed upon SLA outlined in this Order Form:

i. Data Shield SOC team lead (DD SOC Manager)

- Responsible for managing the SOC services and reporting to the Customer.

ii. Data Shield SOC analysts (DD SOC Technician)

- Responsible for delivering the SOC services to the Customer.

iii. Data Shield Incident Manager, Data Defenders (Incident Manager)

- Can be the SOC team lead. Manages incidents and escalation of incidents when required (when manual handling of incidents is needed). Responsible for communicating directly with the Customer's Incident Manager.

iv. Incident Manager, Customer (Customer Dir. of Cyber and Technology Risk)

- Responsible for communicating with Data Defenders and coordinating when incidents that need manual handling occur.

v. Data Defenders Engagement Manager

- Responsible for contract management at Data Defenders. Will also serve as its document owner. Responsible for arranging periodic status meetings with the Customer.

vi. Data Defenders Engagement Manager

- Responsible for monitoring SOC service delivery and facilitating all service level communications with Customer. Responsible for communicating status of SOC services internally at Data Defenders.

vii. Data Defenders Engagement Manager (Change Management)

- Responsible for coordinating delivery of services during change management situations both internally and with Customer.

viii. Customer Dir. of Cyber and Technology Risk (Change Management)

- Responsible for communicating with Data Defenders when implementation of changes are required.

ix. **Data Defenders Business Development (DD Regional SOC Business Development)**

- Responsible for the service delivery budget, contract, and SLA.

b. **SLA Credit Request Process and Limitations.** In order to receive an SLA credit (specified herein) for Service, an Authorized Customer Contact must immediately notify Data Defenders' designated Engagement Manager (EM) of an occurrence within the Data Shield Service that results in the inability of the Customer to access Service ("Service Outage"). A Service Outage does not include an outage that occurs during Scheduled Maintenance. Data Defenders' designated EM will investigate the reported outage and assign a Service Request number. If the EM is able to substantiates the Service Outage that could qualify Customer for the SLA credit ("Verifiable Service Request"), then Customer may request a Service Credit within thirty (30) days after the event giving rise to the credit by contacting the Data Defenders EM and requesting an SLA credit escalation. A Verifiable Service Request must accompany Customer's request for any SLA credit regarding the Service purchased by Customer. Credits will appear on Customer's bill for the Service within sixty (60) days of the SLA credit request, after such SLA credit has been approved by the Data Defenders EM.

If Data Defenders has been found to be out of compliance with agreed SLAs at the conclusion of a qualified service outage investigation request initiated by Customer, Customer will have the following remedies to cure any verified breach of SLAs:

a. Customer shall be credited for the cost component associated with the specific stream of service where the service outage occurred. The service cost credit will be 3% of the monthly Data Defenders cost per service outage instance. The following service credit stipulations shall apply:

i. If the Service that experienced a qualified and verified service delivery outage, and is determined to be eligible for a service credit by the Data Defenders EM, and the cost for that service is billed to the Customer on an Annual Billing Cycle, the monthly Service cost will be determined by dividing the Annual Service cost by 12 to determine the Data Defenders monthly cost for service delivery.

ii. If the Service that experienced a qualified and verified service delivery outage is determined to be eligible for a service credit by the Data Defenders EM, and the cost for that service is billed to the Customer on a Monthly Billing Cycle, the SLA service credit will be determined by using monthly Service cost for the affected Service.

iii. During any Contract Year, Customer's aggregated SLA service credits may not exceed a total of 10% of the monthly cost for the Service where delivery was determined to be out of compliance.

iv. For purpose of calculating SLA credits, this monthly Service cost shall mean the monthly recurring charge (or the calculated monthly charge for Services billed on an Annual Billing Cycle) for such Service, but excluding, in all cases, (i) any monthly recurring fees for the Service features (e.g., domain name hosting or e-mail Service), (ii) all one-time charges, and (iii) at all times excluding the monthly recurring charge attributable to Equipment for such Service. Credits are exclusive of any applicable taxes or fees charged to the Customer or collected by Data Defenders.

c. **SLA Exclusions**

a. **Global SLA Exclusions.** SLAs do not apply and Data Defenders is not responsible for failure to meet an SLA resulting from:

i. Misconduct of Customer or Users of Service.

ii. Failure or deficient performance of power, Equipment, Services, or systems not provided by Data Defenders.

iii. Delay caused or requested by Customer.

iv. Service interruptions, deficiencies, degradations or delays due to any access lines, cabling, or equipment provided by third parties.

v. Service interruptions, deficiencies, degradations, or delays during any period in which Data Defenders or its representatives are not afforded access to the premises where access lines associated with Service are terminated or Data Defenders Equipment is located.

vi. Service interruptions, deficiencies, degradations, or delays during any period when a Service Component is removed from Service for maintenance, replacement, or rearrangement purposes or for the implementation of a Customer order.

vii. Customer's election to not release a Service Component for testing and/or repair and to continue using the Service Component.

viii. Force Majeure conditions including but not limited to acts of God, labor strikes and other labor disturbances, power surges or failures, Internet connectivity, or the act or omission of any third party, or other causes beyond Data Defenders' control, whether or not similar to the foregoing.

ix. Service interruptions, deficiencies, degradations, or delays during any period when a Service Component is removed from Service for maintenance, replacement, or rearrangement purposes by Customer staff.

x. Service interruptions, deficiencies, degradations, or delays in Service caused by any piece of equipment, configuration, routing event, or technology not under the management and control of Data Defenders.

xi. Failure to adhere to Data Defenders recommended configurations on unmanaged equipment.

In addition, Service SLAs do not apply:

xii. If Customer is entitled to other available credits, compensation, or remedies under Customer's MSSTC for the same Service interruption, deficiency, degradation, or delay.

xiii. For Service interruptions, deficiencies, degradations, or delays not reported by Customer to Data Defenders.

xiv. Where Customer reports an SLA failure, but Data Defenders does not find any SLA failure.

xv. When Service is dependent upon other Service with lower SLA.

xvi. If Customer has over thirty (30) day past due balance on any billing or service with Data Defenders.

xvii. After date of Service contract termination.

If Customer elects to use another provider or method to restore Service during the period of interruption, Customer must pay the charges for the alternative Service used.

b. **Service SLA Exclusions.** SLAs do not apply and Data Defenders is not responsible for failure to meet an SLA resulting from:

i. Failure to provide suitable secure environment for on premise devices including but not limited to secure mounting/racking, appropriate cooling and air handling, secure from theft, and loose wires bundled neatly.

d. **Data Shield Sentinel SEIM Log Monitoring.** Log management via Data Shield Sentinel SIEM includes (SEIM)**:**

- Ensuring the comprehensiveness of logs added continuously to the SIEM.
- Ensuring the uninterrupted addition of logs to the SIEM including endpoint agent services.

Customer must initially specify the logs to be included in the SIEM log collection, and Data Defenders must assess the initial specification and point out shortcomings to ensure comprehensiveness. Comprehensiveness must proactively be maintained in change management situations (i.e., ensuring that newly-added systems have their logfiles added to the SIEM as well).

a. **SLA Metrics for Reporting**. The average number of days for when new log sources become operational is defined in business days. The average number of days from the date when Data Defenders has been informed of a new log source being active for collection to the date when logfiles are continuously added to the SIEM is five (5) days. Recently added systems will have higher risks especially if they are internet-facing. The number must be listed per month and reported monthly via email. Data Defenders must ensure the uninterrupted addition of logs to the SEIM, which includes ensuring that end point log forwarding agents are running and that the SEIM receivers are listening and functional.

SLA Metrics for reporting additionally include:

I. The total number of minutes that unique systems were not transmitting logfiles. Approved service windows are not included.

II. The average number of minutes without service for all devices.

III. The total number of minutes the SEIM was not actively receiving log files.

The numbers must be listed per month and reported monthly via email. The average time that logfile collection is inactive must be less than one (1) hour per asset per month. Approved service windows not included.

e. **Security Device Configuration and Management.** Customer submit a complete list of Security Devices to be managed by Data Defenders within thirty (30) days of the Effective Date and in accordance with the Scope of Services defined in this Order Form. All security devices must be correctly configured and managed. This includes:

- Daily verification that devices or applications that need signature updates receive these (i.e., IDS devices receive new signatures).
- Monitoring for new firmware or software version availability.
- Changing default passwords and community strings.
- Documenting passwords in password managers.
- Documenting asset configurations in the CMDB with the agreed-upon level of configuration item detail.
- Ensuring separation of duties between production systems and backup systems holding backup data.

All security devices must pass an initial configuration audit after being configured by Data Defenders. This audit will be performed by the Customer (or a third party employed for this purpose by Customer) and the audit must be performed within one month of the device going active.

I. **SLA Metrics for Reporting.**

1. Number of initial configuration audits performed monthly, indicating audits that passed successfully and those that failed. The number of failed audits must be less than one (1) out of six (6), seen over a period of six (6) months rolling.
2. Number of days per device that signature updates were not received. The number must be less than one (1) day out of ten (10) per device.
3. Number of assets for which new firmware or software versions, including availability date, exist but no change request has been raised by Data Defenders for this update to be performed. The number must be less than one (1) out of ten (10) and lack of awareness of the availability of a firmware or software update must be retroactively corrected the following month, if this happens.

The numbers must be listed per month and reported monthly via email. Rolling numbers must also be reported monthly via email.

f. **DDoS Mitigation.** For on-demand DDoS mitigation:

a. **SLA Metrics for Reporting.** The number of minutes from the detection of an attack until mitigation was active, per attack. For on-demand DDoS attacks that required extra mitigation to nullify: The number of minutes from when initial mitigations were active until extra mitigations became active, per attack.

For always-on DDoS mitigation (for attacks too large to handle):

- The number of minutes until extra mitigations became active, per attack.

The numbers must be listed per month and reported monthly via email listing attack dates, times on/off, and targets.

g. **Security Assessment: Vulnerability Scanning and Assessment.** Vulnerability scanning must be performed monthly and results must be manually assessed by competent resources. The results must be communicated to the Customer monthly with impact assessments and remediation advice.

I. SLA Metrics for Reporting.

1. Vulnerability scan dates and accompanying report dates. Reports must go out less than two (2) days after a scan has been completed.
2. Scans must take place with the agreed intervals (five (5) out of six (6) times) over six (6) month rolling reporting periods.
3. Reports must be completed and delivered to Customer within the agreed amount of days, five (5) out of (6) six times on average over six (6) month rolling reporting periods.
4. For critical or high severity vulnerabilities, manual incident handling must be performed. Reporting must include the number of high or critical vulnerabilities identified, dates identified, and manual incident handling initiation dates. High or critical impact vulnerabilities identified must always be reported manually within eight (8) hours.

h. **Change Management.** Change management means handling changes in coordination between the Customer and Data Defenders. Data Defenders must initiate change requests when new firmware or software updates are available or when incident management situations require such.

Change management processes must follow the official change management policy of the Customer and Data Defenders and will be measured on adherence to the policy.

I. SLA Metrics for Reporting

1. The number of days for Data Defenders to confirm receipt of a change request or change notification. The number of days should be less than one (1) day for priority 1 changes, less than three (3) days for priority 2 changes, and less than five (5) days for priority 3 changes.
2. Data Defenders must work interactively with Customer on change management, which means that deliverables from Data Defenders regarding a change must always be delivered within one (1) day for priority 1 changes, less than three (3) days for priority 2 changes, and less than five (5) days for priority 3 changes (given no errors or delays from Customer).

The numbers must be listed as changes per month and must include initiating party, receipt confirmation date, deliverables delivered date, and change priority and must be reported monthly via email. The numbers should be maintained as rolling numbers for six months rolling.

i. **Incident Management.** Incident management includes:

- Creating, updating, and closing incidents.
- Escalating incidents manually, when required.

- Automatic escalation for incidents that are not solved within the defined resolution time frames.
- Following up on alerts to determine whether or not an alert is a false positive and updating incident management databases with this information.
- For alerts that are not false positives, incident management requires a follow-up to verify if an affected system was vulnerable to a potential payload delivered, plus remediation (in coordination with Customer), if a system was infected.
- Major incidents need to be actively managed through their entire life-cycle.

a. SLA Metrics for Reporting

1. Number of incidents created, their creation date, and their closing date.
2. Number of incidents automatically escalated, their escalation from/to, and escalation time/date. Incidents must automatically escalate from priority 5 to priority 4 after three (3) days, from priority 4 to priority 3 after two (2) days, from priority 3 to priority 2 after one (1) day, from priority 2 to priority 1 after three (3) hours; unclosed priority 1 incidents not closed three (3) hours after Customer reporting these or Data Defenders creating these must be escalated to major incident handling.
3. Number of major incidents, their reporting/creation time, their closing time/day and whether or not a major incident was escalated automatically, and, if yes, from which initial priority.
4. Average Customer satisfaction with major incident handling. Following the closing of a major incident, Customer will always perform a satisfaction survey internally, and the satisfaction percent must always stay above 80% over six (6) months rolling.
5. Number and percentage of incidents manually escalated and reasons for this.
6. Number and percentage of alerts followed up, number and percentage of alerts determined as false positives, number and percentage of alerts without potential impact, and number and percentage of alerts with potential impact plus actions taken.
7. For any alert that could mean a potential breach, this will be handled like a major incident and reporting should be done according to the major incident handling process described above.

The numbers must be listed per month and reported monthly via email. Rolling numbers must also be reported monthly via email.

j. **Forensics and Incident Response Including Malware Reversing and Analysis.** For major incidents, the Data Shield SOC will handle forensics and incident response. This can also mean reversing and analyzing malware. Incident handling will include:

- Data Defenders will provide incident response and/or forensics response personnel when alerted by Customer personnel.
- Data Defenders will provide three-hour SLA for phone support.
- Data Defenders will provide 24-hour SLA for onsite support.

- Data Defenders will provide 8-hour SLA remote incident response support.
- Data Defenders' incident response team will respond when an incident is identified through a range of tools including the eSentire MDR and Customer's Intrusion Detection System (IDS/IPS) and as official declared by Customer Authorized Contact.
- Data Defenders will provide assistance to Customer on in-bound and out-bound communications, including breach notifications, public relations, and crisis communications.

8. **CHANGE OF SCOPE OF SERVICES.** Customer may at any time during the Term of this MSSTC and Order Form, request changes to the Scope of Services of this Order Form. Data Defenders will generate a Change Order Form which will be appended to this Order Form and MSSTC detailing which current in-scope services will be changed or new services to be added to the current Scope of Services for this Order Form. The Change Order Form will also provide detail for the change in pricing and the impact on the service delivery timeline. The Change Order Form must be approved by the Customer Authorized Contact and the Data Defenders Engagement Manager to be accepted as a valid change request by the Customer.

DATA DEFENDERS
Defenders of the Information World™

DATA SHIELD® MANAGED SECURITY SERVICE (MUNICIPAL) – ORDER FORM PRICING

City of Aurora, IL
Information Services Division
44 E. Downer Place
Aurora, IL 60507

Primary Contact: Leela Karumuri, LKarumuri@aurora-il.org, (630) 256-3489
Michael Pegues, Mpegues@aurora-il.org , (630) 236-3471

CUSTOMER MSSTC No.:	20190213-01-DS	**Payment Terms:**	Net 15 Days	**Data Shield Change Order No.:**	20190213-01-002 DS-01	**Notes:**	
SCOPE OF SERVICES				**Data Shield Order Form No.:**	DS-003		

SERVICE #1	**Overwatch:** N/A				**Price Level:**	Fixed Price		
DATA SHIELD MANAGED SECURITY SERVICES	**DESCRIPTION**	**QTY.**	**RETENTION PERIOD**	**CATEGORY**	**Unit Cost:**	**Sub-Total Annual Cost:**	**Billing**	**Total 5-Year Cost:**
SERVICE ADDITION (OPERATIONAL TECHNOLOGY)	200 Series appliance: 18TB capacity 4 - 1G ethernet ports, 2 - 10G SFP ports, 1 - 10G ethernet port Appliance type	1	N/A	**LICENSE**	$ 59,325.00	$ 59,325.00	Annual	$ 296,625.00
eSentire esNETWORK Managed Detection and Response Service	Users	1200						
							Sub-Total esNetwork MDR Service:	**$ 296,625.00**

SERVICE #2	**Overwatch:** No				**Price Level:**	Fixed Price		
DATA SHIELD MANAGED SECURITY SERVICES	**DESCRIPTION**	**QTY.**	**RETENTION PERIOD**	**CATEGORY**	**Unit Cost:**	**Sub-Total Annual Cost:**	**Billing**	**Total 5-Year Cost:**
SERVICE ADDITION (OPERATIONAL TECHNOLOGY)	Endpoints	300	15 Days	**LICENSE**	$ 70.37	$ 21,111.00	Annual	$ 105,555.00
esENDPOINT Detection and Response Powered by CrowdStrike Services							**Sub-Total esENDPOINT MDR Service:**	**$ 105,555.00**

SERVICE #3					**Price Level:**			Fixed Price		
SEIM/SECURITY DEVICE MANAGEMENT	**DESCRIPTION**	**QTY.**	**RETENTION PERIOD**	**CATEGORY**	**Unit Cost:**	**DISC**	**Rate**	**Sub-Total Cost:**	**Billing**	**Total 5-Year Cost:**
SERVICE ADDITION (OPERATIONAL TECHNOLOGY)	Sentinel SEIM Management (Includes Security Device Management of up to three devices)	4 GB/Day	6 Months	**LICENSE**	$ 2,100.00/GB	0%	$ 2,100.00/GB	$ 8,400.00	Annual	$ 42,000.00
	Security Technology Device Management	42 HRS	N/A	**SUBSCRIPTION**	$ 250.00/Hr	40%	$ 150.00/Hr	$ 6,300.00	Annual	$ 31,500.00

DATA SHIELD® MANAGED SECURITY SERVICE
(MUNICIPAL) – ORDER FORM PRICING

City of Aurora, IL
Information Services Division
44 E. Downer Place
Aurora, IL 60507

Primary Contact: Leela Karumuri, LKarumuri@aurora-il.org, (630) 256-3489
Michael Pegues, Mpegues@aurora-il.org , (630) 236-3471

CUSTOMER MSSTC No.: 20190213-01-DS **Payment Terms:** Net 15 Days **Data Shield Change Order No.:** 20190213-01-002 DS-01 **Notes:**

SCOPE OF SERVICES

Data Shield Order Form No.: DS-003

									Sub-Total Sentinel SEIM Service:	**$ 73,000.00**
SERVICE #4					**Price Level:**		Fixed Price			
VULNERABILITY MANAGEMENT	**DESCRIPTION**	**QTY.**	**RETENTION PERIOD**	**CATEGORY**	**Unit Cost:**	**DISC**	**Rate**	**Sub-Total Cost:**	**Billing**	**Total 5-Year Cost:**
SERVICE ADDITION **(OPERATIONAL TECHNOLOGY)**	Vulnerability Management Subscription	75 Hrs	N/A	**SUBSCRIPTION**	$ 250.00/Hr	40%	$ 150.00/Hr	$ 11,250.00	Annual	$ 56,250.00
									Sub-Total Sentinel SEIM Service:	**$ 56,250.00**
SERVICE #5	General Professional Services Annual Hours Allocations for each Contract Year				**Price Level:**		Fixed Price			
DATA SHIELD PROFESSIONAL SERVICES	**DESCRIPTION**	**QTY.(HR)**	**RETENTION PERIOD**	**CATEGORY**	**Unit Cost:**	**DISC**	**Rate**	**Sub-Total Cost:**	**Billing**	**Total 5-Year Cost:**
SERVICE ADDITION	Annual General Hours Allocation	100	N/A	**PRO. SERV.**	$ 250.00/Hr	40%	$ 150.00/Hr	$ 15,000.00	As Incurred	$ 75,000.00
SERVICE ADDITION ***(OPERATIONAL TECHNOLOGY)***	Risk Assessment	50	N/A	**PRO. SERV.**	$ 250.00/Hr	40%	$ 150.00/Hr	$ 7,500.00	As Incurred	$ 37,500.00
SERVICE ADDITION ***(OPERATIONAL TECHNOLOGY)***	Internal/External Penetration Testing	50	N/A	**PRO. SERV.**	$ 250.00/Hr	40%	$ 150.00/Hr	$ 7,500.00	As Incurred	$ 37,500.00
SERVICE ADDITION	vCISO	250	N/A	**PRO. SERV.**	$ 250.00/Hr	40%	$ 150.00/Hr	$ 37,500.00	As Incurred	$ 187,500.00
SERVICE ADDITION	Threat Intelligence Analysis (Incident Response)	300	N/A	**PRO. SERV.**	$ 250.00/Hr	40%	$ 150.00/Hr	$ 45,000.00	As Incurred	$ 225,000.00
									Sub-Total Data Shield Pro. Services:	**$ 562,500.00**
SERVICE #6					**Price Level:**		Fixed Price			
DATA SHIELD POINT SOLUTIONS **Okta Identify Management**	**DESCRIPTION**	**QTY.(HR)**	**RETENTION PERIOD**	**CATEGORY**	**Unit Cost:**	**DISC**	**Rate**	**Sub-Total Annual Cost:**	**Billing Category**	**Total 5-Year Cost:**

DATA SHIELD® MANAGED SECURITY SERVICE (MUNICIPAL) – ORDER FORM PRICING

City of Aurora, IL
Information Services Division
44 E. Downer Place
Aurora, IL 60507

Primary Contact: Leela Karumuri, LKarumuri@aurora-il.org, (630) 256-3489
Michael Pegues, Mpegues@aurora-il.org , (630) 236-3471

CUSTOMER MSSTC No.: 20190213-01-DS **Payment Terms:** Net 15 Days **Data Shield Change Order No.:** 20190213-01-002 DS-01 **Notes:**

SCOPE OF SERVICES

Data Shield Order Form No.: DS-003

SERVICE ADDITION	Single Sign-On, Multi-Factor Authentication, Lifecycle Management, Universal Directory, API Access Management	1200 Users	N/A	**LICENSE**	$ 62,477.00	0%	$ 62,477.00	$ 62,477.00	Annual	$ 312,385.00
SERVICE ADDITION	Training – Okta Essentials	1	N/A	**TRAINING**	$ 3,149.00	0%	$ 3,149.00	$ 3,149.00	On-Time	
SERVICE ADDITION	Okta Support – Premier Success Package	1	N/A	**SUPPORT**	$ 9,375.00	0%	$ 9,375.00	$ 9,375.00	Annual	$ 46,875.00
SERVICE ADDITION	Design & Integration Services	200 Hrs.	N/A	**PRO. SERV.**	$ 250.00/Hr	40%	$ 150.00/Hr	$ 30,000.00	On-Time	
SERVICE ADDITION	Platform Management	50 Hrs.	N/A	**PRO. SERV.**	$ 250.00/Hr	40%	$ 150.00/Hr	$ 7,500.00	Annual	$ 37,500.00
					NEW SUB-TOTAL DATA SHIELD POINT SOLUTION SERVICE (ON-TIME COSTS):			**$ 33,149.00**		
					NEW SUB-TOTAL DATA SHIELD POINT SOLUTION SERVICE (ANNUAL COSTS):			**$ 79,352.00**		**$ 396,760.00**

OTHER NOTES

TOTAL DATA SHIELD MSS COST (ONE-TIME):	**$ 33,149.00**
TOTAL DATA SHIELD MSS COST ANNUALLY:	$ 298,238.00
TOTAL DATA SHIELD MSS 5-YEAR COST:	**$ 1,491,190.00**

IN WITNESS WHEREOF, each of the Parties hereto have caused this Order Form to be executed and delivered by its duly authorized representative as of the date set forth below.

ACCEPTANCE / AUTHORIZATION

	DATA DEFENDERS, LLC.		**CITY OF AURORA, IL**
By:		**By:**	
Print Name:		**Print Name:**	
Title:		**Title:**	
Date:		**Date:**	
	Authorized Signatory		Authorized Signatory