



City Council Meeting Agenda
Monday, November 20, 2023 – 6:30 p.m.
City Hall, 200 South Osage, Sedalia MO

MAYOR: ANDREW L. DAWSON

MAYOR PRO-TEM: RHIANNON M. FOSTER

- A. CALL TO ORDER** – Andrew L. Dawson – Council Chambers
- B. PRAYER & PLEDGE OF ALLEGIANCE**
- C. ROLL CALL**
- D. PUBLIC HEARING** – Annexation Petition – Highway H Property, LLC
- E. PROCLAMATION** – 50 Year Anniversary of the Municipal Building
- F. SPECIAL AWARDS**
 - A. Life Save Awards** – Fire Department
 1. Greg Smith – Captain
 2. Kyle Rupe – Engineer
 3. Tim Borden – Firefighter
 4. Tony Turner - Firefighter
 - B. CIT Awards** – Police Department
- G. SERVICE AWARDS/RETIREMENT AWARDS** – None
- I. APPROVAL OF PREVIOUS SESSION MINUTES**
 - A.** Council Meeting – November 6, 2023
- II. REPORT OF SPECIAL BOARDS, COMMISSIONS AND COMMITTEES**
 - A.** Acceptance of Citizen’s Traffic Advisory Commission minutes dated October 11, 2023
 - B.** Acceptance of Planning & Zoning Commission minutes dated October 4, 2023
- III. ROLL CALL OF STANDING COMMITTEES**
 - A. FINANCE / ADMINISTRATION** – Chairman Chris Marshall; Vice Chairman Jack Robinson
 - 1. Presentation** – Oats: Annual Report (Tracy Walkup, Presenter)
 - 2. Presentation** – Financial Update (Jessica Pyle, Presenter)
 - 3. Budget Amendment and Quote** – Managed Detection & Remediation Purchase - \$9,110.35
Council Discussion led by Chairman Marshall
 - R** Call for Resolution of the City Council of the City of Sedalia, Missouri, stating facts and Reasons for the necessity to amend and increase the City’s Annual Budget for Fiscal Year 2024 – Mayor Dawson
 - O** Call for Ordinance Amending the Budget for the Fiscal Year 2023-2024 and Approving and Accepting a quote for the purchase of Detection and Remediation Services – Mayor Dawson
 - 4. Budget Amendment** – Harding Street Ground Testing - \$35,425.00
Council Discussion led by Chairman Marshall

[Click on any agenda item to view the related documentation](#)

R Call for Resolution of the City Council of the City of Sedalia, Missouri, stating facts and Reasons for the necessity to amend and increase the City's Annual Budget for Fiscal Year 2024 – Mayor Dawson

O Call for Ordinance Amending the Budget for the Fiscal Year 2023-2024 regarding Harding Street Ground Testing – Mayor Dawson

B. PUBLIC SAFETY - Chairman Jack Robinson; Vice Chairman Steve Bloess

1. Strategic Planning Presentation – Animal Services (Randi Battson, Presenter)

C. PUBLIC WORKS – Chairman Thomas Oldham; Vice Chairman Chris Marshall

1. Strategic Planning Presentation – Airport Department (Derrick Dodson, Presenter)

2. RC Mower Purchase – Street Division - \$67,762.50

Council Discussion led by Chairman Oldham

O Call for Ordinance Approving and Accepting a quote for the purchase of an RC Mower to be utilized by the Street Department – Mayor Dawson

3. Budget Amendment – Truck Purchase – Public Works Water Division - \$67,000.00

Council Discussion led by Chairman Oldham

R Call for Resolution of the City Council of the City of Sedalia, Missouri, stating facts and Reasons for the necessity to amend and increase the City's Annual Budget for Fiscal Year 2024 – Mayor Dawson

O Call for Ordinance Amending the Budget for the Fiscal Year 2023-2024 regarding Water Department Truck Purchases – Mayor Dawson

D. COMMUNITY DEVELOPMENT – Chairwoman Rhiannon M. Foster; Vice Chairwoman Tina Boggess

1. Strategic Planning Presentation – Community Development (John Simmons & Devin Lake, Presenters)

2. Granting Special Use Permit – Twilight Motors, LLC – 204 E. 24th – C-1 Local Business to C-3 Commercial

Council Discussion led by Chairwoman Foster

O Call for Ordinance granting a special use permit to Nicholas A. Dilthey for a Car Dealership Business on property located at 204 East 24th Street in the City of Sedalia, Missouri – Mayor Dawson

3. Master Services agreement – Aerial Photography – Pictometry Corp. dba Eagleview - \$305,199.00

Council Discussion led by Chairwoman Foster

O Call for Ordinance Authorizing a Master Services agreement for Aerial Photography service - Mayor Dawson

IV. OTHER BUSINESS

A. APPOINTMENTS – None

B. LIQUOR LICENSES - None

V. MISCELLANEOUS ITEMS FROM MAYOR, CITY COUNCIL AND CITY ADMINISTRATOR

VI. GOOD AND WELFARE

VII. Closed Door Meeting – Motion and Second to move into closed door meeting in the upstairs conference room

pursuant to Subsections 1 (Legal Advice), 2 (Real Estate), and 12 (Negotiated Contracts) of Section 610.021 RSMo.

- A. Roll Call Vote for Closed Door Meeting
- B. Discussion of closed items
- C. Vote on matters, if necessary (require a Roll Call Vote)
- D. Motion and Second with Roll Call Vote to adjourn closed door meeting and return to open meeting

VIII. ADJOURN MEETING

- A. Motion and second to adjourn meeting

Please join the meeting by clicking or touching this link from your smartphone, computer, tablet, or iPad:
<https://global.gotomeeting.com/join/578973061>

If this is the **first time** you have joined a GoToMeeting you will be asked to identify yourself. Please fill in this information. If you would like, and we suggest you do, go ahead and set your preferences to make it easier to join next time. If you are new to GoToMeeting? We suggest to get the app through the following link:

<https://global.gotomeeting.com/install/578973061> This will make joining these meetings quick and easy.

Once you have followed the link above and identified yourself you will be given options for how you want to join in with **audio**.

For **smartphones**: tap on one of the phone numbers and it will dial the phone and the meeting numbers.

For **other devices**: use the feature of call me. The phone audio will be much better than through your computer. This should come up if you have your preferences set up to show it. If it does not, in the upper right-hand corner of the GoToMeeting screen you will see an icon that looks like a gear. Click on the gear and then look for "Phone" and if it is not highlighted click on it. One of the options should be to call me. Put the phone number you want to be called on (direct dial) into the box provided and then click the "Call Me" button. Once the system calls you, you will be asked to hit pound.

Please be mindful of others on the call by eliminating as much background noise as you can. Mute yourself until you are ready to speak. Do not put the call on hold, if you need to leave even for a short time, hang up as you can always dial back in after your other call. If you hear an echo or squeal, you may have your computer speakers on as well as the phone, mute your computer speakers to eliminate this.

If you want to join in **listen only** mode you can dial the following number and enter the access code.

(For supported devices, tap a one-touch number below to join instantly.)

United States (Toll Free): 1 866 899 4679

- One-touch: <tel:+18668994679,,578973061#>

United States: +1 (669) 224-3318

- One-touch: <tel:+16692243318,,578973061#>

Access Code: 578-973-061

The City Council reserves the right to discuss any other topics that are broached during the course of this meeting.

IF YOU HAVE SPECIAL NEEDS, WHICH REQUIRE ACCOMMODATION, PLEASE NOTIFY THE CITY CLERK'S OFFICE AT 827-3000. ACCOMMODATIONS WILL BE MADE FOR YOUR NEEDS

POSTED ON NOVEMBER 17, 2023, AT 3:30 P.M. AT THE SEDALIA MUNICIPAL BUILDING, BOONSLICK REGIONAL LIBRARY, SEDALIA PUBLIC LIBRARY AND ON THE CITY'S WEBSITE AT WWW.SEDALIA.COM



OFFICE OF THE CITY ADMINISTRATOR

To: Honorable Mayor Andrew L. Dawson & City Council Members
From: Kelvin Shaw, City Administrator *KS*
Re: Agenda items for City Council meeting on Monday, November 20, 2023, 6:30 p.m.

Public Hearing For Highway H Property, LLC Annexation Petition – A petition was received for annexation of property owned by Highway H Property, LLC along HH at the North edge of town. In accordance with State Statutes, we must hold a public hearing between 14 and 60 days of receiving such a petition. The hearing is to hear from any interested parties on the appropriateness of the annexation. We must then wait at least 14 days after the hearing to consider adoption of an ordinance to conclude the annexation.

Proclamation For 50 Year Anniversary Of The Municipal Building – In celebration of the 50th anniversary of the municipal building a proclamation will be read. Pictures of the facilities over the years will be available to commemorate the passage of time and historical significance of the facility.

Finance/Administration Committee – There are four items for consideration through the Finance / Administration Committee.

1. As part of our strategic planning process, we ask that our outside service contractors make a presentation. The contract requires such presentation and essentially, we ask that they report on how the funds were used this fiscal year, and then what services and costs they propose for the next fiscal year. This is an important function for these contracts from a legal standpoint, as we must show the general public purpose for the expenditure of these funds. In addition, from an overall resource allocation standpoint, we must review these services to determine how they stack up against all other priorities. For this meeting OATS will make such a report of the service contract with them. They provide transit services to the community, and as per the current contract, we help offset the costs with \$25,000.00 so that affordable transportation services are provided to more individuals.
2. Jessica Pyle, Finance Director, will provide an update on major trends in tax revenue collections.
3. As presented at a previous Council meeting, Monte Richardson, IT Manager, provided an update on a grant he was successful in securing to make our networks more secure. Council has accepted the grant and he has worked with the vendor to update the quote. Staff recommends approval of the budget amendment and the purchase at this time.
4. Staff has been working on a way to facilitate redevelopment of the properties that were once used for the railroad shops at 600 and 125 North Harding. A concern expressed by potential buyers for redevelopment, that is consistently raised, is the status of environmental issues that may need to be remediated in connection with any redevelopment. Therefore, we contracted with an engineering firm to conduct a Phase II Environmental Study to be able to provide this information to prospective developers. Council has previ-

ously given approval for this project and staff recommends formal approval of a budget amendment to appropriate the funds in the amount of \$35,425.

Public Safety Committee – There is one item for consideration through the Public Safety Committee.

1. Randi Battson, our Animal Services Manager, will continue this year's presentations of strategic planning for each department. Manager Battson will present at this meeting an overview of the plans for Animal Control Services.

As a reminder, I ask that in each of the individual presentations that they address the following four questions:

- a) Why is the service needed?
- b) Why should the City be doing it?
- c) What level of service are we providing now?
- d) How are we going to accomplish it? In other words, strategies going forward for services including any major budget requests related to new or expanded initiatives.

These presentations will all lead up to and set the stage for the Council strategic planning session on January 6th (the first Saturday in January). During this session, we review the highlights of each of these individual department strategic plans to bring them together into an overall plan for the City, to include setting relative priorities. This high-level direction from Council then becomes the basis for the budget development to match that strategy. We will then have budget work sessions February through March, culminating with a budget adoption the last meeting in March.

Public Works Committee – There are three items for consideration through the Public Works Committee.

1. Derrick Dodson, our Airport Director, will continue this year's presentations of strategic planning for each department. Director Dodson will present at this meeting an overview of the plans for the Airport.
2. We have several areas where we need to maintain the vegetation that are difficult, at best, for ride on mowing equipment. For example, we have the Springfork Lake Dam, the Rail Spur, Equalization Basins, and Drainage Ditches that all have to be mowed periodically, yet are very steep embankments. Staff has identified specialized equipment that is designed specifically with these types of jobs in mind. They are remote controlled mowers with a low center of gravity, wide base, and track propulsion, giving them the ability to go on these steep grades while the employee stays safely on the less formidable terrain around it. While this was not included in the adopted budget, there have been a couple purchases where we have been able to come in under budget in sufficient amounts to more than cover the cost of adding this equipment. Staff recommends approval of the use of underbudget condition of other equipment and the purchase of a remote-control mower at the cost of \$67,762.50.
3. As discussed in previous meetings, adding staff to the Public Works Department for duties such as utility locates will provide a more timely and better controlled product, while also generating a significant savings over the current contracting. Therefore, this position was approved by Council and has been hired. To make them efficient in these duties we need to

add a vehicle to the fleet for them to use to accomplish these tasks. Staff has again located used pickups from the highway patrol that would be suitable for this use. There are two vehicles available that are heavier duty than needed for this use, along with the lead and copper compliance project. However, these heavy-duty vehicles are better suited to the use by the managers as service vehicles. This would then free up the light duty trucks currently being used for the new personnel. Staff recommends a budget amendment to add two vehicles to the fleet in the water department for \$67,000.

Community Development Committee – There are three items for consideration through the Community Development Committee.

1. John Simmons, our Community Development Director, and Devin Lake, our Chief Building Official (CBO), will continue this year's presentations of strategic planning for each department. Director Simmons will present at this meeting an overview of the plans for Community Development and CBO Lake will present an overview of the plans for the Building and Code Enforcement functions.
2. The owner of the property at 204 East 24th Street submitted an application for a special use permit. The property is currently zoned as C-1 Local Business. Over the years, the business being conducted at this location has progressed to its current use of selling used automobiles and carport structures. C-1 Local Business zoning allowed the previous business use but does not allow for the current usage. The owner originally requested rezoning; however, staff recommended that a special use permit would be more appropriate in this case. The special use permit will allow them to continue their use as is, without opening up the neighborhood to potential later uses that would be more detrimental to the fabric of the surrounding residential area. The Planning and Zoning Commission reviewed the application and they, as well as staff, recommend approval.
3. In September, Council accepted a quote for providing aerial photography and pictometry for our Geographical Information System (GIS). There was some confusion in the quoted amount though. Staff had interpreted the quoted total of \$225,900 to include all three flyovers during the six-year period. However, upon closer review and discussions with the vendor, the amount we interpreted for all three was in fact stated as per project and the vendor's intent was that a project was each flyover. With this clarification, we do not believe the increase in resolution for the County areas is justifiable. The resolution was for 1" inside the city limits and 3" for the rest of the county. Therefore, we proposed to the County and the vendor to use the lower resolution of 6" and they agreed. Staff has worked with them to negotiate a master services agreement and recommends approval. The total is now \$305,199 over the next six years.

NOTICE OF PUBLIC HEARING

~ Annexation Petition ~

The City of Sedalia will hold a public hearing at 6:30 p.m. on Monday, November 20, 2023, in the Council Chambers at the Municipal Building, 200 South Osage Avenue, to consider an annexation petition filed with the City on October 27, 2023.

Public comments concerning the requested annexation will be entertained at the hearing.

Legal Description for the property owned by Highway H Property LLC states the following:

All of the following described tract of land in Pettis County, Missouri, which is contiguous and compact to the existing city limits of the City of Sedalia, Missouri, to-wit:

30.86 ACRES

ALL THAT PART OF THE SOUTHWEST QUARTER OF THE SOUTHWEST QUARTER OF SECTION 22, TOWNSHIP 46 NORTH, RANGE 21 WEST OF THE FIFTH PRINCIPAL MERIDIAN, PETTIS COUNTY, MISSOURI, LYING EAST OF THE NEW EAST RIGHT-OF-WAY LINE OF U.S. HIGHWAY 65 AND NORTH OF THE NORTH RIGHT-OF-WAY LINE OF MISSOURI STATE ROUTE "HH", MORE PARTICULARLY DESCRIBED BY METES AND BOUNDS AS FOLLOWS:

COMMENCING AT THE SOUTHWEST CORNER OF SAID SOUTHWEST QUARTER OF THE SOUTHWEST QUARTER; THENCE NORTH 02°00'22" EAST, ALONG THE WEST LINE OF SAID SOUTHWEST QUARTER OF THE SOUTHWEST QUARTER, 417.52 FEET; THENCE SOUTH 87°00'34" EAST, 25.0 FEET; THENCE SOUTH 86°44'35" EAST, 64.93 FEET TO A POINT ON THE NEW EAST RIGHT-OF-WAY LINE OF SAID U.S. HIGHWAY 65 AT CENTERLINE STATION 733+62.26 AND THE POINT OF BEGINNING; THENCE NORTH 02°03'59" EAST, ALONG SAID EAST RIGHT-OF-WAY LINE, 908.62 FEET TO A POINT ON THE NORTH LINE OF SAID SOUTHWEST QUARTER OF THE SOUTHWEST QUARTER AT CENTERLINE STATION 724+53.64; THENCE SOUTH 87°03'03" EAST, ALONG SAID NORTH LINE, 1211.21 FEET TO THE NORTHEAST CORNER OF SAID SOUTHWEST QUARTER OF THE SOUTHWEST QUARTER; THENCE SOUTH 02°01'13" WEST, ALONG THE EAST LINE OF SAID SOUTHWEST QUARTER OF THE SOUTHWEST QUARTER, 1268.87 FEET TO A POINT ON THE NORTH RIGHT-OF-WAY LINE OF SAID MISSOURI STATE ROUTE "HH"; THENCE NORTH 87°16'59" WEST, ALONG SAID NORTH RIGHT-OF-WAY LINE, 671.64 FEET; THENCE NORTH 02°00'22" EAST, 360.06 FEET; THENCE NORTH 86°44'35" WEST, 540.22 FEET TO THE POINT OF BEGINNING.

Handicapped citizens needing accommodation in order to attend this public hearing should contact the City Administrator's Office at (660) 827-3000 extension 1102 no later than 48 hours prior to the scheduled hearing.

Kelvin Shaw, City Administrator
City of Sedalia

Run 1x
11-10-2023



CITY OF SEDALIA, MISSOURI
CITY COUNCIL MEETING
NOVEMBER 6, 2023

The City has an on-line broadcast of Council Meetings available both live and recorded by going to https://global.gotomeeting.com/join/578973061

The Council of the City of Sedalia, Missouri duly met on Monday, November 6, 2023 at 6:30 p.m. at the Municipal Building in the Council Chambers with Mayor Pro-Tem Rhiannon M. Foster presiding.

ROLL CALL:

Table with 4 columns: Name, Status, Name, Status. Rows include Jack Robinson, Thomas Oldham, Chris Marshall, Tina Boggess, Bob Hiller, Bob Cross, Rhiannon Foster, Steve Bloess.

SERVICE AWARDS:

Table with 4 columns: Award, Recipient, Department, Service. Rows include 30 Year Gift Card/Certificate for Donald Sattler, Kenneth Schlesselman, David Murray and 5 Year Pin/Certificate for Bryan Allen.

SPECIAL AWARDS:

Fire Department Badge Pinning: Fire Chief Matt Irwin presented Andrew Allen with his Firefighter Badge. Mr. Allen graduated from the Holt Summit Fire Academy and has met all the requirements to wear the badge of the Sedalia Fire Department.

RETIREMENT AWARDS: None

MINUTES: The Council Meeting minutes of October 16, 2023 were approved on motion by Oldham, seconded by Marshall. All in Favor.

REPORTS OF SPECIAL BOARDS, COMMISSIONS & COMMITTEES: None

ROLL CALL OF STANDING COMMITTEES:

PUBLIC SAFETY – Jack Robinson, Chairman; Steve Bloess, Vice Chairman

Presentation: Pettis County Joint Communications Budget

Pettis County Joint Communications Director Dannelle Lauder gave an update on Joint Communications from October 2022 thru September 2023. Joint Communications is fully staffed, however, all staff is not fully trained. They have two new recruits going through the training process.

2,000 calls per week on average (Administrative and 911) and are estimated to exceed it by close of 2023. When you include out-going calls, Joint Communications averages 101,000 calls annually. The National expectancy for answering calls is 5 seconds or less. Ms. Lauder stated that in 2022, Joint Communications averaged 4.1 seconds and for 2023, they are answering within 3.9 seconds. For Administrative calls they were at 5.2 seconds in 2022 and 4.7 seconds for 2023.

For 2024, NCMC certification (Missing Children readiness program) is a top area of focus. Currently, no rural agencies in the State of Missouri hold this certification. Joint Communications' application has been submitted for the first initial review and they are awaiting any advisements or recommendations to pursue full application. Director Lauder anticipates receiving this by December 1, 2023, so she can submit the full application as quickly as possible. Other goals are the APCO Training Program Certification, NG911 Grant Funding available through the Missouri 911 Service Board, work toward 100% De-escalate Crisis Intervention Training and a D-Negotiator on Each Shift to help support law enforcement efforts. In addition, they will be expanding their Peer Support and Quality Assurance programs.

Director Lauder expanded on NG 911 (Next Generation 911). Due to the age of the current system, the parts to repair the system are no longer available. The system limits and restricts what can and cannot be done. With Next Gen ESI Net, you have a more efficient disaster recovery mode which would only require an internet connection. In addition to ESI Net, Joint Communications would qualify for NG Call Handling which is a hosted solution that allows calls to be taken from any center should the need arise to evacuate the current facility. The system would reduce contractual obligation by \$37,000.

Director Lauder presented the following baseline budget and a budget with Next Gen 911 Grant funding:

Expenditures 2024		Revenues 2024	
Full Time Salaries*	\$808,663.13	Any Device Fee	\$415,000.00
Shift Differential	\$8,299.20	State Wide Prepaid Tax	\$25,000.00
Salary Expense Total	\$816,962.33	Pettis County	\$216,163.00
Benefits	\$338,555.38	City of Sedalia	\$316,163.00
Salary & Wage Benefit	\$1,147,218.51	Pettis County Ambulance Dist.	\$166,163.00
Office Supplies	\$3,000.00	Government Total	\$1,138,489.00
New Equipment	\$3,455.78	Interest & Miscellaneous	\$7,000.00
Equipment Repair	\$5,000.00	Rollover from 2023	\$464,401.75
Travel & Training	\$19,600.00	Interest Total	\$471,401.75
Telephone	\$87,501.08	Revenues Total	\$1,609,890.75
Contractual Services*	\$308,062.75	Balance Forward	\$27,651.81
County Insurance	\$6,000.00		
Miscellaneous	\$2,400.83		
Supplies/Equip. Total	\$435,020.43		
Expenditure Total	\$1,582,238.94		

Expenditures 2024 with Grant		Revenues 2024 with Grant Consideration	
Full Time Salaries*	\$808,663.13	Any Device Fee	\$415,000.00
Shift Differential	\$8,299.20	State Wide Prepaid Tax	\$25,000.00
Salary Expense Total	\$816,962.33	Pettis County	\$216,163.00
Benefits	\$338,555.38	City of Sedalia	\$316,163.00
Salary & Wage Benefit	\$1,147,218.51	Pettis County Ambulance Dist.	\$166,163.00
Office Supplies	\$3,000.00	Government Total	\$1,138,489.00
New Equipment	\$3,455.78	Interest & Miscellaneous	\$7,000.00
Equipment Repair	\$5,000.00	Rollover from 2023	\$464,401.75
Travel & Training	\$19,600.00	Interest Total	\$471,401.75
Telephone	\$57,039.59	Grant Award	\$725,110.92
Contractual Services*	\$270,228.87	Revenues Total	\$2,335,001.67

County Insurance	\$6,000.00		Balance Forward	\$740,490.21
Miscellaneous	\$2,400.83			
Supplies/Equip. Total	\$366,725.07			
Grant Match*	\$80,567.88			
Expenditure Total	\$1,594,511.46			

*Salaries: Increased due to request for 2 additional positions. Contractual Services: Estimated increase due to reaching end of several contracts and agency must pay for non-negotiable maintenance agreements. Grant Match : Next Gen Platform and hosted system.

- The Budget Amendment in the amount of \$1,680.00 is for the purchase of bicycle lights for the Sedalia Police Department.

RESOLUTION NO. 2062 – A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF SEDALIA, MISSOURI, STATING FACTS AND REASONS FOR THE NECESSITY TO AMEND AND INCREASE THE CITY’S ANNUAL BUDGET FOR FISCAL YEAR 2024 was read once by title and approved on motion by Oldham, seconded by Robinson. All in Favor.

BILL NO. 2023-206, ORDINANCE NO. 11921 – AN ORDINANCE AMENDING THE BUDGET FOR THE FISCAL YEAR 2023-2024 REGARDING PURCHASE OF POLICE BICYCLE LIGHTS was read once by title.

2nd Reading – Motion by Oldham 2nd by Bloess. All in Favor.

Final Passage – Motion by Oldham, 2nd Marshall. All in Favor.

Roll Call Vote: Voting “Yes” were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted “No”.

- The Budget Amendment and quotes are for the purchase of radios and repeaters for the Sedalia Fire Department.

RESOLUTION NO. 2063 – A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF SEDALIA, MISSOURI, STATING FACTS AND REASONS FOR THE NECESSITY TO AMEND AND INCREASE THE CITY’S ANNUAL BUDGET FOR FISCAL YEAR 2024 was read once by title and approved on motion by Oldham, seconded by Robinson. All in Favor.

BILL NO. 2023-207, ORDINANCE NO. 11922 – AN ORDINANCE AMENDING THE BUDGET FOR THE FISCAL YEAR 2023-2024 AND APPROVING AND ACCEPTING QUOTES FOR THE PURCHASE OF RADIOS AND REPEATERS FOR THE FIRE DEPARTMENT was read once by title.

2nd Reading – Motion by Oldham, 2nd by Robinson. All in Favor.

Final Passage – Motion by Oldham, 2nd by Marshall. All in Favor.

Roll Call Vote: Voting “Yes” were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted “No”.

- The Resolution authorizes submission of a Grant application for communication equipment to be used by the Sedalia Police Department.

RESOLUTION NO. 2064 – A RESOLUTION AUTHORIZING THE SEDALIA POLICE DEPARTMENT TO ACT AS AN AGENT FOR THE CITY OF SEDALIA IN THE APPLICATION PROCESS FOR THE SFY 2024 AMERICAN RESCUE PLAN ACT STATE AND LOCAL FISCAL RECOVERY FUND FIRST RESPONDER & INTEROPERABLE COMMUNICATIONS EQUIPMENT GRANT TO BE UTILIZED BY THE SEDALIA POLICE DEPARTMENT was read once by title and approved on motion by Cross, seconded by Oldham. All in Favor.

- The Resolution authorizes submission of a Grant application for capital improvements to be used by the Sedalia Fire Department.

RESOLUTION NO. 2065 – A RESOLUTION AUTHORIZING THE SEDALIA FIRE DEPARTMENT TO ACT AS AN AGENT FOR THE CITY OF SEDALIA IN THE APPLICATION PROCESS FOR THE 2024 DEPARTMENT OF PUBLIC

SAFETY CIEG GRANT TO BE UTILIZED BY THE SEDALIA FIRE DEPARTMENT was read once by title and approved on motion by Oldham, seconded by Robinson. All in Favor.

PUBLIC WORKS – Thomas Oldham, Chairman; Chris Marshall, Vice Chairman

Strategic Planning Presentation – Street/Sanitation/Mowing/Alley Maintenance

Interim Public Works Director Chris Davies presented the Strategic Plan for Street/Sanitation/Mowing/Alley Maintenance. Mr. Davies reviewed all of the departments within Public Works and determined that the department structure could be reorganized. With this reorganization, new positions would be added: Operations Director for the Street Division, Utility Director for the two water divisions, a Civil Engineer and an Asset Management Director. Director Davies also recommended that an additional staff member should be added to assist with pretreatment and stormwater management which is currently being handled by 1 person.

Director Davies stated that the most valuable asset the City has are roads. If the City had to replace them today, it would cost approximately \$1 Billion. By maintaining roads, it lessens the cost by extending the life of the road throughout the system. The pavement management concept has core questions which assist in determining what action needs to be taken. This allows identification of the right treatment for the pavement condition and allows planning for future investment in pavement management. It is a proven method used throughout the United States and can be used for roads and sidewalks. It assists the City to evaluate the current status of roads and plan based on those road conditions. Director Davies stated that if it is something the City is interested in pursuing, you buy the software and staff the position for a year to finalize the street evaluation. The following year, the demand for the position to fulfill street evaluation would significantly lessen and the employee could be utilized to complete other tasks.

Director Davies recommended that Sanitation should move to fully self-sufficient and self-funded. Currently, general funds are being used and this goal could be achieved by going to a volume-based system. The cost for services currently provided are being supported mostly by the rate payers. The question is should the City move to volume-based so recipients pay for the services they receive. Current equipment is failing and is expensive to repair.

The City owns 289 properties, not including right-of-ways. Director Davies stated this requires a lot of mowing with very little staff. If the City wants to maintain these properties properly, we need the equipment and staff to do so.

- The agreement with Wilson & Company is for obtaining and analyzing data and preparing designs to better streets and mitigate damages as part of the Safe Streets and Roads for All Action Plan.

BILL NO. 2023-208, ORDINANCE NO. 11923 – AN ORDINANCE AUTHORIZING AN OWNER-ENGINEER AGREEMENT FOR THE SAFE STREETS AND ROADS FOR ALL (SS4A) ACTION PLAN was read once by title.

2nd Reading – Motion by Oldham, 2nd by Marshall. All in Favor.

Final Passage – Motion by Oldham, 2nd by Marshall. All in Favor.

Roll Call Vote: Voting “Yes” were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted “No”.

- The agreement with Burns & McDonnell is for aeration upgrades at the Central Wastewater Treatment Plant.

BILL NO. 2023-209, ORDINANCE NO. 11924 – AN ORDINANCE AUTHORIZING AN AGREEMENT FOR AERATION UPGRADES AT THE CENTRAL WASTEWATER TREATMENT PLANT was read once by title.

2nd Reading – Motion by Oldham 2nd by Robinson. All in Favor.

Final Passage – Motion by Oldham, 2nd by Marshall. All in Favor.

Roll Call Vote: Voting “Yes” were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted “No”.

- The budget amendment and purchase ratification is for a boiler for the Water Filtration Plant.

RESOLUTION NO. 2066 – A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF SEDALIA, MISSOURI, STATING FACTS AND REASONS FOR THE NECESSITY TO AMEND AND INCREASE THE CITY'S ANNUAL BUDGET FOR FISCAL YEAR 2024 was read once by title and approved on motion by Oldham, seconded by Marshall. All in Favor.

BILL NO. 2023-210, ORDINANCE NO. 11925 – AN ORDINANCE AMENDING THE BUDGET FOR THE FISCAL YEAR 2023-2024 AND RATIFYING THE EMERGENCY PURCHASE AND INSTALLATION OF A BOILER AT THE WATER FILTRATION PLANT was read once by title.

2nd Reading – Motion by Oldham, 2nd by Marshall. All in Favor.

Final Passage – Motion by Oldham, 2nd by Bloess. All in Favor.

Roll Call Vote: Voting "Yes" were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted "No".

➤ The agreement with H. W. Lochner is for an Aviation Project Consultant for the Sedalia Regional Airport.

BILL NO. 2023-211, ORDINANCE NO. 11926 – AN ORDINANCE AUTHORIZING THE SELECTION OF AN AVIATION PROJECT CONSULTANT FOR AIRFIELD IMPROVEMENTS AT THE SEDALIA REGIONAL AIRPORT was read once by title.

2nd Reading – Motion by Oldham, 2nd by Marshall. All in Favor.

Final Passage – Motion by Oldham, 2nd by Marshall. All in Favor.

Roll Call Vote: Voting "Yes" were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted "No".

➤ The budget amendment is for the addition of the position of Asset Management Director.

RESOLUTION NO. 2067 – A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF SEDALIA, MISSOURI, STATING FACTS AND REASONS FOR THE NECESSITY TO AMEND AND INCREASE THE CITY'S ANNUAL BUDGET FOR FISCAL YEAR 2024 was read once by title and approved on motion by Oldham, seconded by Robinson. All in Favor.

BILL NO. 2023-212, ORDINANCE NO. 11927 – AN ORDINANCE AMENDING THE BUDGET FOR THE FISCAL YEAR 2023-2024 AND ADDING A NEW CLASSIFICATION AND JOB DESCRIPTION FOR THE POSITION OF ASSET MANAGEMENT DIRECTOR was read once by title.

2nd Reading – Motion by Oldham, 2nd by Robinson. All in Favor.

Final Passage – Motion by Oldham, 2nd by Marshall. All in Favor.

Roll Call Vote: Voting "Yes" were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted "No".

FINANCE & ADMINISTRATION – Chris Marshall, Chairman; Jack Robinson, Vice Chairman

➤ The Ordinance is for calling a General Election to be held on April 2, 2024, for the purpose of electing 1 councilman from each of the four Wards.

BILL NO. 2023-213, ORDINANCE NO. 11928 – AN ORDINANCE CALLING A GENERAL ELECTION TO BE HELD ON APRIL 2, 2024 FOR THE PURPOSE OF ELECTING ONE COUNCILMAN FROM EACH OF THE FOUR WARDS IN THE CITY OF SEDALIA, MISSOURI was read once by title.

2nd Reading – Motion by Oldham, 2nd by Marshall. All in Favor.

Final Passage – Motion by Oldham, 2nd by Bloess. All in Favor.

Roll Call Vote: Voting "Yes" were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted "No".

- The Ordinance is for calling a Bond Election to be held February 6, 2024 for funding for the North Wastewater Treatment Plant. A program is available through a potential Grant to offset the cost and low interest loans for such projects through the State Revolving Fund. These are tax exempt Bonds at half the market rate. To qualify, the borrower must have voter approval. With voter approval, the City will make the March 1, 2024 deadline for submission.

BILL NO. 2023-214, ORDINANCE NO. 11929 – AN ORDINANCE CALLING A BOND ELECTION IN THE CITY OF SEDALIA, MISSOURI was read once by title.

2nd Reading – Motion by Oldham, 2nd by Robinson. All in Favor.

Final Passage – Motion by Oldham, 2nd by Bloess. All in Favor.

Roll Call Vote: Voting “Yes” were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted “No”.

- The Ordinance amends the City of Sedalia’s Sick Leave Buy Back Policy to clarify buy back qualifications.

BILL NO. 2023-215, ORDINANCE NO. 11930 – AN ORDINANCE AMENDING THE CITY OF SEDALIA’S SICK LEAVE BUY BACK POLICY was read once by title.

2nd Reading – Motion by Oldham, 2nd by Marshall. All in Favor.

Final Passage – Motion by Oldham, 2nd by Marshall. All in Favor.

Roll Call Vote: Voting “Yes” were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted “No”.

- The Ordinance amends City Code to incorporate Federal purchasing requirements.

BILL NO. 2023-216, ORDINANCE NO. 11931 – AN ORDINANCE OF THE CITY OF SEDALIA, MISSOURI AMENDING THE CITY CODE AND ADOPTING AMENDED FINANCIAL POLICIES REGARDING PURCHASING was read once by title.

2nd Reading – Motion by Oldham, 2nd by Marshall. All in Favor.

Final Passage – Motion by Oldham, 2nd by Marshall. All in Favor.

Roll Call Vote: Voting “Yes” were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted “No”.

COMMUNITY DEVELOPMENT – Rhiannon M. Foster, Chairwoman; Tina Boggess, Vice Chairwoman

- The Ordinance authorizes the Pettis County Collector to collect special tax assessments. These costs come about when property owners fail to comply with property maintenance standards.

BILL NO. 2023-217, ORDINANCE NO. 11932 – AN ORDINANCE AUTHORIZING THE ISSUANCE AND COLLECTION OF A SPECIAL TAX BILL BY THE PETTIS COUNTY COLLECTOR’S OFFICE was read once by title.

2nd Reading – Motion by Oldham, 2nd by Marshall. All in Favor.

Final Passage – Motion by Oldham, 2nd by Robinson. All in Favor.

Roll Call Vote: Voting “Yes” were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted “No”.

- In May 2021, City Council added to City code the licensing for mobile food vendors to be able to obtain a 3-day license rather than for an entire year. The intent was to allow vendors to purchase a license for 3 days at a time in the amount of \$25.00. Language was added to the Code but not the fee schedule.

BILL NO. 2023-218, ORDINANCE NO. 11933 – AN ORDINANCE AMENDING SECTION 12-278 OF THE CITY’S CODE OF ORDINANCES REGARDING AN ADDITIONAL FEE FOR A PER DIEM MOBILE FOOD VENDOR LICENSE AND INCORPORATING SAID FEE INTO THE CITY’S FEE SCHEDULE was read once by title.

2nd Reading – Motion by Cross, 2nd by Oldham. All in Favor.

Final Passage – Motion by Cross, 2nd by Oldham. All in Favor.

Roll Call Vote: Voting "Yes" were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted "No".

APPOINTMENTS: None

BIDS: None

LIQUOR LICENSES: The following new and renewal Liquor Licenses were read and approved on motion by Oldham, seconded by Boggess. All in Favor.

New

*Paige Shearer dba The Local Tap, 700 South Ohio, Liquor by the Drink

Renewals:

*Cathy Geotz dba Break Time #3084, 318 West Broadway, Packaged Liquor

*Philip Sherman dba Dollar General #19535, 4215 East Broadway, Packaged Liquor

MISCELLANEOUS ITEMS FROM MAYOR/COUNCIL/ADMINISTRATOR:

Mayor Pro-Tem Rhiannon M. Foster extended an invitation to attend the Veterans Day Parade on Saturday and added that the Veterans Day Breakfast will be Friday, November 10, 2023, beginning at 7:30 a.m. at the High School. Mayor Pro-Tem Foster also commented that signs will be placed in Sedalia near the City Limit signs with the names of POW-MIA Veterans.

Mayor Pro-Tem Rhiannon M. Foster stated that a Santa's Helpers Toy Run was held from Cole Camp to Sedalia on motorcycles and Sedalia Police and Fire Departments were honored with plaques for their involvement in the campaign for 20 years.

Councilman Hiller stated that the new statue entitled "Scout" was revealed this past Saturday at the Trails End Site at the Missouri State Fairgrounds.

GOOD & WELFARE:

Rene Vance, 19813 Tanglenook, stated that last month she represented Sedalia Seniors in Jefferson City, Missouri, for the Silver Haired Legislation session. Following a debate, they did come up with five legislative priorities. The five priorities are to increase funding for transportation, increase accessibility to public buildings, require special dementia training for Long Term Care facilities, increase Medicaid special needs allowance to \$100 per month and money recovered by Missouri Health to be returned to the Missouri Health Network.

Cory City, 1804 South Park, stated that there have been many lawsuits against the City regarding Code Enforcement and nce he compiles the full list of complaints, he will forward them to the City Council. His major complaint is in regards to his trash can that is behind his house and has been there for 12 months after it should have been picked up. He has called waste management and he and his wife have spoken with Mayor Dawson about it but it has yet to be picked up. Code Enforcement wants to fine him for something that the City has failed to pick up.

The meeting adjourned at 8:12 p.m. on motion by Oldham, seconded by Bloess to a closed-door meeting in the upstairs conference room pursuant to subsections 1 (Legal Advice), 2 (Real Estate), 3 (Personnel), 9 (Negotiations with employee groups) and 12 (Negotiated Contracts) of Section 610.021 RSMo. Roll Call Vote: Voting "Yes" were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted "No".

The regular meeting reopened at 9:00 p.m. on motion by Oldham, seconded by Bloess. All in favor.

Jack Robinson	Present	Bob Hiller	Present
Thomas Oldham	Present	Bob Cross	Present
Chris Marshall	Present	Rhiannon Foster	Present
Tina Boggess	Present	Steve Bloess	Present

BUSINESS RELATED TO CLOSED DOOR MEETING:

BILL NO. 2023-219, ORDINANCE NO. 11934 – AN ORDINANCE AUTHORIZING A LABOR AGREEMENT BY AND BETWEEN THE CITY OF SEDALIA, MISSOURI AND SEDALIA FIRE FIGHTERS LOCAL 103 OF THE INTERNATIONAL ASSOCIATION OF FIRE FIGHTERS was read once by title.

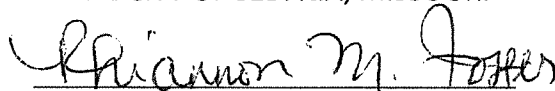
2nd Reading – Motion by Oldham, 2nd by Marshall. All in favor.

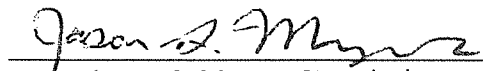
Final Passage – Motion by Oldham, 2nd by Robinson. All in favor.

Roll Call Vote: Voting “Yes” were Robinson, Oldham, Marshall, Boggess, Hiller, Cross, Foster and Bloess. No one voted “No”.

The regular meeting adjourned at 9:02 p.m. on motion by Oldham, seconded by Marshall. All in favor.

THE CITY OF SEDALIA, MISSOURI


 Rhiannon M. Foster, Mayor Pro-Tem


 Jason S. Myers, City Clerk

TRAFFIC ADVISORY COMMISSION MEETING

October 11, 2023

The Traffic Advisory Commission duly met on Wednesday, October 11, 2023 at 12:00 p.m. at the City of Sedalia Municipal Building. The meeting was called to order by Chairman Esquivel.

ROLL CALL:

Members		Ex-Officio Members	
Deidre Esquivel	Present	AJ Silvey	Not Present
James Callis	Present	Matt Irwin	Present
John Rucker	Present	Chris Davies	Present
Dennis Henderson	Present		
Byron Matson	Not Present	Secretary	Elizabeth Nations
Sherry Broyles	Not Present		
Charles Leftwich	Present		

Minutes from the September 13, 2023 meeting were approved.

Guests: Police Chief Matt Wirt, Police Patrol Commander Adam Hendricks, Code Enforcement Officer James Denny and Fire Inspector Jacob Carver.

OLD BUSINESS:

Availability of Handicap Parking Downtown

The Sedalia Main Streets Committee did approve to move forward with the proposed number of handicap spots and their placement. When the meeting minutes from the Sedalia Main Streets meeting are approved and provided to the Commission, the Commission can then move forward with the request.

Mr. Callis made the motion for the request to remain tabled in order for the Sedalia Main Streets approved meeting minutes to be provided to the Traffic Advisory Commission. Mr. Callis seconded. All were in favor.

NEW BUSINESS:

Designate No Parking on the North Side of W. 2nd St. from Winchester Dr. West to Where the Street Dead Ends

Code Enforcement Officer James Denny has requested that “No Parking” be designated on the north of side of the road. When vehicles are parked on both sides of the street, it does not meet Section 503.2.1 of the International Fire Code.

Chief Irwin stated while he is in support of designating the area as “No Parking” but with using the Fire Code then it would open up every numbered and named street within the City to be looked at and the roadway would need to have a 20-foot roadway in order to meet the Code. He also stated if this request is tied to the Fire Code going forward it would be hard to not to approve other requests as they would come in.

Currently Jim’s Tire Express customer vehicles are being parked along both sides of the roadway. With the vehicles parked then it makes it difficult for Fire and Police to traverse the roadway. Mr. Denny stated he has spoken to the business about moving the vehicles to other areas but no action was taken.

Ms. Esquivel suggested someone reach out to the business again and ask as a courtesy for the vehicles to not be parked on the south side of the roadway.

Mr. Rucker motioned to deny the request. Mr. Leftwich seconded. All were in favor.

OTHER ITEMS FOR DISCUSSION:

Mr. Callis stated the speed limit on Winchester Dr. is currently 25 mph from Main St. to W. 16th St. He would like traffic counters to be placed in order to see how fast the vehicles are traveling from W. 10th St. to W. 16th St. He would like for the speed limit to possibly be increased. Public Works will be placing the counters on Winchester Dr. in the area between W. 10th St. to W.16th St. to gather the data requested.

Mr. Callis asked for the motion to be made and included in the minutes that the Commission wishes Ms. Nations a Happy Birthday.

There was general discussion concerning various intersections and construction projects.

The next meeting date is November 15, 2023.

The meeting adjourned at 12:41 p.m.



Let's Cross Paths

PLANNING & ZONING COMMISSION

Wednesday, October 4, 2023

Council Chambers

5:30 pm

Planning & Zoning Commission

Tolbert Rowe	Absent	Andrew Dawson	Present
Ann Richardson	Absent	Teresa McDermott	Absent
Rhonda Ahern	Present	Mike Privitt	Absent
Valerie Bloess	Present	Ann Graff	Present
Jerry Ross	Present		
Chris Marshall	Present		

STAFF:

- Kelvin Shaw
- John Simmons
- Jilene Streit
- Devin Lake

- Ann Richardson, Vice-Chairman called the meeting to order at 5:30 pm
- Roll Call
- Welcome two new members, Ian Shoemaker & Ann Graff
- Chris Marshall made the motion to approve the minutes from the August 2, 2023 meeting. Mayor Dawson seconded the motion. All approved.

➤ **New Business**

Open Public Hearing – 1012 North Ohio. Application by PIB Sedalia for a church building. Wants to rezone from R-1 Single Family Residential to C-3 Commercial. Public Hearing open at 5:35 p.m.

Isreal Baeza, Church Building Committee Chairman represented the application with a summary of justification of the rezoning. No comments. Public Hearing closed 5:38 pm. John Simmons went through the particulars to rezone of the application from current R-1 Single Family Residential to C-3 Commercial. Staff recommends approval of this rezoning and it is in the general interest of the public. Val Bloess made the motion to recommend approval; Terry McDermott seconded. YES - 8; NO - 0. This application will move to Council for the October 16, 2023 meeting.

Open Public Hearing- 600 S Missouri. Application by Les Maisons LLC (Paul Beard). Public Hearing open at 5:41pm. Application is to rezone property at 600 S Missouri from R-1 Single Family Residential to R-3 Multi-Family. Present use of property is a four-plex built in 1971. No representation from owner. John Simmons read the letter from Paul Beard that was submitted with the application.

John Rhoads, 1411S Ohio - spoke in favor of the rezoning. Family owns a large amount of property in that neighborhood, many of which are multi-family & were built prior to the ordinance in 1983 that changed this to single family. This property was zoned wrong from this change. It was changed so that historic homes couldn't be converted into multi-family homes. This was not built as a single family home. It won't be a historic home. Believe this change will make a precedent moving forward other than maybe that this board would be willing to look at properties individually and change things that aren't right to start with. There are 10 houses on this block, 3 of which are single family. Need to protect this property owner's value in this property and future property owners, but not just the property owners of a small group.

The following individuals spoke in opposition of the rezoning:

Jan Bahner 705 W 3rd
Linda Wells, 617 W 5th
Missy, 607 W 6th
Heather & Steve Cooper, 608 W 5th
Melissa Turner, 517 W 6th
Judy Woolery, 624 W 7th
Billy Dunn, 700 W 6th
Richard Bahner, 705 W 3rd
Lee Scribner, 720 W 10th
Chris Paszkiewicz, 712 W Broadway
Bill Woolery, 624 W 7th
Michelle Bassett, 717 W 6th
Heather Smith, 809 W 6th

Letters were sent and read by John Simmons:

Barbara Schrader
Byron Matson
Rachel Dawson
Lindsey & Brian Phillips
Richard Bahner
e-mail from Wendy Smith

Close Public Hearing at 6:13 pm.

Mayor Andrew Dawson and Chairperson Rhonda Ahern abstain from voting. John Simmons said in the packet that was sent to you was the Ordinance from 1983 which created the R-1 zoning, a copy of a newspaper clipping from the Sedalia Democrat explaining the issue from 1983. John Simmons answered the question of tearing down, building a new 4-plex. The applicant applied for the rezoning due to if a catastrophe were to happen that they could rebuild a 4-plex in its place. Right now it is a legal non-confirming property, that the zoning change was enacted after the building had been built.

The property would need to be zoned R-3 to rebuild a 4-plex. The intent of the ordinance back in 1983 if something should befall one of these multi-family residential conversions that if something were to happen they could only be rebuilt as a single family residential. This application is due to the intent to sell the property however, the lender will not finance the property without the reassurance they could rebuild the 4-plex and not a single family residential. John Simmons read through the specifics of the staff recommendation. Staff recommendation is to deny the rezoning application. Terry McDermott made the motion to approve the rezoning. NO-6; YES-0; ABSTAIN - 2. This recommendation will go to Council on October 16, 2023.

Open Public Hearing- 204 E 24th Street. Special Use Permit application from Nicholas Dilthey.

Public Hearing opened at 6:27 p.m. John Simmons indicated the property is currently zoned C-1. Applicant had originally requested rezoning to C-3, staff recommended after the cancelled September meeting, that this would be better served as a Special Use Permit. C-3 is too broad of a category to allow that zoning in that area.

Nicholas Dilthey, owner was present for the meeting. He purchased this property in 2017 and has been selling cars ever since. Hasn't had any problems, no complaints. Ever since he was growing up there has always been a car business there. Just purchased the property knowing he could sell cars there and now all of a sudden it's become a problem. That business is what supports his family and supports Sedalia by the revenue it brings in. Val wanted to know if he's had the license to sell cars there. Nick said he's had city license there for the last five years. He bought the property knowing he could sell vehicles there.

Gary Lahmeyer of 201 E 24th Street spoke and he has two properties across the street and have been there for probably 70 years. This property has always been a car lot or retail lot. He has no complaints or problems with the place and to his knowledge none of his neighbors have any complaints.

John said he did receive one phone call before the September meeting for the rezoning application, property owner across the street to the north was opposed to it.

The public hearing closed at 6:32. John said in the packet was a letter from Baker Legal Services, Daniel Baker, on behalf of the applicant. John also drove past the property in mid-September & took some pictures of the property. Applicant requests Special Use Permit to continue the use of the property for automobile sales. Currently used for the sale of used automobiles and carport structures. This use is in conflict with the zoning and applicant has received a notice of violation of the city code. In the last few years have changed the way of communication between departments. He was issued a business license before code enforcement noticed was in conflict of zoning ordinance. Commercial building was erected in 1977 and housed an automobile implement service. Current owner has been selling automobiles since 2019 until code enforcement revealed this was in violation of the zoning code. Applicant submitted rezoning application for the September Planning & Zoning meeting but that meeting was cancelled due to lack of quorum. The recommendation at that time was to deny the rezoning to C-3 commercial. Staff recommended that a Special Use Permit be applied for as a special use permit is tied to the applicant and not the land. Should the land change hands, the special use permit ceases. The new owner has the opportunity to approach the board for another special use permit. Staff recommends the application for the Special Use Permit be approved due to the used car lot is not obtrusive to the neighborhood and does not increase traffic; the use would be attached to the applicant and not the land. Should the applicant ever sell the property the use would be invalidated whereas with rezoning to C-3 Commercial, other uses intrusive to residential neighborhoods would be allowed. Under Article V of the City of Sedalia's zoning code, "automobile or trailer sales rooms or yards, other than premises where used vehicles are dismantled" are eligible to apply for a Special Use permit. Making this recommendation with some stipulations.

Building Official, Devin Lake explained the conditions she's concerned with. Code Enforcement issued a violation letter for motor vehicles in February 2023, accumulation of trash & rubbish & zoning violation. To date the motor vehicles & zoning is still not compliant. The trash & rubbish has been taken care of. Also realized the carport constructed there did not obtain a building permit to be constructed there so a new violation letter was sent out last week. He has appeared in municipal court for these violations so seeing that the property is still in violation of the International Property Maintenance Code staff has made the recommendation of stipulations of this special use permit including: occupant must maintain the property in compliance with the International Property Maintenance Code; City may revoke special use permit upon violation of that code; sale of goods on that lot is limited to used vehicles, any other use of the exterior of the property is prohibited and preparation of sale of vehicles must be conducted inside the building and not on the exterior: Devin's recommendation all of these must be in compliance within 30 days. Mayor Dawson asked if there is any type of notice if found in violation or does the revocation happen automatically?

Devin said if found in violation again they would be issued another violation letter & per code they have 10 days to take care of the issue. Rhonda said he's selling carports as well. Devin said the sale of carports would be prohibited. Devin said there would be an appeals process for the revoking of the business license because of the revoking of the special use permit from having violations. John said the case of the carport is there was no building permit for it. Nick said he didn't know he had to have a permit. Devin said since this violation has been open since February that's why her recommendation would be that all those violations need to be corrected within 30 days. Ann said she doesn't feel comfortable having all these questions.

Terry said her question is that he has to maintain his property according to the International Property Maintenance Code is the owner aware of everything entailed in this IPMC? Devin said it's available on our City's website. John said the violations he received in the past are what the concern is. Terry said she just didn't know if there is anything else in there that he may not be aware of that might just pop up. Nick said the carport is just for display. It is anchored to the ground. Nick sells the carports for Coast to Coast . He didn't know you had to have a permit for this carport. Mr. Saker asked if it's possible to get a carport to keep it. Devin said as long as a sale isn't occurring and as long as it meets all the setbacks that would have been addressed during the building permit process. Not moving carports in & out, used as a display building only. Jerry Ross made a motion to table for 30 days, seconded by Rhonda Ahern for Mr. Dilthey to come into compliance with these issues.

- Old Business - None
- Next meeting - November 8, 2023

Jerry Ross made the motion to adjourn the meeting. Chris Marshall seconded. All approved. Meeting adjourned.

**CITY COUNCIL
OF THE CITY OF SEDALIA, MISSOURI**

RESOLUTION NO. _____

**A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF SEDALIA, MISSOURI,
STATING FACTS AND REASONS FOR THE NECESSITY TO AMEND AND INCREASE
THE CITY'S ANNUAL BUDGET FOR FISCAL YEAR 2024.**

WHEREAS, Section 67.010 of the Revised Statutes of Missouri requires each political subdivision of the State of Missouri ("State") to prepare an annual budget and establishes the requirements for that budget; and

WHEREAS, the City of Sedalia, Missouri ("City"), is a city of the third classification created pursuant to Chapter 77, RSMo, and is a political subdivision of the State of Missouri; and

WHEREAS, the City Council of the City adopted and approved the City's annual budget for Fiscal Year 2023 in accordance with the requirements of Section 67.010, RSMo, by Ordinance No. 11535 on March 21, 2022, and

WHEREAS, Sections 67.030 and 67.040 authorize and provide a procedure for the City Council to amend the City's annual budget to increase expenditures in any fund; and

WHEREAS, expenses for City's operations for Fiscal Year 2024 have been higher than budgeted, but do not exceed revenues plus the City's unencumbered balance brought forward from previous years; and

WHEREAS, the City Council of the City desire to state the facts and reasons necessitating an amendment to increase certain expenditures in the Fiscal Year 2024 annual budget.

NOW THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF SEDALIA, MISSOURI, AS FOLLOWS:

Section 1. Expenditures from the City's General Fund must be increased by a total of \$91,103.55 above the amount authorized in the adopted annual budget for Fiscal Year 2024. An amendment to increase said budget is necessary for the following facts and reasons:

- A. IT Network Security Enhancements and Management
- B. Offset mostly with 10% matching grant through Homeland Security.

Section 2. This Resolution shall take effect immediately upon its execution by the Mayor or otherwise as provided by law.

PASSED by the City Council of the City of Sedalia, Missouri, on November 20, 2023

Presiding Officer of the Council

ATTEST: _____
Jason S. Myers, City Clerk

BILL NO. _____

ORDINANCE NO. _____

AN ORDINANCE AMENDING THE BUDGET FOR THE FISCAL YEAR 2023-2024 AND APPROVING AND ACCEPTING A QUOTE FOR THE PURCHASE OF DETECTION AND REMEDIATION SERVICES.

NOW THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE CITY OF SEDALIA, MISSOURI as follows:

Section 1. The 2023-2024 fiscal year budget beginning April 1, 2023 and ending March 31, 2024 is hereby amended to modify certain budgeted line items as they appear on the attached schedule and made a part hereof as Exhibit A as if fully set out herein.

Section 2. The City Council of Sedalia, Missouri hereby approves and accepts the quote by and between the City of Sedalia, Missouri and Sophos, Inc and shall pay the sum and amount of Ninety-One Thousand One Hundred Three Dollars and Fifty-Five Cents (\$91,103.55), offset by a reimbursement of \$81,993.20 through a Grant by the Missouri Department of Homeland Security and the City's 10% match of \$9,110.35 as more fully described in the quote attached to this Ordinance and incorporated by reference herein.

Section 3. The Mayor, City Administrator or IT Manager are authorized and directed to execute and the City Clerk is hereby authorized and directed to attest and fix the seal of the City of Sedalia, Missouri on the quote in substantively the same form and content as the quote has been proposed.

Section 4. The City Clerk is hereby directed to file in his office a duplicate or copy of the quote after it has been executed by the parties or their duly authorized representatives.

Section 5. This ordinance shall be in full force and effect from and after its passage and approval.

Read two times by title, copies of the proposed ordinance having been made available for public inspection prior to the time the bill is under consideration by the Council and passed by the Council of the City of Sedalia, Missouri this 20th day of November 2023.

Presiding Officer of the Council

Approved by the Mayor of said City this 20th day of November 2023.

Andrew L. Dawson, Mayor

ATTEST:

Jason S. Myers, Clerk

Exhibit A
City of Sedalia
FY24 Budget Amendment 11/20/2023 IT Network Security Enhancements

Account / Description	Current Budget	Change	Amended Budget	Comments
Revenues / Source of Funds				
10-00-432-00	(201,179.62)	(81,993.20)	(283,172.82)	Homeland Security Grant Funds
Total Revenue Change		<u>(81,993.20)</u>		
Expenditures / Uses of Funds				
10-59-351-05 IT Capital - Software	-	73,046.83	73,046.83	Detection Software
10-09-225-00 IT Maintenance Agreements	40,178.17	18,056.72	58,234.89	Detection Management
			-	
			-	
			-	
Total Expenditure Change		<u>91,103.55</u>		
			<u><u>(9,110.35)</u></u>	Net Increase (Decrease) In Projected Fund Balance

City of Sedalia
Information Technology Services
200 S. Osage, Sedalia, MO 65301

To: Kelvin Shaw, C.P.A., City Administrator

From: Monte Richardson MWR

Date: 11/16/23

Re: Network Security Enhancement

Sir:

I have been awarded a grant through the Department of Homeland Security to bolster our IT infrastructure security. One of the targeted items in that grant is the ability to monitor and respond to cyber threats in a timely manner.

There are several reasons for the City to bolster our ability to monitor and respond to these threats. We have a trust relationship with the citizens to protect their data and be able to provide services as needed in a timely manner 24x7x365. Recovery from a cyber-event can be very expensive and time consuming if not addressed in a timely manner. Meeting the challenges of cybersecurity requires a specific skillset and time resource that the City is not able to provide on its own. Many organizations similar to the City have leveraged Security Operations Center as a Service (SOCaaS) where a vendor with the skillset and manpower monitors networks around the clock and responds to threats immediately.

I initially screened five vendors and selected four vendors to review and get quotes from. The features that I was looking for included Endpoint Detection & Remediation, Network Detection and Remediation (other devices such as switches/firewalls, etc.), Vulnerability Scanning, and Penetration Testing. All four vendors had different approaches to addressing EDR, NDR, Vulnerability Scanning, and Pen Testing.

Sophos was the winning bidder. Their quote came in at \$99,411.19 for 24 months of coverage. Their quote did not include Pen Testing but does include initial vulnerability scanning in order to validate network health at the beginning of the managed service.

Their solution is vendor agnostic not requiring everything to be Sophos branded to provide full service protection. They provide a warranty in case of a "breach incident" to cover recovery expenses and ransomware payment. The warranty is not meant to replace cyber-insurance and was not a deciding factor in the evaluations. Sophos, like all other vendors, provides monthly and quarterly reporting, a case manager in case of a breach incident, an established incident response plan and customized levels of intervention based on organization desires.

Compelling elements of their proposal were the ability to leverage existing software the City is using and the overarching ability to ingest network traffic across the board regardless of brand or architecture with ease. The other proposals that were considered

were over budget, required significant software installation and/or more specialized equipment installation to accomplish the same feature set.

This purchase would be made through the NCPA/Omnia Cooperative Purchasing Program, a nationally recognized cooperative procurement program. This particular purchasing agreement was competitively bid at the request of the Region XIV Education Service Center, Abilene, TX and awarded to TD Synnex. Relevant information regarding NCPA/Omnia, TD Synnex and Region XIV ESC are attached.

Definitions related to tabulation results

1. SOC – Security Operations Center (as a Service), manpower and tools to ingest network traffic, analyze questionable traffic, respond to alerts from tools and software platforms, ability to separate false positives from real threats in real time, respond in real time when threats are identified.
2. EDR – Endpoint Detection & Remediation, is software designed to protect computers and servers from identified threats, report suspicious activity identified on the computer, execute predefined actions based on threats identified.
3. MDR – Managed Detection & Remediation, professional services conducted by the SOC personnel when a breach incident is identified.
4. NDR – Network Detection & Remediation, tools and skills to ingest and analyze network traffic beyond the endpoint. Typically this element detects breach incidents where intruders are in the process of exploring the network elements, switches, hosts, and devices, seeking to identify weaknesses that can be exploited.
5. PenTesting – properly known as penetration testing, is a targeted attack on the customer network from inside and/or outside the network to assess overall security and identify weakness and known vulnerabilities that exist on the network.
6. Vulnerability Scan – a relatively automated process of scanning hardware, software, and network elements for potential risks and attack vectors that could be exploited by an attacker to gain privileged access to resources and/or data. Vulnerability Scanning is a point in time event. Scans can be done as a one-time event or as something done on a periodic basis. The City is seeking professional services for periodic scanning and remediation.

Tabulated quotes are as follows:

Vender	TOTAL		SOC/MDR	EDR	Setup	NDR	PenTesting	Vuln Scan
3rd Wave	\$115,200.00	\$57,600.00	\$97,200.00	Incl	None	None	\$18,000.00	None
Sophos	\$99,411.19	\$49,705.60	\$79,701.39	Incl	None	\$19,709.80	None	None
Vigilante	\$189,140.72	\$94,570.36	\$148,080.56	\$9,032.80	\$10,007.56	\$129,040.20	\$25,000.00	\$41,060.16
11:11*	\$142,965.50	\$47,655.17	\$121,606.56	incl	\$5,066.94	Incl	\$16,292.00	incl

I would like to have this on the Council Agenda for 11/20/23 for approval of the purchase of Central Managed Detection and Response Complete (desktop), Central Managed Detection and Response (server) and Central Network Detection and Response from Blue Tree Technology of Riverside MO for \$91,103.55 for a 22 month

term. Please note that this the current quote is a revision of the original. A revision was required because there was an extended delay in getting acceptable contract provisions and the quote needed to be adjusted to keep the purchase within the period of performance in the grant. The purchase will be made under NCPA cooperative procurement contract # 01-97. See the attached quote from Blue Tree Technology and supporting documentation from Sophos, Omni/NCPA, and TD Synnex. Under the terms of the grant, the City has a 10% match requirement of \$9,110.35 with the balance, \$81,993.20 to be reimbursed by the Missouri Department of Homeland Security. This purchase will required a budget amendment as well for FY24 as well.

Respectfully submitted.



Renewal Proposal

Client:	City of Sedalia
Delivered on:	November 15, 2023



Welcome

Dear Monte

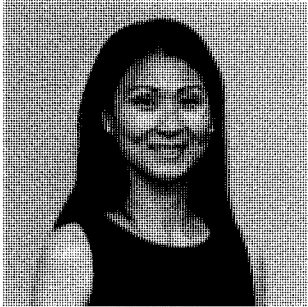
I wanted to thank you for the opportunity to submit a proposal.

Our goal is to do everything we can to make this an effortless process. I understand your time is valuable and I appreciate you allowing us to serve you!

Regards,

A handwritten signature in black ink, appearing to read "Isadora Horning", written over a horizontal line.

Isadora Horning and the team at Blue Tree Technology



ABOUT BLUE TREE TECHNOLOGY

Who are we?

We are a dynamic IT company that is minority women-owned and located in Riverside, Missouri. We take pride in delivering top-notch, friendly IT support services.

Our team of IT support professionals has a wealth of experience, with over a hundred years of combined expertise in installing, configuring, and maintaining IT infrastructure for Small and Medium Businesses. We comprehend the unique requirements of our clients and implement solutions that suit their businesses in the short and long term.

As your reliable IT partner, we offer personalized service and advice tailored to your specific needs.

Core Values

Our Core Values are a critical aspect of our business, and we believe that they are a key indicator of our success in providing IT solutions to our clients. We encourage you to review our Core Values and see if they align with your own business values. We firmly believe that a strong alignment of values is the foundation for a successful and mutually beneficial partnership.

- **Service Excellence:**
 - Respectful
 - Patient Listening
 - Compassionately Helpful
- **Teachable:**
 - Curious
 - Critical Thinking
 - Shares Knowledge
- **Calm Under Stress:**
 - De-escalating
 - Confident
 - Good Humor
- **Grace:**
 - Speaks truth with love



Quote

Blue Tree Technology
1827 NW Vivion Road
Riverside, MO 64150
United States

T: 816-256-2595

Prepared for City of Sedalia
Monte Richardson
200 South Osage Avenue
Sedalia, MO 65301
United States

T: 660-827-3000
E: mrichardson@sedalia.com

Table with quote details: Quote # 6051 v7, Date November 15, 2023, Expires November 30, 2023, Contact Glen Sharp

ACCEPT QUOTE

City of Sedalia - Upgrade Intercept X to MDR 2023

One-Time Fees

Table with 4 columns: Item, Qty, Price, Total. Lists items like MDRCEU22AERGAA, MDRCS22BCRGAA, and MDRNDU22AFRGAA with their respective quantities and prices.

† Non-taxable item

Please contact us if you have any questions.

Summary table: One-Time Subtotal \$98,134.60, Discount (\$7,031.05), Total One-Time \$91,103.55 USD

ACCEPT QUOTE



Cost Breakdown

Category	One-Time Fees
Product	\$98,134.60
Discount	(\$7,031.05)
Total	\$91,103.55 USD

Contract Name: COS Sophos MDR

Contract #NCPA 01-97

MICHAEL L. PARSON
Governor

SANDRA K. KARSTEN
Director



Lewis & Clark State Office Bldg.
Mailing Address: P.O. Box 749
Jefferson City, MO 65101-0749
Telephone: 573-751-4905
Fax: 573-751-5399

STATE OF MISSOURI
DEPARTMENT OF PUBLIC SAFETY
OFFICE OF THE DIRECTOR

February 21, 2023

Mr. Kelvin Shaw, City Administrator
Sedalia Police Department
200 W. 2nd St.
Sedalia, MO 65301

RE: FY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Award #EMW-2022-CY-00031-NR6

Dear Mr. Shaw:

Thank you for your recent application submission to the FY 2022 State and Local Cybersecurity Grant Program (SLCGP). Your application has been selected for funding in the amount of \$161,224.64. As a condition of this award, you are required to contribute a cost match in the amount of \$17,913.85 of non-Federal funds, or ten percent of the total approved project costs of \$179,138.49.

Enclosed is the FY 2022 SLCGP Subaward Agreement for Sedalia Police Department. The Missouri Office of Homeland Security asks you to carefully review and sign the documentation provided. By signing the Subaward Agreement and initialing each page of the Articles of Agreement and Special Conditions you are certifying your acceptance of the award conditions. Once signed and initialed, please return the documents to our office no later than March 21, 2023.

The project period of performance for this award begins December 1, 2022 and ends November 30, 2025.

A risk assessment for this award was completed in accordance with requirements from 2 CFR 200.332. Sedalia Police Department received a total score of seventeen (17), which classifies the agency as a medium risk subrecipient of noncompliance with the FY 2022 SLCGP.

We look forward to working with you on this award. Should you have any questions or need additional information, do not hesitate to contact Chelse Dowell at (573) 751-3879 or Chelse.Dowell@dps.mo.gov.

Sincerely,

Joni McCarter, Program Manager
Missouri Department of Public Safety
Office of Homeland Security

Attachment(s): Subaward Agreement
Articles of Agreement/Special Conditions

Alcohol & Tobacco Control • Capitol Police • Fire Safety • Gaming Commission • Highway Patrol
State Emergency Management Agency • Veterans Commission



Missouri Department of Public Safety
Office of Homeland Security
Division of Grants
 P.O. Box 749, Jefferson City, MO 65101
 Telephone: 573-526-6125 Fax: 573-526-9012

SUBAWARD AGREEMENT

SUBRECIPIENT NAME Sedalia Police Department		DATE 02/21/2023	
ADDRESS 200 West 2nd Street		FEDERAL IDENTIFICATION NUMBER EMW-2022-CY-00031	OHS CONTROL NUMBER NR6
CITY Sedalia		STATE MO	ZIP CODE 65301
TOTAL AMOUNT OF THE FEDERAL AWARD \$179,138.49		AMOUNT OF FEDERAL FUNDS OBLIGATED BY THIS ACTION \$161,224.64	
TOTAL AMOUNT OF FEDERAL FUNDS OBLIGATED TO THE SUBRECIPIENT \$161,224.64		TOTAL APPROVED COST SHARING OR MATCHING \$17,913.85	
PROJECT PERIOD FROM 12/01/2022	PROJECT PERIOD TO 11/30/2025	FEDERAL AWARD DATE 12/01/2022	
PROJECT TITLE FY 2022 SLCGP-Non-Rural – Sedalia Police Department		FUNDED BY FY 2022 State and Local Cybersecurity Grant Program	
FEDERAL AWARING AGENCY Department of Homeland Security	PASS THROUGH ENTITY MO Department of Public Safety/Office of Homeland Security	IS THIS AWARD R&D YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	INDIRECT COST RATE YES <input type="checkbox"/> NO <input checked="" type="checkbox"/> AMOUNT
CATALOG OF FEDERAL DOMESTIC ASSISTANCE (CFDA) NUMBER 97.137		METHOD OF PAYMENT (Reimbursement – Advanced) Reimbursement	
CONTACT INFORMATION			
OHS GRANT SPECIALIST		SUBRECIPIENT PROJECT DIRECTOR	
NAME Chelse Dowell		NAME Monte Richardson, IT Director	
E-MAIL ADDRESS Chelse.Dowell@dps.mo.gov		ADDRESS (If different from above) 200 South Osage Avenue	
TELEPHONE (573) 751-3879		CITY, STATE AND ZIP CODE Sedalia, MO 65301	
PROGRAM MANAGER Joni McCarter		TELEPHONE 660-851-7625	E-MAIL ADDRESS mrichardson@sedalia.com
SUMMARY DESCRIPTION OF PROJECT <p>The purpose of the Fiscal Year 2022 State and Local Cybersecurity Grant Program (SLCGP) is to assist state, local, and territorial (SLT) governments with managing and reducing systemic cyber risk. Through funding from the Infrastructure Investment and Jobs Act, also known as the Bipartisan Infrastructure Law, the SLCGP enables DHS to make targeted cybersecurity investments in SLT government agencies, thus improving the security of critical infrastructure and improving the resilience of the services SLT governments provide their community.</p>			
AWARDING AGENCY APPROVAL		SUBRECIPIENT AUTHORIZED OFFICIAL	
TYPED NAME AND TITLE OF DPS OFFICIAL Sandra K. Karsten, Director		TYPED NAME & TITLE OF SUBRECIPIENT AUTHORIZED OFFICIAL Kelvin Shaw, City Administrator	
SIGNATURE OF APPROVING DPS OFFICIAL	DATE	SIGNATURE OF SUBRECIPIENT AUTHORIZED OFFICIAL	DATE
<p>THIS SUBAWARD IS APPROVED SUBJECT TO SUCH CONDITIONS OR LIMITATIONS SET FORTH ON THE ATTACHED SPECIAL CONDITION(S). BY SIGNING THIS SUBAWARD AGREEMENT THE SUBRECIPIENT IS AGREEING TO READ AND COMPLY WITH ALL SPECIAL CONDITIONS.</p>			

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

TABLE OF CONTENTS

Article I	Summary Description of Award
Article II	DHS Standard Terms and Conditions Generally
Article III	Assurances, Administrative Requirements, Cost Principles, Representations and Certifications
Article IV	General Acknowledgements and Assurances
Article V	Acknowledgement of Federal Funding from DHS
Article VI	Activities Conducted Abroad
Article VII	Age Discrimination Act of 1975
Article VIII	Americans with Disabilities Act of 1990
Article IX	Best Practices for Collection and Use of Personally Identifiable Information (PII)
Article X	Civil Rights Act of 1964 – Title VI
Article XI	Civil Rights Act of 1968
Article XII	Copyright
Article XIII	Debarment and Suspension
Article XIV	Drug-Free Workplace Regulations
Article XV	Duplication of Benefits
Article XVI	Education Amendments of 1972 (Equal Opportunity in Education Act) – Title IX
Article XVII	Energy Policy and Conservation Act
Article XVIII	False Claims Act and Program Fraud Civil Remedies
Article XIX	Federal Debt Status
Article XX	Federal Leadership on Reducing Text Messaging while Driving
Article XXI	Fly America Act of 1974
Article XXII	Hotel and Motel Fire Safety Act of 1990
Article XXIII	John S. McCain National Defense Authorization Act of Fiscal Year 2019
Article XXIV	Limited English Proficiency (Civil Rights Act of 1964, Title VI)
Article XXV	Lobbying Prohibitions
Article XXVI	National Environmental Policy Act
Article XXVII	Nondiscrimination in Matters Pertaining to Faith-Based Organizations
Article XXVIII	Non-Supplanting Requirement
Article XXIX	Notice of Funding Opportunity Requirements
Article XXX	Patents and Intellectual Property Rights
Article XXXI	Procurement of Recovered Materials
Article XXXII	Rehabilitation Act of 1973
Article XXXIII	Reporting of Matters Related to Recipient Integrity and Performance
Article XXXIV	Reporting Subawards and Executive Compensation
Article XXXV	Required Use of American Iron, Steel, Manufactured Products, and Construction Materials
Article XXXVI	SAFECOM
Article XXXVII	Terrorist Financing
Article XXXVIII	Trafficking Victims Protection Act of 2000 (TVPA)
Article XXXIX	Universal Identifier and System of Award Management
Article XL	USA PATRIOT Act of 2001
Article XLI	Use of DHS Seal, Logo, and Flags
Article XLII	Whistleblower Protection Act
Article XLIII	Environmental Planning and Historic Preservation (EHP) Review
Article XLIV	Disposition of Equipment Acquired Under the Federal Award
Article XLV	Office of Homeland Security, Specific
Article XLVI	Special Conditions

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

Article I – Summary Description of Award

The purpose of the FY 2022 HSGP is to support state and local efforts to prevent terrorism and other catastrophic events and to prepare the Nation for the threats and hazards that pose the greatest risk to the security of the United States. The HSGP provides funding to implement investments that build, sustain, and deliver the 32 core capabilities essential to achieving the National Preparedness Goal of a secure and resilient Nation. Among the five basic homeland security missions noted in the DHS Quadrennial Homeland Security Review, HSGP supports the goal to Strengthen National Preparedness and Resilience. The building, sustainment, and delivery of these core capabilities are not exclusive to any single level of government, organization, or community, but rather, require the combined effort of the whole community.

Article II – DHS Standard Terms and Conditions Generally

The Fiscal Year (FY) 2022 DHS Standard Terms and Conditions apply to all new federal financial assistance awards funded in FY 2022. These terms and conditions flow down to subrecipients unless an award term or condition specifically indicates otherwise. The United States has the right to seek judicial enforcement of these obligations.

All legislation and digital resources are referenced with no digital links. The FY 2022 DHS Standard Terms and Conditions will be housed on dhs.gov at www.dhs.gov/publication/fy15-dhs-standard-terms-and-conditions.

Article III – Assurances, Administrative Requirements, Cost Principles, Representations and Certifications

I. DHS financial assistance recipients must complete either the Office of Management and Budget (OMB) Standard Form 424B Assurances – Non-Construction Programs, or OMB Standard Form 424D Assurances – Construction Programs, as applicable. Certain assurances in these documents may not be applicable to your program, and the DHS financial assistance office (DHS FAO) may require applicants to certify additional assurances. Applicants are required to fill out the assurances applicable to their program as instructed by the awarding agency.

II. DHS/OHS financial assistance subrecipients are required to follow the applicable provisions of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards located at Title 2 Code of Federal Regulations (C.F.R.) Part 200 and adopted by DHS at 2 C.F.R. Part 3002.

III. By accepting this agreement the subrecipient and its executives, as defined in 2 C.F.R. section 170.315, certify that the subrecipient's policies are in accordance with OMB's guidance located at 2 C.F.R. Part 200, all applicable federal laws, and relevant Executive guidance.

Article IV – General Acknowledgements and Assurances

All subrecipients, successors, transferees, and assignees must acknowledge and agree to comply with applicable provisions governing DHS access to records, accounts, documents, information, facilities and staff.

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT
ARTICLES OF AGREEMENT

1. Subrecipients must cooperate with any compliance reviews or compliance investigations conducted by DHS/OHS.
2. Subrecipients must give DHS/OHS access to, and the right to examine and copy records, accounts and other documents and sources of information related to the award and permit access to facilities or personnel.
3. Subrecipients must submit timely, complete and accurate reports to the appropriate DHS/OHS officials and maintain appropriate backup documentation to support the reports.
4. Subrecipients must comply with all other special reporting, data collection, and evaluation requirements, as prescribed by law or detailed in program guidance.
5. Recipients (as defined in 2 C.F.R. Part 200 and including recipients acting as pass-through entities) of federal financial assistance from DHS or one of its awarding component agencies must complete the *DHS Civil Rights Evaluation Tool* within thirty (30) days of receipt of the Notice of Award for the first award under which this term applies. Recipients of multiple awards of DHS financial assistance should only submit one completed tool for their organization, not per award. After the initial submission, recipients are required to complete the tool once every two (2) years if they have an active award, not every time an award is made. Recipients should submit the completed tool, including supporting materials, to CivilRightsEvaluation@hq.dhs.gov. This tool clarifies the civil rights obligations and related reporting requirements contained in the DHS Standard Terms and Conditions. Subrecipients are not required to complete and submit this tool to DHS. The evaluation tool can be found at <https://www.dhs.gov/publication/dhs-civil-rights-evaluation-tool>.

The DHS Office for Civil Rights and Civil Liberties will consider, in its discretion, granting an extension if the recipient identified steps and a timeline for completing the tool. Recipients should request extensions by emailing the request to civilrightsevaluation@hq.dhs.gov prior to expiration of the 30-day deadline.

Article V – Acknowledgement of Federal Funding from DHS

Subrecipients must acknowledge their use of federal funding when issuing statements, press releases, requests for proposals, bid invitations, and other documents describing projects or programs funded in whole or in part with Federal funds.

Article VI – Activities Conducted Abroad

Subrecipients must ensure that project activities performed outside the United States are coordinated as necessary with appropriate government authorities and that appropriate licenses, permits, or approvals are obtained.

Article VII – Age Discrimination Act of 1975

Subrecipients must comply with the requirements of the Age Discrimination Act of 1975, Pub. L. No. 94-135 (1975) (codified as amended at Title 42, U.S. Code, section 6101 et seq.), which prohibits discrimination on the basis of age in any program or activity receiving federal financial assistance.

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023
SUBAWARD AGREEMENT ARTICLES OF AGREEMENT	

Article VIII – Americans with Disabilities Act of 1990

Subrecipients must comply with the requirements of Titles, I, II and III of the Americans with Disabilities Act, Pub. L. No. 101-336 (1990) (codified as amended 42 U.S.C. sections 12101-12213), which prohibits subrecipients from discriminating on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities.

Article IX – Best Practices for Collection and Use of Personally Identifiable Information (PII)

Subrecipients who collect personally identifiable information (PII) are required to have a publicly available privacy policy that describes standards on the usage and maintenance of PII they collect. DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual. Subrecipients may also find the DHS Privacy Impact Assessments: Privacy Guidance and Privacy template as useful resources respectively.

Article X – Civil Rights Act of 1964 – Title VI

Subrecipients must comply with the requirements of Title VI of the Civil Rights Act of 1964 (codified as amended at 42 U.S.C. section 2000d et seq.), which provides that no person in the United States will, on the grounds of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving federal financial assistance. DHS implementing regulations for the Act are found at 6 C.F.R. Part 21 and 44 C.F.R. Part 7.

Article XI – Civil Rights Act of 1968

Subrecipients must comply with Title VIII of the Civil Rights Act of 1968, Pub. L. No. 90-284, as amended through Pub. L. 113-4, which prohibits subrecipients from discriminating in the sale, rental, financing, and advertising of dwellings, or in the provision of services in connection therewith, on the basis of race, color, national origin, religion, disability, familial status, and sex (see 42 U.S.C. section 3601 et seq.), as implemented by the U.S. Department of Housing and Urban Development at 24 C.F.R. Part 100. The prohibition on disability discrimination includes the requirement that new multifamily housing with four or more dwelling units—i.e., the public and common use areas and individual apartment units (all units in buildings with elevators and ground-floor units in buildings without elevators) - be designed and constructed with certain accessible features. (See 24 C.F.R. Part 100, Subpart D.)

Article XII – Copyright

Subrecipients must affix the applicable copyright notices of 17 U.S.C. sections 401 or 402 and an acknowledgement of U. S. Government sponsorship (including the award number) to any work first produced under federal financial assistance awards.

Article XIII – Debarment and Suspension

Subrecipients are subject to the non-procurement debarment and suspension regulations implementing Executive Orders (E.O.) 12549 and 12689, which are at 2 C.F.R. Part 180, as adopted by DHS at 2 C.F.R. Part 3000. These regulations restrict federal financial assistance awards, subawards, and contracts with certain parties that are debarred, suspended, or otherwise excluded from or ineligible for participation in federal assistance programs and activities.

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

Article XIV – Drug-Free Workplace Regulations

Subrecipients must comply with drug-free workplace requirements in Subpart B (or Subpart C, if the subrecipient is an individual) of 2 C.F.R. Part 3001, which adopts the Government-wide implementation (2 C.F.R. Part 182) of Sec. 5152-5158 of the Drug-Free Workplace Act of 1988 (41 U.S.C. sections 8101-8106).

Article XV – Duplication of Benefits

Any cost allocable to a particular federal financial assistance award provided for in 2 C.F.R. Part 200, Subpart E may not be charged to other federal financial assistance awards to overcome fund deficiencies; to avoid restrictions imposed by federal statutes, regulations, or federal financial assistance award terms and conditions; or for other reasons. However, these prohibitions would not preclude subrecipients from shifting costs that are allowable under two or more awards in accordance with existing federal statutes, regulations, or the federal financial assistance award terms and conditions.

Article XVI – Education Amendments of 1972 (Equal Opportunity in Education Act) – Title IX

Subrecipients must comply with the requirements of Title IX of the Education Amendments of 1972, Pub. L. No. 92-318 (1972) (codified as amended at 20 U.S.C. section 1681 et seq.), which provide that no person in the United States will, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any educational program or activity receiving federal financial assistance. DHS implementing regulations are codified at 6 C.F.R. Part 17 and 44 C.F.R. Part 19.

Article XVII – Energy Policy and Conservation Act

Subrecipients must comply with the requirements of the Energy Policy and Conservation Act, Pub. L. No. 94-163 (1975) (codified as amended at 42 U.S.C. section 6201 et seq.), which contain policies relating to energy efficiency that are defined in the state energy conservation plan issued in compliance with this Act.

Article XVIII – False Claims Act and Program Fraud Civil Remedies

Subrecipients must comply with the requirements of the False Claims Act, 31 U.S.C. sections 3729-3733, which prohibits the submission of false or fraudulent claims for payment to the federal government. (See 31 U.S.C. sections 3801-3812, which details the administrative remedies for false claims and statements made.)

Article XIX – Federal Debt Status

All subrecipients are required to be non-delinquent in their repayment of any federal debt. Examples of relevant debt include delinquent payroll and other taxes, audit disallowances, and benefit overpayments. (See OMB Circular A-129.)

Article XX– Federal Leadership on Reducing Text Messaging while Driving

Subrecipients are encouraged to adopt and enforce policies that ban text messaging while driving as described in E.O. 13513, including conducting initiatives described in Section 3(a) of the Order when on official Government business or when performing any work for or on behalf of the federal government.

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

Article XXI – Fly America Act of 1974

Subrecipients must comply with Preference for U.S. Flag Air Carriers (air carriers holding certificates under 49 U.S.C.) for international air transportation of people and property to the extent that such service is available, in accordance with the International Air Transportation Fair Competitive Practices Act of 1974, 49 U.S.C. section 40118, and the interpretative guidelines issued by the Comptroller General of the United States in the March 31, 1981, amendment to Comptroller General Decision B-138942.

Article XXII – Hotel and Motel Fire Safety Act of 1990

Subrecipients must ensure that all conference, meeting, convention, or training space funded in whole or in part with federal funds complies with the fire prevention and control guidelines Section 6 of the Hotel and Motel Fire Safety Act of 1990, 15 U.S.C. section 2225a.

Article XXIII – John S. McCain National Defense Authorization Act of Fiscal Year 2019

Subrecipients, their contractors, and subcontractors are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (2018) and 2 C.F.R. sections 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. Beginning August 13, 2020, the statute – as it applies to DHS recipients, subrecipients, and their contractors, and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

Article XXIV – Limited English Proficiency (Civil Rights Act of 1964, Title VI)

Subrecipients must comply with the Title VI of the Civil Rights Act of 1964 (42 U.S.C. section 2000d et seq.) prohibition against discrimination on the basis of national origin, which requires that recipients of federal financial assistance take reasonable steps to provide meaningful access to persons with limited English proficiency (LEP) to their programs and services. For additional assistance and information regarding language access obligations, please refer to the DHS Recipient Guidance <https://www.dhs.gov/guidance-published-help-department-supported-organizations-provide-meaningful-access-people-limited> and additional resources on <http://www.lep.gov>.

Article XXV– Lobbying Prohibitions

Subrecipients must comply with 31 U.S.C. section 1352, which provides that none of the funds provided under a federal financial assistance award may be expended by the subrecipient to pay any person to influence, or attempt to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any federal action related to the federal award or contract, including any extension, continuation, renewal, amendment, or modification.

Article XXVI – National Environmental Policy Act

Subrecipients must comply with the requirements of the National Environmental Policy Act of 1969, Pub. L. No. 91-190 (1970) (codified as amended at 43 U.S.C. section 4321 et seq.) (NEPA) and the Council on Environmental Quality (CEQ) Regulations for Implementing the Procedural Provisions of NEPA, which require subrecipients to use all practicable means within their authority, and consistent with other essential considerations of national policy, to create and maintain conditions under which people and nature can

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

exist in productive harmony and fulfill the social, economic, and other needs of present and future generations of Americans.

Article XXVII – Nondiscrimination in Matters Pertaining to Faith-Based Organizations

It is DHS policy to ensure the equal treatment of faith-based organizations in social service programs administered or supported by DHS or its component agencies, enabling those organizations to participate in providing important social services to beneficiaries. Subrecipients must comply with the equal treatment policies and requirements contained in 6 C.F.R. Part 19 and other applicable statutes, regulations, and guidance governing the participations of faith-based organizations in individual DHS programs.

Article XXVIII – Non-Supplanting Requirement

Subrecipients receiving federal financial assistance awards made under programs that prohibit supplanting by law must ensure that federal funds do not replace (supplant) funds that have been budgeted for the same purpose through non-federal sources.

Article XXIX – Notice of Funding Opportunity Requirements

All of the instructions, guidance, limitations, and other conditions set forth in the Notice of Funding Opportunity (NOFO) for this program are incorporated here by reference in the award terms and conditions. All subrecipients must comply with any such requirements set forth in the program NOFO.

Article XXX – Patents and Intellectual Property Rights

Subrecipients are subject to the Bayh-Dole Act, 35 U.S.C. section 200 et seq., unless otherwise provided by law. Subrecipients are subject to the specific requirements governing the development, reporting, and disposition of rights to inventions and patents resulting from federal financial assistance awards located at 37 C.F.R. Part 401 and the standard patent rights clause located at 37 C.F.R. section 401.14.

Article XXXI – Procurement of Recovered Materials

Subrecipients must comply with section 6002 of the Solid Waste Disposal Act, Pub. L. No. 89-272 (1965), (codified as amended by the Resource Conservation and Recovery Act, 42 U.S.C. section 6962.) The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 C.F.R. Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition.

Article XXXII – Rehabilitation Act of 1973

Subrecipients must comply with the requirements of Section 504 of the Rehabilitation Act of 1973, Pub. L. No. 93-112 (1973) (codified as amended at 29 U.S.C. section 794), which provides that no otherwise qualified handicapped individuals in the United States will, solely by reason of the handicap, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving federal financial assistance.

Article XXXIII – Reporting of Matters Related to Recipient Integrity and Performance

If the total value of the subrecipient's currently active grants, cooperative agreements, and procurement contracts from all federal awarding agencies exceeds \$10,000,000 for any period of time during the period of performance of this federal award, you must comply with the requirements set forth in the government-wide Award Term and Condition for Recipient Integrity and Performance Matters located at 2 C.F.R. Part

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

200, Appendix XII, the full text of which is incorporated here by reference in the award terms and conditions.

Article XXXIV – Reporting Subawards and Executive Compensation

Subrecipients are required to comply with the requirements set forth in the government-wide award term on Reporting Subawards and Executive Compensation located at 2 C.F. R. Part 170, Appendix A, the full text of which is incorporated here by the reference in the award terms and conditions.

Article XXXV – Required Use of American Iron, Steel, Manufactured Products, and Construction Materials

Subrecipients must comply with the Build America, Buy America Act (BABAA), which was enacted as part of the Infrastructure Investment and Jobs Act Sections 70901-70927, Pub. L. No. 117-58 (2021); and Executive Order 14005, Ensuring the Future is Made in All of America by All of America’s Workers. See also Office of Management and Budget (OMB), Memorandum M-22-11, Initial Implementation Guidance on Application of Buy America Preference in Federal Financial Assistance Programs for Infrastructure.

Subrecipients of federal financial assistance programs for infrastructure are hereby notified that none of the funds provided under this award may be used for a project for infrastructure unless:

1. All iron and steel used in the project are produced in the United States – this means all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States;
2. All manufactured products used in the project are produced in the United States – this means the manufactured product was manufactured in the United States; and the cost of the components of the manufactured product that are mined, produced, or manufactured in the United States is greater than 55 percent of the total cost of all components of the manufactured product, unless another standard for determining the minimum amount of domestic content of the manufactured product has been established under applicable law or regulation; and
3. All construction materials are manufactured in the United States – this means that all manufacturing processes for the construction material occurred in the United States.

The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools, equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and furnishings, such as movable chairs, desk, and portable computer equipment, that are used at or within the finished infrastructure project, but are not an integral part of the structure or permanently affixed to the infrastructure project.

Waivers

When necessary, subrecipients may apply for, and the agency may grant, a waiver from these requirements.

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

a. When the federal agency has made a determination that one of the following exceptions applies, the awarding official may waive the application of the domestic content procurement preference in any case in which the agency determines that:

1. Applying the domestic content procurement preference would be inconsistent with public interest;
2. The types of iron, steel, manufactured products, or construction materials are not produced in the United States in sufficient and reasonably available quantities or of a satisfactory quality; or
3. The inclusion of iron, steel, manufactured products, or construction materials produced in the United States will increase the cost of the overall project by more than 25 percent.

A request to waive the application of the domestic content procurement preference must be in writing. The agency will provide instructions on the format, contents, and supporting materials required for any waiver request. Waiver requests are subject to public comment periods of no less than 15 days and must be reviewed by the OMB Made in America Office. There may be instances where an award qualifies, in whole, or in part, for an existing waiver described. For awards by the Federal Emergency Management Agency (FEMA), existing waivers are available and the waiver process is described at “Buy America” Preference in FEMA Financial Assistance Programs for Infrastructure. For awards by other DHS components, please contact the applicable DHS FAO.

To see whether a particular DHS federal financial assistance program is considered an infrastructure program and thus required to include a Buy America preference, please either contact the applicable DHS FAO, or for FEMA awards, please see Programs and Definitions: Build America, Buy America Act.

Article XXXVI – SAFECOM

Subrecipients receiving federal financial assistance awards made under programs that provide emergency communication equipment and its related activities must comply with the SAFECOM Guidance for Emergency Communication Grants, including provisions on technical standards that ensure and enhance interoperable communications.

Article XXXVII – Terrorist Financing

Subrecipients must comply with E.O. 13224 and U.S. law that prohibit transactions with, and the provisions of resources and support to, individuals and organizations associated with terrorism. Subrecipients are legally responsible to ensure compliance with the Order and laws.

Article XXXVIII – Trafficking Victims Protection Act of 2000 (TVPA)

Subrecipients must comply with the requirements of the government-wide financial assistance award term which implements Section 106 (g) of the Trafficking Victims Protection Act of 2000, (TVPA) (codified as amended by 22 U.S.C. section 7104). The award term is located at 2 C.F.R. section 175.15, the full text of which is incorporated here by reference.

Article XXXIX – Universal Identifier and System of Award Management

Subrecipients are required to comply with the requirements set forth in the government-wide financial assistance award term regarding the System for Award Management and Universal Identifier Requirements located at 2 C.F.R. Part 25, Appendix A, the full text of which is incorporated here by reference.

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

Article XL– USA PATRIOT Act of 2001

Subrecipients must comply with requirements of Section 817 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), which amends 18 U.S.C. sections 175-175c.

Article XLI – Use of DHS Seal, Logo and Flags

Subrecipients must obtain permission from their DHS FAO prior to using the DHS seal(s), logos, crests or reproductions of flags or likenesses of DHS agency officials, including use of the United States Coast Guard seal, logo, crests or reproductions of flags or likenesses of Coast Guard officials.

Article XLII – Whistleblower Protection Act

Subrecipients must comply with the statutory requirements for whistleblower protections (if applicable) at 10 U.S.C. section 2409, 41 U.S.C. 4712, and 10 U.S.C. section 2324, 41 U.S.C. sections 4304 and 4310.

Article XLIII – Environmental Planning and Historic Preservation (EHP) Review

DHS/FEMA funded activities that may require an Environmental Planning and Historic Preservation (EHP) review are subject to the FEMA EHP review process. This review does not address all federal, state, and local requirements. Acceptance of federal funding required subrecipient to comply with all federal, state, and local laws.

DHS/FEMA is required to consider the potential impacts to natural and cultural resources of all projects funded by DHS/FEMA grant funds, through its EHP review process, as mandated by: the National Environmental Policy Act; National Historic Preservation Act of 1966, as amended; National Flood Insurance Program regulations; and, any other applicable laws and executive orders. To access the FEMA EHP screening form and instructions, go to the DHS/FEMA website. In order to initiate EHP review of your project(s), you must complete all relevant sections of this form and submit it to the OHS/Grant Programs Directorate (GPD) along with all other pertinent project information. The EHP review process must be completed before funds are released to carry out the proposed project; otherwise DHS/FEMA may not be able to fund the project due to noncompliance with EHP laws, executive orders, regulations, and policies.

If ground disturbing activities occur during construction, applicant will monitor ground disturbance, and if any potential archeological resources are discovered, applicant will immediately cease work in that area and notify the pass-through entity, if applicable, and DHS/FEMA.

Article XLIV – Disposition of Equipment Acquired Under the Federal Award

For purposes of original or replacement equipment acquired under this award, state subrecipients must follow the disposition requirements in accordance with state laws and procedures.

Article XLV – Office of Homeland Security, Specific

By accepting this award, the subrecipient agrees:

1. To utilize standard resource management concepts, such as typing inventorying, organizing and tracking resources that facilitate the identification, dispatch, deployment and recovery of their resources.

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

2. To coordinate with their stakeholders to examine how they integrate preparedness activities across disciplines, agencies, and levels of government.

3. Equipment means tangible personal property (including information technology systems) having a useful life of more than one year and a per-unit acquisition cost, which equals or exceeds the lesser of the capitalization level established by the non-federal entity for financial statement purposes, or \$1,000. Expenditures for equipment shall be in accordance with the approved budget. The subrecipient shall use and manage equipment in accordance with its procedures as long as the equipment is used for its intended purposes. When original or replacement equipment acquired under this award by the subrecipient is no longer needed for the original project or program or for other activities currently or previously supported by OHS, you must request instructions from OHS to make proper disposition of the equipment pursuant to 2 C.F.R. § 200.313 and the OHS Administrative Guide.

4. Expenditures for supplies and operating expenses shall be in accordance with the approved budget and documentation in the form of paid bills and vouchers shall support each expenditure. Care shall be given to assure that all items purchased directly relate to the specific project objectives for which the contract was approved.

5. For Contractual Services the following general requirements will be followed when subcontracting for work or services contained in this grant award:
 - a. All consultant and contractual services shall be supported by written contracts stating the services to be performed, rate of compensation and length of time over which the services will be provided, which shall not exceed the length of the grant period.
 - b. As described in the OHS Administrative Guide for Homeland Security Grants, a copy of any contractual agreement made as a result of this award must be forwarded to OHS for review or be readily available for review prior to execution of the contract.

6. OHS reserves the right to terminate any contract entered into as a result of this grant award at its sole discretion and without penalty or recourse by giving a thirty (30) day written notice to the subrecipient of the effective date of termination. In the event of termination pursuant to this paragraph, all documents, data, and reports prepared by the subrecipient under the contract shall, at the option of the OHS, become property of the State of Missouri. The subrecipient shall be entitled to receive just and equitable compensation for that work completed prior to the effective date of termination.

7. It is understood and agreed upon that in the event funds from state and/or federal sources are not appropriated and continued at an aggregate level sufficient to cover the contract costs, or in the event of a change in federal or state laws relevant to these costs, the obligations of each party hereunder shall thereupon be terminated immediately upon receipt of written notice.

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

8. To follow the grant program guidelines as stated in the OHS Administrative Guide for Homeland Security Grants, as well as the Information Bulletins released by OHS to provide important updates, clarifications and policy statements related to the State and Local Cybersecurity Grant Program (SLCGP).
9. To follow requirements of the DHS Grant Programs Directorate Information Bulletins.
10. In the event OHS determines that changes are necessary to the award document after an award has been made, including changes to period of performance or Articles of Agreement, the subrecipient will be notified of the changes in writing. Once notification has been made, any subsequent request for funds will indicate subrecipient acceptance of the changes to the award.
11. Prior written approval from OHS is required prior to making any change to the OHS approved budget for this award.
12. To submit Grant Status Reports to OHS by the due dates of July 10 and January 10 throughout the grant period, which must include the status updates of the milestones achieved. Final Status Reports are due to OHS within 45 days after the end of the project period.
13. All items that meet the OHS definition of equipment that are purchased with State and Local Cybersecurity Grant Funds must be tagged "Purchased with U.S. Department of Homeland Security Funds."
14. Projects that involve changes to the natural or built environment require the completion and approval of an Environmental Historic Preservation Screening Form (EHP) prior to initiating any work on the project. Changes to the project after the approval of the EHP requires OHS review and approval. Changes to the project may require the submission and approval of an updated EHP Screening Form. DHS/FEMA is required to consider the potential impacts to natural and cultural resources of all projects funded by DHS/FEMA grant funds, through its EHP Review process, as mandated by the National Environmental Policy Act; National Historic Preservation Act of 1966, as amended; Nation Flood Insurance Program regulation; and, any other applicable laws and Executive Orders.
15. Purchases from a single feasible source must have prior approval from the OHS.
16. **National Incident-Based Reporting System (NIBRS) formerly Uniform Crime Reporting (UCR):** Subrecipients that are a law enforcement agency, assure its agency is in compliance with the state provisions of Section 43.505 RSMo which states each law enforcement agency is required to submit crime incident reports to the department of public safety on forms or in the format prescribed by the department, and submit any other crime incident information which may be required by the department of public safety. Law enforcement agencies will be considered non-compliant if they have not submitted MIBRS reports for three or more months. The subrecipient must remain compliant with section 43.505 RSMo for the duration of the grant period of performance.

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

17. **Vehicle Stops Report:** Subrecipients that are a law enforcement agency, assure its agency is in compliance with the state provisions of Section 590.650.3 RSMo relating to vehicle stop reporting and will remain in full compliance for the duration of the grant period of performance.
18. **Police Use of Force Transparency Act of 2021:** Subrecipients that are a law enforcement agency, assure its agency is in compliance with the state provisions of Section 590.1265 RSMo relating to use of force incidents reporting standards and procedures, and publication of report data, analysis report. The subrecipient must remain compliant with section 590.1265 for the duration of the grant period of performance.
19. **Custodial Interrogations:** Subrecipients that are a law enforcement agency, assure its agency is in compliance with the state provisions of Section 590.700.4 RSMo relating to custodial interrogations and has adopted a written policy to record custodial interrogations of persons suspected of committing or attempting to commit the felony crimes described in subsection 2 of this section.
20. **Intoxication-Related Traffic Offenses:** Subrecipients that are a law enforcement agency, assure its agency is in compliance with the state provisions of Section 590.030 RSMo. The law enforcement agency shall enroll in the state and federal Rap Back programs on or before January 1, 2022 and will continue to remain enrolled. The law enforcement agency shall take all necessary steps to maintain officer enrollment for all officers commissioned with that agency in the Rap Back program. An officer shall submit to being fingerprinted at any law enforcement agency upon commissioning and for as long as the officer is commissioned with that agency.
21. **Rap Back Program Participation:** Subrecipients that are a law enforcement agency, assure its agency is in compliance with the state provisions of Section 43.544 RSMo relating to forwarding intoxication-related offenses and has adopted a written policy to forward arrest information for all intoxication-related traffic offenses to the central repository as required by Section 43.503 RSMo.
22. **Fire Department Registration:** Subrecipients that are a fire protection agency, assure its agency is in compliance with the state provisions of Section 320.271 RSMo relating to fire department registration. All fire protection districts, fire departments, and all volunteer fire protection associations as defined in section 320.300 shall complete and file with the state fire marshal within sixty days after January 1, 2008, and annually thereafter, a fire department form provided by the state fire marshal.
23. Subrecipient is required to complete the Nationwide Cybersecurity Review (NCSR) each year throughout the grant period of performance. The NCSR enables agencies to benchmark and measure progress of improving their cybersecurity posture. The Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent for each recipient and subrecipient should complete the NCSR. If there is no CIO or CISO, the most senior cybersecurity professional should complete the assessment. The NCSR is available at no cost to the user and takes approximately 2-3 hours to complete. The NCSR will be open

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

October 1 and must be completed by each subrecipient and the Completion Certified submitted to the OHS no later than December 31.

24. When purchasing information technology and/or cybersecurity services and equipment with SLCGP funds, please ensure that you have researched critical vulnerabilities, data security, point of origin, overseas manufacturers and supply chain risks pertaining to the product/brand you wish to acquire. In 2020 DHS published the following Data Security Business Policy: https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf. FEMA also has an Authorized Equipment List: <https://www.fema.gov/grants/tools/authorized-equipment-list>. If you still have questions or need additional information call: 573-526-0153.

25. If the subrecipient's cybersecurity posture does not contain the following benchmarks: (1) cybersecurity and/or data security policies, (2) cybersecurity training awareness program, (3) cybersecurity incident response plan, and (4) receive cybersecurity threat intelligence, the subrecipient must achieve these benchmarks during the grant period of performance. The subrecipient will be required to document work towards these benchmarks as part of the Narrative Project Progress component of each Status Report. The OHS has resources available to assist with these benchmarks. If assistance is needed, please contact the OHS Cybersecurity Team by phone at 573-526-0153 or by email at securityintel@mshp.dps.mo.gov.

26. Subrecipients must subscribe to the Missouri Office of Homeland Security (OHS) Cybersecurity Program and participate in information sharing with federal, state, and local agencies. (i.e., Missouri Office of Homeland Security (OHS), Missouri Information Analysis Center (MIAC), St Louis Fusion Center, Kansas City Regional Fusion Center). Entities can subscribe to the OHS Cybersecurity Program by emailing securityintel@mshp.dps.mo.gov with your name, agency/entity, title, desk phone, work phone, and email address.

27. Subrecipients are required to participate in the following free services by CISA:

1. Web Application Scanning is an "internet scanning-as-a-service." This service assess the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.

2. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static, IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLCGP. For more information, visit [CISA's Cyber Hygiene Information Page](#).

28. The subrecipient agency must attend and complete the FY 2022 State and Local Cybersecurity Grant Program (SLCGP) Compliance Workshop. No claims will be reimbursed

AUTHORIZED OFFICIAL INITIALS

GRANT PROGRAM FY 2022 State and Local Cybersecurity Grant Program	SUBRECIPIENT Sedalia Police Department
AWARD NUMBER EMW-2022-CY-00031-NR6	DATE 02/21/2023

SUBAWARD AGREEMENT

ARTICLES OF AGREEMENT

by the OHS until a member of the subrecipient agency has completed the Compliance Workshop.

Article XLVI – Special Conditions

1. Funding for this program is on hold by DHS/FEMA. The subrecipient agency will be contacted by the OHS when this funding hold has been released and project activities can begin.

AUTHORIZED OFFICIAL INITIALS

5. Attached hereto is documentation affirming Placer's enrollment and participation in a federal work authorization program with respect to the employees working in connection with the contracted services.

Further, Affiant saith not.

John E. Sullivan
John E. Sullivan (Nov 15, 2023 15:34 EST)
AFFIANT SIGNATURE

John E. Sullivan
AFFIANT PRINTED NAME

Nov 15, 2023

Subscribed and sworn to before me this _____ day of _____, 20__.

My Commission Expires: _____ Notary Public

(Printed Name)

SOPHOS

Security made simple.

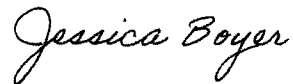
Attn: City of Sedalia, Missouri

Re. Work Authorization Affidavit, Pursuant to 285.530, RSMo

To Whom It May Concern,

This is to confirm that Sophos, Inc. is enrolled and fully participates in a federal work authorization program, namely, E-verify for all employees in the United States, including the everyone hired in the state of Missouri.

Sincerely,

A handwritten signature in cursive script that reads "Jessica Boyer".

Jessica Boyer

Human Resources Department

Sophos, Inc.

SOPHOS END USER TERMS OF USE

THIS SOPHOS END USER TERMS OF USE (“**AGREEMENT**”) BETWEEN CUSTOMER AND SOPHOS LIMITED (“**SOPHOS**”) GOVERNS CUSTOMER’S ACCESS AND USE OF THE SOPHOS PRODUCTS (WHICH INCLUDES SOFTWARE, CLOUD SERVICES AND MANAGED SERVICES) AND IS A LEGALLY BINDING AND ENFORCEABLE CONTRACT.

1. DEFINITIONS

1.1 “Affiliate” means, with respect to each party, an entity that controls, is controlled by, or is under common control with such party. For the purposes of this definition, “control” means the beneficial ownership of more than fifty percent (50%) of the voting power or equity in an entity.

1.2 “Beta Product” means any Product (or portion of a Product) that Sophos identifies as beta, pre-release, early access, or preview, and that is made available to Customer during the Subscription Term but not made generally available for use.

1.3 “Cloud Service” means the hosted software-as-a-service offering or other cloud-enabled feature of the Software.

1.4 “Confidential Information” means any non-public, confidential, or proprietary information of the disclosing party that is clearly marked confidential or reasonably should be assumed to be confidential given the nature of the information and the circumstances of disclosure, including any Beta Products and related Documentation.

1.5 “Customer” means the company or legal entity identified in the applicable Schedule, or in the event there is no applicable Schedule, “Customer” means: (a) the company or legal entity on whose behalf a User accesses or uses the Service, or (b) an individual who accesses or uses the Service on such individual’s own behalf.

1.6 “Customer Content” means all software, data (including Personal Data), non-Sophos or third-party applications, and any other content, communications or material, in any format, and any system, network, or infrastructure provided or made accessible by Customer or User to Sophos in connection with Customer’s access and use of the Product.

1.7 “Documentation” means any technical specifications, online help content, user manuals, or similar materials pertaining to the implementation, operation, access, and use of the Product that are made available by Sophos, as may be revised by Sophos from time to time.

1.8 “Entitlement” means the quantity of units of the Product that Customer has purchased and the associated Subscription Term, each as set forth on the applicable Schedule.

1.9 “Fixes” means any custom or sample code, files, or scripts provided by Sophos as part of the provision of technical support for Hardware or Product that do not form part of Sophos’s standard offerings.

1.10 “Hardware” means any Sophos appliance or physical computing components (whether new or refurbished, and whether or not subject to payment of a fee) on which the Software operates, and any related components or peripherals (including, but not limited to, power cords, fans, power supply modules, drives, carries, ship kits, and rack mount kits).

1.11 “Managed Service” means any managed security services or other associated security services for which the Service Description is published with this Agreement at <https://www.sophos.com/en-us/legal>.

1.12 “Partner” means Sophos authorized reseller, distributor, or other independent third party from which Customer purchases a subscription to the Product.

1.13 “Personal Data” means any information relating to an identified or identifiable individual or that is otherwise defined as “personal data”, “personal information”, or “personally identifiable information” under applicable data protection laws.

1.14 “Product” means Software, Service, Service Software, Trial Product, or Beta Product that Customer is authorized to access and use under the terms of this Agreement (and any data generated by them, excluding Customer Content), including any applicable support and maintenance services, Documentation, and any Fixes.

1.15 “Sanctions and Export Control Laws” means any law, regulation, statute, prohibition, or similar measure applicable to the Product and/or to either party relating to the adoption, application, implementation, and enforcement of economic sanctions, export controls, trade embargoes, or any other restrictive measures, including, but not limited to, those administered and enforced by the European Union, the United Kingdom, and the United States, which shall be considered applicable to the Product.

1.16 “Schedule” means the order confirmation issued by Sophos, or other equivalent documentation, that details Customer’s purchase of a Product and the Entitlement, and may include other access and use details for the Product.

1.17 “Service” means a Managed Service or Cloud Service that Customer is authorized to access and use under the terms of this Agreement.

1.18 “Service Description” means Sophos’s description of a Security Service’s features, including any additional Service-specific terms and requirements, available at <https://www.sophos.com/en-us/legal.aspx>.

1.19 “Service Software” means any Software made available by Sophos for Customer’s use in connection with a Service.

1.20 “Software” means Sophos computer programs including updates, upgrades, firmware, including any software embedded in Hardware, and applicable Documentation.

1.21 “Sophos Materials” means (i) all Sophos proprietary materials, any written or printed summaries, analyses or reports generated in connection with a Product, including written reports that are created for Customer in the course of providing a Service, and (ii) data generated by Sophos in connection with Customer’s use of a Product, including but not limited to, detections, threat data, indicators of compromise, and any contextual data (but excluding Customer Content).

1.22 “Subscription Term” means the term of Customer’s authorized access and use of the Product, as set forth in the applicable Schedule.

1.23 “Third Party Services” has the meaning set forth in Section 3.3 below.

1.24 “Threat Intelligence Data” means any information about malware, threats, actual or attempted security events, including but not limited to their frequency, source, associated code or metadata, general identifiers, attacked sectors, and geographies that: (i) Customer provides to Sophos in connection with this Agreement, or (ii) is collected or discovered by Sophos in connection with Customer’s access and use of the Product, excluding any

information or data that identifies Customer or to the extent that it includes Personal Data. For the avoidance of doubt, Threat Intelligence Data is not Confidential Information of Customer.

1.25 “Trial Product” has the meaning set forth in Section 2.4(a) below.

1.26 “Trial Term” has the meaning set forth in Section 2.4(a) below.

1.27 “Usage Data” means any diagnostic and usage-related information from the use, performance and operation of the Product, including, but not limited to, type of browser, Product features, and systems that are used and/or accessed, and system and Product performance-related data.

1.28 “Use Level” has the meaning set forth in Section 2.2 below.

1.29 “User” means Customer’s and its permitted Affiliates’ employees, contractors, and similar personnel authorized by Customer or its Affiliates to access and use the Product on such entity’s behalf.

2. PRODUCT USE AND RESTRICTIONS

2.1 License and Right to Access and Use. Subject to Customer’s compliance with the terms of this Agreement, Sophos grants Customer a non-exclusive, non-transferable, worldwide license and right to access and use the Product listed in the Schedule during the applicable Subscription Term solely for Customer’s internal information security purposes, except that Customers may use Sophos Factory for Customer’s internal business purposes. Customer may permit its Affiliates and Users to use the Product in accordance with this Agreement, provided that Customer remains fully responsible and liable for their use of the Product and compliance with the terms and conditions of this Agreement. Customer may make a reasonable number of copies of the Software for backup or disaster recovery purposes. Additionally, during the Agreement term, Sophos grants to Customer a limited, non-exclusive license to use such Sophos Materials solely and for Customer’s own internal information security purposes only.

2.2 Use Level. The Entitlement together with the defined Product unit(s) or meter(s) specified in the Licensing Guidelines at <https://www.sophos.com/en-us/legal.aspx> form the applicable Customer access and use level (“**Use Level**”). Customer may access and use the Product in accordance with the applicable Use Level, and may not exceed the Use Level at any time. Customer’s use and access of the Product in excess of its Entitlement may result in degraded, incomplete or failed Service delivery. If Customer wishes to increase its Use Level, it must first purchase the corresponding additional Entitlement. If Customer exceeds its Use Level, Customer will pay any invoice for such excess use issued by Sophos or a Partner in accordance with Section 6.

2.3 Restrictions. Except as specifically permitted in this Agreement, Customer will not (and will not allow an Affiliate, User, or third party to), directly or indirectly: (a) sublicense, resell, rent, lease, distribute, market, commercialize, or otherwise transfer rights to, or usage of, all or any portion of the Product, or provide the Product on a timesharing, service bureau, or other similar basis; (b) modify, copy, adapt, translate, create derivative works of, reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code of, any part of the Product, except when expressly permitted by law and when essential to achieve interoperability of the Software with another software program; (c) remove, alter, or obscure any proprietary rights notices contained in or affixed to the Product; (d) attempt to gain unauthorized access to the Product; (e) attempt to disrupt, degrade, impair, or violate the integrity, security, or performance of the Product, including, without limitation, by executing any form of network monitoring; (f) use the Product to store, transmit, or propagate any viruses, software routines, or other code designed to permit unauthorized access, to disable, erase or otherwise harm software, hardware or data, or to perform any other harmful actions; (g) upload any content to Product that is unlawful, pornographic, obscene,

indecent, harassing, racially or ethnically offensive, harmful, threatening, discriminatory, defamatory, or facilitates or promotes illegal activities; (h) take any action that imposes or may impose an unreasonable or disproportionately large load on Sophos's infrastructure, as determined by Sophos in its sole discretion; (i) disable or circumvent any monitoring or billing mechanism related to the Product; (j) use any feature of Sophos APIs for any purpose other than in the performance of, and in accordance with, this Agreement; or (k) access or use the Product in a manner that violates applicable law or regulation, infringes third party rights, or violates the terms and conditions of this Agreement.

2.4 Trial Products, Beta Products, Free Products and Fixes.

(a) If Sophos permits Customer to conduct a free trial or evaluation of a Product ("**Trial Product**"), Customer may access and use the Trial Product for thirty (30) days, or such other duration specified by Sophos in writing ("**Trial Term**").

(b) From time to time, Sophos may invite Customer to try a Beta Product, for a period specified by Sophos and at no charge, which Customer may accept or decline in Customer's sole discretion. Customer will comply with testing guidelines that Sophos provides in connection with Customer's access and use of a Beta Product and will make reasonable efforts to provide Feedback in accordance with Section 5.3. Sophos may discontinue a Beta Product at any time in its sole discretion and may not make it generally available.

(c) Trial Products and Beta Products are provided for internal testing and evaluation solely for Customer's own internal information security purposes.

(d) Sophos may make certain Products, portions of certain Products, or certain usage tiers available free of charge ("**Free Product**"). Customer's right to access and use Free Product is not guaranteed for any period of time and Sophos reserves the right, in its sole discretion, to: (i) limit or terminate Customer's use of Free Product; or (ii) reduce, change, or deprecate the functionality of Free Product. For Free Product, only community support is available via <https://community.sophos.com>. Sophos may make certain Products available for personal use ("**Home Use License**"). Customer may only use Products made available under Home Use License for their own non-commercial personal use and not for any other purposes. Fixes may only be used in conjunction with the Hardware or Product for which such Fixes were developed.

(e) TRIAL PRODUCTS, BETA PRODUCTS, FREE PRODUCTS, HOME USE LICENSES AND FIXES ARE PROVIDED "AS IS" WITHOUT ANY SUPPORT, INDEMNITY, LIABILITY OR REMEDY OF ANY KIND. TO THE EXTENT ALLOWED BY APPLICABLE LAW, SOPHOS EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY, CONDITION, OR OTHER IMPLIED TERM AS TO MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF TRIAL PRODUCTS, BETA PRODUCTS, FREE PRODUCTS, HOME USE LICENSES OR FIXES.

(f) The terms of this Section 2.4 apply, and prevail over any conflicting terms in this Agreement, with respect to all access to and use of Trial Products, Beta Products, Free Products, Home Use Licenses or Fixes.

2.5 Modifications to Product and Agreement.

2.5.1 Product. Sophos may in its sole discretion modify or update the Product from time to time without materially reducing or degrading its overall functionality.

2.5.2 Agreement.

(a) Sophos may modify the terms of this Agreement from time to time by posting a modified version on <https://www.sophos.com/legal.aspx> or an alternate site Sophos identifies. Unless otherwise noted by Sophos, all modifications will apply to any Entitlements acquired or renewed after the date of modification. If Sophos makes any material change to the Agreement that will become effective upon an earlier date ("**Immediate Modification**"), Sophos will notify Customers: (i) in accordance with Section 11.2 (**Notice**); or (ii) by posting a notice in the Product console.

(b) In the event of an Immediate Modification, except where required by law, regulation, court order, or guidance issued by a government regulator, Customer will have the right to terminate the Agreement within thirty (30) days of the date of Sophos's Immediate Modification notice if Customer objects to such Immediate Modification, and the termination will be effective at the end of the thirty (30) day period. Customer's or a User's continued access and use of the Product following thirty (30) days after the date of the Immediate Modification notice will constitute Customer's acceptance of the Immediate Modification and updated Agreement. If Customer terminates the Agreement as provided in this paragraph, Sophos will provide or authorize a pro rata refund of the fees paid by Customer to Sophos or the Partner, respectively, for the remainder of the applicable Subscription Term. Customer will be responsible for all fees incurred prior to the effective date of termination.

2.6 Support. Sophos will provide the technical support specified in the applicable Schedule or documentation during the Subscription Term. Additional technical support packages may be available for an additional fee. Technical support packages are described at: <https://www.sophos.com/en-us/support/technical-support.aspx>. From time to time, Sophos performs scheduled maintenance to update the servers, software, and other technology that are used to provide the Service and will use commercially reasonable efforts to provide prior notice of such scheduled maintenance. Customer acknowledges that, in certain situations, Sophos may need to perform emergency maintenance of the Service without providing prior notice.

2.7 Open Source. The Product may contain open source software that are made available under applicable open source license agreements. This Agreement does not alter any rights or obligations Customer may have under the applicable open source licenses. Any open source software that is delivered as part of the Product and which may not be removed or used separately from the Product is covered by the warranty, support and indemnification provisions applicable to the Product.

2.8 Hardware. The use of Hardware is governed by this Agreement, as modified by the Sophos Hardware Terms available at <https://sophos.com/legal/hardware-terms>. In the event of any conflict between the Hardware Terms and this Agreement, the Hardware Terms will take precedence.

3. CUSTOMER OBLIGATIONS

3.1 Access and Use. Customer is solely responsible for: (a) accessing and using the Product in accordance with the Documentation; (b) determining the suitability of the Product for Customer's internal information security purposes; (c) configuring the Product appropriately; (d) complying with any regulations and laws (including, without limitation, export, data protection, and privacy laws) applicable to Customer Content and Customer's use of the Product; (e) Customer's and Users' access and use of the Product; (f) all activity occurring under Customer's Product and support accounts, including the rights and privileges Customer grants to Users and any activity undertaken or decision made by Users regarding Product delivery and usage; (g) providing all reasonable information and assistance required for Sophos to deliver the Product, or enable Customer's or Users' access and use of the Product; (h) using reasonable means to protect the account information and access credentials (including passwords and devices, or information used for multi-factor authentication purposes) used by Customer and Users to access the

Product; and (i) promptly notifying Sophos of any unauthorized account use or other suspected security breach, or unauthorized use, copying, or distribution of the Product or Customer Content.

3.2 Accuracy of Information. Customer agrees to provide complete and accurate Customer and User identification information in connection with access to and use of the Product, including but not limited to providing reasonable Customer and User contact details and information upon Sophos's or Partner's request.

3.3 Third Party Services. The Product may enable or require Customer to associate its Product account with, link to, or otherwise access, third parties' websites, platforms, content, products, services, or information ("**Third Party Services**"). Third Party Services are not part of the Product, and Sophos does not control and is not responsible for the Third Party Services. Customer is solely responsible for: (a) obtaining and complying with any terms of access and use of the Third Party Services, including any separate fees or charges imposed by the provider of the Third Party Services; and (b) configuring the Third Party Services appropriately. Sophos disclaims all responsibility and liability arising from or related to Customer's access or use of the Third Party Services, including any impact on Product capabilities as a result of Customer's use of, or reliance upon, the Third Party Services.

3.4 Critical Applications. The Product is not fault tolerant and use of the Product is not recommended in or in association with safety critical applications where the failure of the Products to perform can reasonably be expected to result in death, personal injury, loss of property, or severe physical or environmental damage. Any use contrary to this disclaimer is at Customer's own risk and Sophos is not liable for such use.

4. CUSTOMER CONTENT; PROTECTION OF CUSTOMER CONTENT; CONFIDENTIALITY; USE OF DATA

4.1 Customer Content. Customer is solely responsible for all Customer Content, including but not limited to its accuracy, quality, and legality. Customer represents and warrants that it: (a) has the legal rights to provide Customer Content to Sophos or/and to other users of the Product as applicable; (b) has provided any required notices and has obtained any consents and/or authorizations (including any required from Users) related to its access and use of the Product and the processing of and access to Customer Content by Sophos; and (c) will comply with all applicable laws and regulations for collecting and processing Customer Content, and transferring Customer Content to Sophos. Customer is responsible for taking and maintaining appropriate steps to protect the confidentiality, integrity, and security of Customer Content, including but not limited to: (i) controlling access that Customer provides to Users; and (ii) backing up Customer Content. In some cases, Sophos may make certain Sophos consumer products available to Customer for personal use by users associated with Customer's organization or institution, and in such cases, Customer agrees that Customer is solely responsible for: (1) providing any required notices and (2) obtaining necessary consents and/or authorizations related to the access/use of the consumer products by the users and the processing of and access to users' information by Sophos.

4.2 Use of Customer Content by Sophos. Customer grants Sophos a non-exclusive, worldwide, royalty-free license to access and use the Customer Content to perform its obligations and exercise its rights under this Agreement.

4.3 Protection and Processing of Customer Content by Sophos. Sophos will maintain appropriate administrative, physical, and technical measures designed to protect the security, confidentiality, and integrity of Customer Content processed by Sophos. The Data Processing Addendum ("**DPA**") located at <https://www.sophos.com/en-us/legal/data-processing-addendum.aspx> is incorporated by reference into this Agreement if the provision of Product constitutes any "processing" by Sophos of any "personal data" within the Customer Content, but only to the extent such processing falls within the scope of "Applicable Data Protection Laws" (each term as defined in the DPA). In the event of any conflict between the terms of the DPA and this Agreement, the terms of the DPA will take precedence.

4.4 Content Restrictions. If Customer's access and use of the Product requires Customer to comply with industry-specific data security or data protection obligations, Customer will be solely responsible for such compliance. Customer may not use the Product in a way that would subject Sophos to those industry-specific regulations without obtaining Sophos' prior written agreement.

4.5 Confidentiality.

(a) Each party acknowledges that it and its Affiliates ("**Receiving Party**") may have access to Confidential Information of the other party and its Affiliates ("**Disclosing Party**") in connection with this Agreement. The Receiving Party will use the same degree of care that it uses to protect the confidentiality of its own Confidential Information of like kind (but not less than reasonable care). The Receiving Party agrees to (i) not use any Confidential Information for any purpose other than to perform its obligations and exercise its rights under this Agreement, and (ii) restrict dissemination of Confidential Information only to individuals or third parties with a "need to know" such information and who are under a substantially similar duty of confidentiality. A Receiving Party may disclose the Disclosing Party's Confidential Information in any legal proceeding or as required as a matter of applicable law or regulation (such as in response to a subpoena, warrant, court order, governmental request, or other legal process); provided, however, that to the extent permitted by applicable law, the Receiving Party will (1) promptly notify the Disclosing Party before disclosing the Disclosing Party's Confidential Information; (2) reasonably cooperate with and assist the Disclosing Party, at the Disclosing Party's expense, in any efforts by the Disclosing Party to contest the disclosure; and (3) disclose only that portion of the Disclosing Party's Confidential Information that is legally required to be disclosed. Notwithstanding the foregoing, with prior written notice to Sophos, Customer may disclose Confidential Information when required to disclose Confidential information by court order or other applicable law, such as the Missouri Open Records and Meetings Act. Trade secrets and software shall be considered closed records as governed by the Missouri Open Records and Meetings Act, Chapter 610, RSMo.

(b) Notwithstanding the above, a Disclosing Party's Confidential Information will not include information that: (i) is or becomes a part of the public domain through no act or omission of the Receiving Party; (ii) was in the Receiving Party's lawful possession prior to the disclosure by the Disclosing Party and had not been obtained by the Receiving Party either directly or indirectly from the Disclosing Party; (iii) is lawfully disclosed to the Receiving Party by a third party without restriction on the disclosure; or (iv) is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information.

4.6 Usage Data and Threat Intelligence Data. Sophos may collect, access, use, process, transmit, or store Usage Data and Threat Intelligence Data for: (a) product improvement; (b) research and development purposes; and (c) deriving statistical data using information that is aggregated, anonymized, de-identified, or otherwise rendered not reasonably associated or linked to an identifiable individual or to Customer or Users ("**Statistical Data**"). Sophos retains all intellectual property rights in such Statistical Data. Sophos may share Threat Intelligence Data (including from Customer Content, if it is anonymized, de-identified, or otherwise rendered not reasonably associated or linked to an identifiable individual or Users) for the purposes of promoting awareness of security risks, and anti-spam and security threat research.

5. OWNERSHIP RIGHTS

5.1 Customer Ownership. Except as expressly provided otherwise in this Agreement, as between Sophos and Customer, Customer retains all right, title, and interest in and to Customer Content.

5.2 Sophos Ownership. As between Sophos and Customer, Sophos retains all right, title, and interest, including all intellectual property rights, in and to the Product and Sophos Materials, including all improvements, enhancements,

modifications, derivative works, logos, and trademarks. Sophos reserves all rights in and to the Product that are not expressly granted under this Agreement.

5.3 Feedback. Customer or Users may provide suggestions, enhancement or feature requests, or other feedback to Sophos with respect to the Product (“**Feedback**”). If Customer provides Feedback, Sophos may use the Feedback without restriction and without paying any compensation to Customer, and Customer hereby irrevocably assigns to Sophos all intellectual property rights in and to such Feedback.

6. FEES, PAYMENT AND TAXES

If Customer is purchasing a subscription to the Product from a Partner, all provisions related to fees, taxes, and payment terms will be exclusively between the Partner and Customer. Otherwise, Customer will pay Sophos, or the local Sophos sales Affiliate, the fees for the Product within thirty (30) days of the invoice date (in the currency and via the payment method specified on the invoice), unless otherwise noted in the applicable invoice. If permitted by applicable law, any delay in making payment shall entitle Sophos to charge interest on the overdue payment. All fees are exclusive of value added tax and any other federal, state, municipal, or other governmental taxes, duties, licenses, fees, excises, or tariffs, and Customer is responsible for paying any taxes assessed based on Customer’s purchases under the Agreement.

7. WARRANTIES; DISCLAIMERS; LIMITATION OF LIABILITY

7.1 Warranties. Each party warrants to the other party that it has the requisite authority to enter into this Agreement. Sophos warrants that: (a) for a period of ninety (90) days from the purchase date the Software will perform substantially in accordance with the Documentation; and (b) during the Subscription Term, it will provide the Services using commercially reasonable skill and care, and the Services will materially conform to the corresponding Documentation. Customer’s sole and exclusive remedy for Sophos’s breach of the foregoing warranty is, at Sophos’s option, either (i) repair or replacement of the Product, or (ii) a pro rata refund of the fees paid to Sophos or a Partner for the period in which Sophos was in breach of the foregoing warranty. This warranty is conditioned upon Customer providing Sophos prompt written notice of the Product’s non-conformity, and using the Product in compliance with this Agreement and in accordance with the Documentation. Where Sophos provides a refund of fees paid for Software, Customer must return or destroy all copies of the applicable Software.

7.2 Warranty Disclaimer. EXCEPT AS EXPRESSLY STATED IN SECTION 7.1, TO THE EXTENT ALLOWED BY APPLICABLE LAW, SOPHOS AND ITS THIRD-PARTY LICENSORS AND SUPPLIERS EXPRESSLY DISCLAIM ALL WARRANTIES AND CONDITIONS OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY, CONDITION, OR OTHER IMPLIED TERM AS TO MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THE PRODUCT. SOPHOS MAKES NO WARRANTY OR REPRESENTATION THAT THE PRODUCT: (A) WILL BE UNINTERRUPTED, COMPLETELY SECURE, ERROR-FREE, FAILSAFE, OR FREE OF VIRUSES; (B) WILL MEET CUSTOMER’S BUSINESS REQUIREMENTS OR OPERATE WITH CUSTOMER’S CURRENT SYSTEMS; OR (C) WILL IDENTIFY OR REMEDIATE ALL THREATS OR INDICATORS OF COMPROMISE. SOPHOS IS NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION, OR SECURITY OF THE PRODUCT THAT MAY ARISE FROM CUSTOMER CONTENT, THIRD PARTY SERVICES, OR ANY OTHER SERVICES PROVIDED BY THIRD PARTIES. SOPHOS DISCLAIMS ANY RESPONSIBILITY OR LIABILITY FOR ANY INTERCEPTION OR INTERRUPTION OF ANY COMMUNICATIONS THROUGH THE INTERNET, NETWORKS, OR SYSTEMS OUTSIDE SOPHOS’S CONTROL.

7.3 Limitation of Liability.

IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES, OR ANY LOSS OF REVENUES, BUSINESS, PROFITS (IN EACH CASE WHETHER DIRECT OR INDIRECT), OR DATA LOSS OR CORRUPTION IN CONNECTION WITH THIS AGREEMENT OR THE PRODUCT, EVEN IF THE DAMAGES WERE FORESEEABLE OR A PARTY HAD BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES.

IN NO EVENT WILL THE AGGREGATE LIABILITY OF SOPHOS OR ITS AFFILIATES FOR DIRECT DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE PRODUCT EXCEED THE TOTAL AMOUNT PAID OR PAYABLE BY CUSTOMER TO SOPHOS OR THE PARTNER, AS APPLICABLE, UNDER THIS AGREEMENT DURING THE APPLICABLE SUBSCRIPTION TERM.

THE LIMITATION OF LIABILITY HEREIN WILL NOT APPLY TO LIABILITY ARISING FROM A PARTY'S INFRINGEMENT OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, INDEMNIFICATION OBLIGATIONS, OR THE FRAUD, GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF A PARTY.

THE LIMITATIONS AND EXCLUSIONS OF LIABILITY IN THIS SECTION 7.3 APPLY (A) WHETHER SUCH CLAIMS ARISE UNDER CONTRACT, TORT (INCLUDING NEGLIGENCE), EQUITY, STATUTE, OR OTHERWISE, AND (B) NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY REMEDY. NOTHING IN THIS AGREEMENT LIMITS OR EXCLUDES ANY LIABILITY WHICH CANNOT BE LIMITED OR EXCLUDED UNDER ANY APPLICABLE LAW.

8. INDEMNIFICATION

8.1 Indemnification by Sophos.

(a) Sophos will (i) indemnify, defend, and hold Customer harmless from any third party claim, action, suit, or proceeding alleging that Customer's access and use of the Product in accordance with this Agreement infringes such third party's patent, trademark, or copyright; and (ii) reimburse Customers' reasonable attorney's fees and costs actually incurred and any damages finally awarded against Customer by a court of competent jurisdiction or agreed to by Sophos in a settlement. If a third-party claim is made or appears likely to be made, Sophos, in its sole discretion, may: (1) procure the right for Customer to continue accessing or using the Product under the terms of this Agreement; or (2) modify or replace the Product to be non-infringing without material decrease in functionality. If Sophos, in its sole discretion, determines that neither of the foregoing options is reasonably feasible, Sophos may terminate the Customer's license to or right to use the Product upon written notice to Customer, and provide or authorize a pro rata refund of the fees paid by Customer to Sophos or the Partner, respectively, for the remainder of the applicable Subscription Term. The foregoing shall be Sophos's entire obligation and Customer's exclusive remedy regarding any third-party claim against Customer.

(b) Sophos will have no indemnity obligation for any claim to the extent such claim, in whole or in part, is based on: (i) a modification of the Product by Customer or a third party; (ii) access or use of the Product in a manner that violates the terms and conditions of this Agreement; (iii) technology, designs, instructions, or requirements provided by Customer or a third party on Customer's behalf; (iv) combination, operation, or use of the Product with non-Sophos products, software, services, or business processes, if a claim would not have occurred but for such combination, operation, or use; or (v) Customer Content or Third Party Services.

8.2 Indemnification by Customer. Except if prohibited by law, Customer will indemnify, defend, and hold harmless Sophos, its Affiliates, and their officers, directors, employees, contractors, and agents against any claims, liabilities, and expenses (including court costs and reasonable attorneys' fees) that are incurred as a result of or in connection with: (a) Customer Content, including Customer's failure to follow applicable laws, obtain all necessary consents related to Customer Content, or comply with Section 4.4 (**Content Restrictions**); (b) Customer's access or use of the Product in a manner not expressly permitted by this Agreement; (c) Customer's violation of any third party rights;

(d) Customer's violation of applicable laws or regulations; or (e) any work product created in reliance on the Product and use of such work product by Customer or a third party.

8.3 Indemnification Procedures. The indemnified party ("Indemnitee") will: (a) promptly notify the indemnifying party ("Indemnitor") in writing of any indemnifiable claim; (b) give Indemnitor all reasonable assistance, at Indemnitor's expense; and (c) give Indemnitor sole control of the defense and settlement of the claim. Any settlement of a claim will not include a specific performance obligation other than the obligation to cease using the Product, or an admission of liability by the Indemnitee, without the Indemnitee's consent. The Indemnitee may join in the defense of an indemnifiable claim with counsel of its choice and at its own expense.

9. TERM AND TERMINATION

9.1 Term. This Agreement will remain in effect until the expiration of the applicable Subscription Term or Trial Term, unless earlier terminated pursuant to this Section 9.2.

9.2 Agreement Termination and Service Suspension. Either party may terminate this Agreement and any then-current applicable Schedule if the other party materially breaches its obligations hereunder and does not cure the breach within thirty (30) days after receipt of written notice of the breach. Sophos, in its sole discretion, may terminate the Agreement without liability if Sophos reasonably believes that Customer's or User's access and use of the Product could subject Sophos, its Affiliates or any third party to liability. Sophos may immediately suspend Customer's or User's access and use of the Service, or portions of the Service, if: (a) Sophos believes there is a significant threat to the functionality, security, integrity, or availability of the Service to Customer or to other customers; (b) Customer breaches Section 2.1 (**License and Right to Use**), Section 2.2 (**Use Level**) Section 2.3 (**Restrictions**), Section 6 (**Fees, Payment, and Taxes**), and/or Section 10.1 (**Export Compliance**); or (c) Customer fails to pay the fee to the Partner for the Product, where applicable. When reasonably practicable and lawfully permitted, Sophos will provide Customer with advance notice of any such Service suspension. Sophos will use reasonable efforts to re-establish the Service promptly after it determines that the issue causing the suspension has been resolved. Any Service suspension under this Section shall not excuse Customer's payment obligations under this Agreement.

Either party may terminate this contract for convenience by serving notice of intent to terminate upon the other party by the means specified above. Such notice shall specify the date of termination, but in no event shall either party terminate the contract for convenience upon less than thirty (30) days' notice to the other party; provided that the parties may mutually agree to waive the thirty (30) day requirement to shorten the time for notice of termination, in the event of termination for convenience. Customer acknowledges that if Customer terminates this Agreement for convenience, Customer will not receive any refund of any fees paid.

9.3 Effect of Termination. Upon termination or expiration of this Agreement: (a) all Customer rights under this Agreement relating to the Product will immediately terminate; (b) Customer is no longer authorized to access the Product or Customer's account; and (c) Customer must destroy any copies of the Product within Customer's control. Upon any termination by Customer for Sophos's uncured material breach of the Agreement, Sophos will provide or authorize a pro rata refund of the fees paid by Customer to Sophos or the Partner, respectively, for the remainder of the applicable Subscription Term. Upon any termination by Sophos for Customer's uncured material breach of the Agreement, Customer will pay any unpaid fees covering the remainder of the then-current Subscription Term.

9.4 Customer Content upon Termination. After termination or expiration of this Agreement, Customer agrees that Sophos has no obligation to Customer to retain Customer Content, which may thereafter be permanently deleted

by Sophos. Sophos will protect the confidentiality of Customer Content residing in the Service for as long as such information resides in the Service.

9.5 End-of-Life. Customer's right to use the Product, and any features of the Product, is subject to the end-of-life policy available at <https://www.sophos.com/en-us/content/product-lifecycle.aspx>. Customer acknowledges and agrees that it is Customer's sole responsibility to review the end-of-life policy for each Product.

10. EXPORT CONTROL; COMPLIANCE WITH LAWS

10.1 Export Compliance. Customer is solely responsible for ensuring that the Product is used, accessed, and disclosed in compliance with Sanctions and Export Control Laws. Customer certifies that Customer or Users, or any party that owns or controls Customer or Users, are not (a) ordinarily resident in, located in, or organized under the laws of any country or region subject to economic or financial trade sanctions or trade embargoes imposed, administered, or enforced by the European Union, the United Kingdom, or the United States; (b) an individual or entity on the Consolidated List of Persons, Groups, and Entities Subject to European Union Financial Sanctions; the U.S. Department of the Treasury's List of Specially Designated Nationals and Blocked Persons or Foreign Sanctions Evaders List; the U.S. Department of Commerce's Denied Persons List or Entity List; or any other sanctions or restricted persons lists maintained by the European Union, the United Kingdom, or the United States; or (c) the target or subject of any Sanctions and Export Laws. Customer further certifies that it and Users will not, directly or indirectly, export, re-export, transfer, or otherwise make available (i) the Product, or (ii) any data, information, software programs, and/or materials resulting from the Product (or direct product thereof) to any person described in (a) through (c) or in violation of, or for any purpose prohibited by, Sanctions and Export Control Laws, including for proliferation-related end uses. Customer agrees that Sophos has no obligation to provide the Product where Sophos believes the provision of the Product could violate Sanctions and Export Control Laws. Further details are available at <https://www.sophos.com/en-us/legal/export.aspx>.

10.2 Compliance with Laws. Each party agrees to comply with all laws applicable to the actions and obligations contemplated by this Agreement. Each party warrants that, during the term of this Agreement, neither party nor any of its officers, employees, agents, representatives, contractors, intermediaries, or any other person or entity acting on its behalf has taken or will take any action, directly or indirectly, that contravenes (a) the United Kingdom Bribery Act 2010, (b) the United States Foreign Corrupt Practices Act 1977, or (c) any other applicable anti-bribery laws or regulations anywhere in the world.

11. GENERAL

11.1 Assignment. Customer may not sublicense, assign, or transfer its rights or obligations under this Agreement without Sophos's prior written consent. Sophos may in its sole discretion assign, novate, subcontract, or otherwise transfer any of its rights or obligations hereunder.

11.2 Notice. Sophos may provide Customer with notice (a) if applicable to the Product, by means of a general notice on the Product portal, on the Sophos.com website, or any other website used as part of the Product, and (b) if specific to the Customer, by electronic mail to the e-mail address in Sophos's records. All notices to Sophos concerning this Agreement will be addressed to The Legal Department, Sophos Limited, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, United Kingdom with a copy to legalnotices@sophos.com.

11.3 Waiver & Severability. Failure by either party to enforce any term or condition of this Agreement will not be construed as a waiver of any of its rights under it. If any provision of the Agreement is held to be invalid or

unenforceable, the remaining provisions of the Agreement will remain in force to the fullest extent permitted by law.

11.4 Force Majeure. Except for payment obligations, neither party will be liable to the other for any delay or failure to perform hereunder due to circumstances beyond such party's reasonable control.

11.5 Community Forum. Customer and other Sophos customers may exchange ideas and technical insight related to Sophos offerings in the Sophos Community site at <https://community.sophos.com/>. Sophos does not endorse, warrant, or guarantee any information posted on that site, and Customer alone assumes the risk of using any such information.

11.6 Third Party Flow-down. If the Product is Sophos Central Wireless, the Google Maps / Google Earth Additional Terms of Service (including the Google Privacy Policy) apply to use of the Product. If the Product utilizes the Talos Rules, Cisco Inc. is a third-party beneficiary to this Agreement with regards to Customer's use of the Talos Rules.

11.7 Service Monitoring. Customer acknowledges that Sophos continuously monitors the Service to: (a) track usage and Entitlement, (b) provide support, (c) monitor the performance, integrity, and stability of the Service's infrastructure, (d) prevent or remediate technical issues, and (e) detect and address illegal acts or violations of Section 2.3 (**Restrictions**).

11.8 Audit Rights. To the extent tracking of Customer's Use Level (**Section 2.2**) is not possible, Sophos may audit Customer's use of the Product to verify that Customer's usage complies with the applicable Entitlement, including without limitation through self-certifications, on-site audits and/or audits done using a third party auditor. An audit will be done upon reasonable notice and during normal business hours, but not more often than once each year unless a material discrepancy was identified during the course of a prior review. Customer further agrees to keep accurate records sufficient to certify Customer's compliance with this Agreement, and, upon Sophos's request, Customer will promptly provide the necessary details certifying Customer's aggregate usage of the Product. Sophos will bear the costs of any such audit (other than Customer's costs associated with any self-certification), except where the audit demonstrates that the amount of the underpayment exceeds five percent (5%) of the fees due. In such case, in addition to purchasing appropriate Entitlement and paying for past excess usage, Customer will reimburse Sophos all reasonable and demonstrable costs of the audit.

11.9 United States Government Users; Non-Waiver of Government Immunity.

(a) The Product and Documentation are considered "commercial computer software" and "commercial computer software documentation" for the purposes of FAR 12.212 and DFARS 227.7202, as amended, or equivalent provisions of agencies that are exempt from the FAR or that are U.S. state or local government agencies. Any use, modification, reproduction, release, performance, display, or disclosure of the Product by the U.S. Government and U.S. state and local government agencies will be governed solely by this Agreement, and except as otherwise explicitly stated in this Agreement, all provisions of this Agreement shall apply to the U.S. Government and U.S. state and local government agencies.

(b) If Customer is a federal, state, or other governmental instrumentality, organization, agency, institution, or subdivision, the limitations of liability and Customer's indemnity obligations herein shall apply only in the manner and to the extent permitted by applicable law, and without waiver of Customer's constitutional, statutory, or other immunities, if any.

11.10 Governing Law and Jurisdiction. If the Customer that has purchased access and use of the Product is located in the United States of America, Canada, or Latin America, this Agreement shall be governed by and construed in

accordance with the laws of the State of Delaware, notwithstanding its conflicts of law principles, and all claims arising out of or relating to this Agreement or the Product shall be brought exclusively in the federal or state courts located in the Delaware. The parties agree that the UN Convention on Contracts for the International Sale of Goods (CISG, Vienna, 1980) shall not apply to this Agreement.

11.11 Survival. The following sections, together with any other terms necessary for the interpretation or enforcement of this Agreement, will survive termination or expiration of this Agreement: 1 (**Definitions**), 4.5 (**Confidentiality**) for five (5) years, 4.6 (**Usage Data and Threat Intelligence Data**), 5 (**Ownership Rights**), 6 (**Fees, Payment and Taxes**), 7 (**Warranties; Disclaimers; Limitation of Liability**), 8 (**Indemnification**), 9.3 (**Effect of Termination**), 9.4 (**Customer Content upon Termination**), and 11 (**General**).

11.12 Independent Parties. Sophos and Customer are independent contractors, and nothing in this Agreement will create a partnership, joint venture, agency, franchise, sales representative, or employment relationship between the parties.

11.13 Entire Agreement. If Sophos and Customer have signed a separate written agreement covering access and use of the Product, the terms of such signed agreement will take precedence over any conflicting terms of this Agreement. Otherwise, this Agreement, the Service Description (where applicable), the Schedule, the Licensing Guidelines, and the documents and policies referenced herein constitute the entire agreement between the parties with respect to the Product and supersede all prior or contemporaneous oral or written communications, agreements or representations with respect to the Product. The Service Description is incorporated by reference into this Agreement if Customer's purchase and use of the Service is described in the Service Description. If there are any inconsistencies between the English language version of this Agreement and any translated version, the English language version shall prevail.

11.14 State of Missouri Required Provisions.

Pursuant to Debarment and Suspension regulations imposed by the Federal Government, Sophos agrees to comply with Executive Orders 12549 and 12689, in that a contract award (see 2 CFR 180.220) must not be made to parties listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. Sophos agrees to comply with the above provisions.

Pursuant to the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352) Contractors that apply or bid for an award exceeding \$100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award. Sophos agrees to comply with the above provisions.

Executed by the parties' duly authorized representatives as of the: **Date**)

(the "Effective

SOPHOS LIMITED

CUSTOMER

Signature

Signature

Name (print)

Name (print)

Title (print)

Title (print)

Date

Date

Sophos Managed Detection and Response



MDR

24/7 Threat Detection and Response

Sophos MDR is a fully managed 24/7 service delivered by experts who detect and respond to cyberattacks targeting your computers, servers, networks, cloud workloads, email accounts, and more.

Ransomware and Breach Prevention Services

The need for always-on security operations has become an imperative. However, the complexity of modern operating environments and the velocity of cyberthreats make it increasingly difficult for most organizations to successfully manage detection and response on their own.

With Sophos MDR, our expert team stops advanced human-led attacks. We take action to neutralize threats before they can disrupt your business operations or compromise your sensitive data. Sophos MDR is customizable with different service tiers, and can be delivered via our proprietary technology or using your existing cybersecurity technology investments.

Cybersecurity Delivered as a Service

Enabled by extended detection and response (XDR) capabilities that provide complete security coverage wherever your data reside, Sophos MDR can:

- **Detect more cyberthreats than security tools can identify on their own**
Our tools automatically block 99.98% of threats, which enables our analysts to focus on hunting the most sophisticated attackers that can only be detected and stopped by a highly trained human.
- **Take action on your behalf to stop threats from disrupting your business**
Our analysts detect, investigate, and respond to threats in minutes — whether you need full-scale incident response or help making accurate decisions.
- **Identify the root cause of threats to prevent future incidents**
We proactively take actions and provide recommendations that reduce risk to your organization. Fewer incidents mean less disruption for your IT and security teams, your employees, and your customers.

Compatible with the Cybersecurity Tools You Already Have

We can provide the technology you need from our award-winning portfolio, or our analysts can leverage your existing cybersecurity technologies to detect and respond to threats.

Sophos MDR is compatible with security telemetry from vendors such as Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace, and many others. Telemetry is automatically consolidated, correlated, and prioritized with insights from the Sophos Adaptive Cybersecurity Ecosystem (ACE) and Sophos X-Ops threat intelligence unit.

Highlights

- Stop ransomware and other advanced human-led attacks with a 24/7 team of threat response experts
- Maximize the ROI of your existing cybersecurity technologies
- Let Sophos MDR execute full-scale incident response, work with you to manage security incidents, or deliver detailed threat notifications and guidance
- Improve cyber-insurance coverage eligibility with 24/7 monitoring and endpoint detection and response (EDR) capabilities
- Free up your internal IT and security staff to focus on business enablement

SOPHOS

MDR That Meets You Where You Are

Sophos MDR is customizable with different service tiers and threat response options. Let the Sophos MDR operations team execute full-scale incident response, work with you to manage cyberthreats, or notify your internal security operation teams any time threats are detected. Our team quickly learns the who, what, when, and how of an attack. We can respond to threats in minutes.

Key Capabilities

24/7 Threat Monitoring and Response

We detect and respond to threats before they can compromise your data or cause downtime. Backed by six global security operations centers (SOCs), Sophos MDR provides around-the-clock coverage.

Compatible with Non-Sophos Security Tools

Sophos MDR can integrate telemetry from third-party endpoint, firewall, identity, email, and other security technologies as part of Sophos ACE.

Full-Scale Incident Response

When we identify an active threat, the Sophos MDR operations team can execute an extensive set of response actions on your behalf to remotely disrupt, contain and fully-eliminate the adversary.

Weekly and Monthly Reporting

Sophos Central is your single dashboard for real-time alerts, reporting, and management. Weekly and monthly reports provide insights into security investigations, cyberthreats, and your security posture.

Sophos Adaptive Cybersecurity Ecosystem

Sophos ACE automatically prevents malicious activity and enables us to search for weak signals for threats that require human intervention to detect, investigate, and eliminate.

Expert-Led Threat Hunting

Proactive threat hunts performed by highly-trained analysts uncover and rapidly eliminate more threats than security products can detect on their own. The Sophos MDR operations team can also use third-party vendor telemetry to conduct threat hunts and identify attacker behaviors that evaded detection from deployed toolsets.

Direct Call-in Support

Your team has direct call-in access to our Security Operations Center (SOC) to review potential threats and active incidents. The Sophos MDR operations team is available 24/7/365 and backed by support teams across 26 locations worldwide.

Dedicated Incident Response Lead

We provide you with a Dedicated Incident Response Lead who collaborates with your internal team and external partner(s) as soon as we identify an incident and works with you until the incident is resolved.

Root Cause Analysis

Along with providing proactive recommendations to improve your security posture, we perform root cause analysis to identify the underlying issues that led to an incident. We give you prescriptive guidance to address security weaknesses so they cannot be exploited in the future.

Sophos Account Health Check

We continuously review settings and configurations for endpoints managed by Sophos XDR and make sure they are running at peak levels.

Threat Containment

For organizations that choose not to have Sophos MDR perform full-scale incident response, the Sophos MDR operations team can execute threat containment actions, interrupting the threat and preventing spread. This reduces workload for internal security operations teams and enables them to rapidly execute remediation actions.

Intelligence Briefings: "Sophos MDR ThreatCast"

Delivered by the Sophos MDR operations team, the "Sophos MDR ThreatCast" is a monthly briefing available exclusively to Sophos MDR customers. It provides insights into the latest threat intelligence and security best practices.

Breach Protection Warranty










Included with Sophos MDR Complete one-, two-, and three-year licenses, the warranty covers up to \$1 million in response expenses. There are no warranty tiers, minimum contract terms, or additional purchase requirements.

Sophos Service Tiers

	Sophos Threat Advisor	Sophos MDR	Sophos MDR Complete
24/7 expert-led threat monitoring and response	✓	✓	✓
Compatible with non-Sophos security products	✓	✓	✓
Weekly and monthly reporting	✓	✓	✓
Monthly intelligence briefing: "Sophos MDR ThreatCast"	✓	✓	✓
Sophos Account Health Check		✓	✓
Expert-led threat hunting		✓	✓
Threat containment: attacks are interrupted, preventing spread <small>Uses full Sophos XDR agent (protection, detection, and response) or Sophos XDR Sensor (detection and response)</small>		✓	✓
Direct call-in support during active incidents		✓	✓
Full-scale incident response: threats are fully eliminated <small>Requires full Sophos XDR agent (protection, detection, and response)</small>			✓
Root cause analysis			✓
Dedicated Incident Response Lead			✓
Breach Protection Warranty <small>Covers up to \$1 million in response expenses</small>			✓








Sophos MDR Included Integrations

Security data from the following sources can be integrated for use by the Sophos MDR operations team at no additional cost. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.

 <p>Sophos XDR</p> <p>The only XDR platform that combines native endpoint, server, firewall, cloud, email, mobile, and Microsoft integrations</p> <p>Integrates with Sophos XDR, Sophos Firewall, Sophos Email, and Sophos Cloud</p>	 <p>Sophos Firewall</p> <p>Monitor and filter incoming and outgoing network traffic to stop advanced threats before they have a chance to cause harm</p> <p>Integrates with Sophos XDR, Sophos Email, and Sophos Cloud</p>	 <p>Microsoft Graph Security</p> <ul style="list-style-type: none"> • Microsoft Defender for Endpoint • Microsoft Defender for Cloud • Microsoft Defender for Cloud Apps • Microsoft Defender for Identity • Identity Protection (Azure AD) • Microsoft Azure Sentinel • Office 365 Security and Compliance Center • Azure Information Protection
 <p>Sophos Endpoint</p> <p>Block advanced threats and detect malicious behaviors—including attackers mimicking legitimate users</p> <p>Integrates with Sophos XDR, Sophos Firewall, Sophos Email, and Sophos Cloud</p>	 <p>Sophos Email</p> <p>Protect your inbox from malware and benefit from advanced AI that stops targeted impersonation and phishing attacks</p> <p>Integrates with Sophos XDR, Sophos Firewall, Sophos Cloud, and Sophos Cloud</p>	 <p>Office 365 Management Activity</p> <p>Provides information on user, admin, system, and policy actions and events from Office 365 and Azure Active Directory logs</p>
 <p>Sophos Cloud</p> <p>Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and Google Cloud Platform</p> <p>Integrates with Sophos XDR, Sophos Firewall, Sophos Email, and Sophos Cloud</p>	 <p>90-Days Data Retention</p> <p>Retains data from all Sophos products and any third-party (non-Sophos) products in the Sophos Data Lake</p>	 <p>Third-Party Endpoint Protection</p> <p>Compatible with...</p> <ul style="list-style-type: none"> • Microsoft • CrowdStrike • SentinelOne • Trend Micro • Trellix • BlackBerry (Cylance) • Symantec (Broadcom) • Havalarebytes

Add-On Integrations

Security data from the following third-party sources can be integrated for use by the Sophos MDR operations team via the purchase of Integration Packs. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.

 Sophos Network Detection and Response Continuously monitor activity inside your network to detect suspicious actions occurring between devices that otherwise are unseen. Learn more about NDR	 Firewall Compatible with... <ul style="list-style-type: none">• Palo Alto Networks• Fortinet• Check Point• Cisco• SonicWall	 Identity Compatible with... <ul style="list-style-type: none">• Okta• Duo• ManageEngine
 Public Cloud Compatible with... <ul style="list-style-type: none">• AWS Security Hub• AWS CloudTrail• Orca Security• Google Cloud Platform Security	 Email Compatible with... <ul style="list-style-type: none">• Proofpoint• Mimecast	 Network Compatible with... <ul style="list-style-type: none">• Darktrace• Tinkst Canary• Skyhigh Security
 1-Year Data Retention		

Sophos MDR Guided Onboarding

For an additional purchase, Sophos MDR Guided Onboarding is available for remote onboarding assistance. The service provides hands-on support for a smooth and efficient deployment, ensures best practice configurations, and delivers training to maximize the value of your MDR service investment. You are provided a dedicated contact from the Sophos Professional Services organization who will be with you through your first 90 days to make sure your implementation is a success. Sophos MDR Guided Onboarding includes:

Day 1 - Implementation

- Project kickoff
- Configure Sophos Central and review of features
- Build and test deployment process
- Configure MDR integrations
- Configure Sophos NDR sensor(s)
- Enterprise-wide deployment

Day 30 - XDR Training

- Learn to think and act like a SOC
- Understand how to hunt for indicators of compromise
- Gain an understanding of using our XDR platform for administrative tasks
- Learn to construct queries for future investigations

Day 90 Security Posture Assessment

- Review current policies for best practice recommendations
- Discuss features that are not in use that could provide additional protection
- Security assessment following NIST framework
- Receive summary report with recommendations from our review

To learn more, visit

sophos.com/uk/en

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Sophos Breach Protection Warranty



MDR

At Sophos, we make your cybersecurity our responsibility. The Sophos Breach Protection Warranty is included at no additional charge with our Sophos MDR Complete subscription. It covers up to \$1 million in response expenses for qualifying customers.

Trusted Protection for Complete Peace of Mind

More organizations trust Sophos for MDR than any other security vendor. With the Sophos Breach Protection Warranty, Sophos MDR Complete customers enjoy the reassurance and peace of mind that comes with having financial coverage if a breach happens.

Included with Sophos MDR Complete

The warranty is included automatically and at no additional charge with new purchases or renewals of Sophos MDR Complete annual subscriptions. There are no warranty tiers, minimum contract terms, or additional purchase requirements.

Up to \$1 Million in Response Expenses

The warranty covers response expenses following a ransomware incident within an environment protected by Sophos MDR Complete:

- Up to \$1,000 per breached machine
- Up to \$1 million in total response expenses
- Up to \$100,000 ransom payment (as part of per-device limit)

Reflecting the reality of today's operating environments, breached machines include endpoints, servers, and Windows and macOS devices. The warranty covers a wide range of incurred expenses, including data breach notification, PR, legal, and compliance.

For full terms and conditions of the warranty, visit www.sophos.com/legal

Clear, Comprehensive Coverage

- Automatically provided - no need to apply
- Included with one-, two-, and three-year subscriptions
- Included with new and renewal license purchases
- Covers endpoints, servers, and devices running Windows and macOS
- No warranty tiers that restrict coverage
- No additional license purchase requirements
- No geographic restrictions*

Warranty Overview

- Up to \$1,000 per breached machine
- Up to \$1 million in total response expenses
- Up to \$100,000 for ransom payment (as part of per-device limit)
- Covers a range of incurred expenses, including data breach notification, PR, legal, and compliance

SOPHOS

FAQs

This FAQ provides additional details about the Sophos Breach Protection Warranty. For full terms and conditions, visit www.sophos.com/legal.

What does the warranty cover?

The warranty covers the irretrievable loss of data caused by a ransomware incident on Windows and MacOS endpoints and servers running the latest version of Sophos Endpoint Protection in an environment protected by Sophos MDR Complete.

How much coverage does the warranty provide?

The warranty covers reimbursement of incurred expenses up to \$1,000 per qualifying device (Windows and macOS). Total coverage per customer is \$1,000 multiplied by the number of impacted qualifying devices up to \$1 million.

Do I have to request the warranty?

No. The warranty is provided automatically and at no additional charge with all new purchases or renewals of Sophos MDR Complete one-, two-, and three-year subscriptions. Customers must accept the warranty terms and conditions to be covered by the policy, this is done during the license purchase process.

Are there any geographic restrictions?

*No. There are no geographic restrictions, other than the exclusion of embargoed countries. The warranty is available to all Sophos MDR Complete customers wherever they are located.

What expenses are reimbursed under the warranty?

For approved claims, Sophos will cover a broad range of incurred expenses, including legal consultation fees, notification of impacted individuals, ransom payments, and regulatory penalties.

Are there security posture requirements to qualify for response expenses?

Yes. Customers must maintain a strong cybersecurity posture, which involves (but is not limited to):

- Keeping devices, applications, and OS patched and up to date
- Maintaining up-to-date and properly installed and configured Sophos Endpoint Protection across all eligible devices
- Maintaining MFA authentication for RDP use

Is there a minimum claim value?

Yes. The minimum claim is \$5,000.

Can I purchase the warranty separately?

No. It is only available with the purchase or renewal of a Sophos MDR Complete one-, two-, or three-year subscription.

Who underwrites the warranty?

Sophos underwrites the warranty directly, demonstrating our confidence in the quality of protection we deliver.

Sophos MDR

Managed Detection and Response That Meets You Where You Are

Sophos MDR is a fully managed service delivered by security experts who detect and respond to cyberattacks targeting your computers, servers, networks, cloud workloads, email accounts, and more. It is customizable with different service tiers and can be delivered via our proprietary technology or using your existing cybersecurity technology. We work with:

- Sophos' award-winning solutions, including endpoint, firewall, cloud, and email protection
- Products from third-party vendors such as Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace, and many others
- Any combination of our technology and third-party vendors' technology

Whether you want full-scale incident response or help making accurate security decisions, Sophos MDR provides expert support 24/7/365. To learn more, visit www.sophos.com/mdr or speak with a Sophos adviser today.



Compatible with Your Environment

We can use our tools, third-party tools, or any combination of the two



Compatible with Your Needs

Whether you need full-scale incident response or help making more accurate decisions



Compatible with Your Business

Our team has deep experience hunting down threats in every industry



4.8/5 average rating

by 100 reviews | 2022

Gartner Peer Insights™



Top Vendor in the 2022 G2 Grid® for MDR Services serving the midmarket



Our website, content, products, design, offers and so on. All rights reserved. Sophos is a registered trademark of Sophos Limited. All other trademarks are the property of their respective owners. Sophos is not responsible for the content of any external links. Sophos is not responsible for the content of any external links. Sophos is not responsible for the content of any external links. Sophos is not responsible for the content of any external links.



United Kingdom and Worldwide Sales
Tel: +44 (0)1617 671131
Email: sales@sophos.com

North American Sales
Tel: Free 1-888-666-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9106 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62261166
Email: salesasia@sophos.com

© 2022 Sophos Limited. All rights reserved. Sophos is a registered trademark of Sophos Limited. All other trademarks are the property of their respective owners. Sophos is not responsible for the content of any external links. Sophos is not responsible for the content of any external links. Sophos is not responsible for the content of any external links. Sophos is not responsible for the content of any external links.



Cybersecurity as a Service Delivered | Sophos

This Service Description describes Sophos Managed Detection and Response and Sophos Managed Detection and Response Complete (each a “**Service**”). All capitalized terms in this Service Description have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section below.

This Service Description is part of and incorporated into, as applicable: (i) Customer’s or Managed Service Provider’s manually or digitally-signed agreement with Sophos covering the purchase of a Service subscription; (ii) Managed Service Provider’s manually or digitally-signed agreement(s) with Sophos covering its purchase of Offerings of which the Service is a part; or (iii) if no such signed agreement exists, then this Service Description will be governed by the terms of the Sophos End User Terms of Use posted at <https://www.sophos.com/legal> (collectively referred to as the “**Agreement**”). To the extent there is a conflict between the terms and conditions of the Agreement and this Service Description, the terms and conditions of this Service Description will take precedence.

Notwithstanding anything to the contrary in the Agreement, Customer/MSP acknowledges and agrees that: (i) Sophos may modify or update the Service from time to time without materially reducing or degrading its overall functionality; and (ii) Sophos may modify or update this Service Description at any time to accurately reflect the Service being provided, and any updated Service Description will become effective upon posting to <https://www.sophos.com/legal>.

I. DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement, have the meaning given below:

“**Case**” is a Detection or set of Detections that has high severity level and warrants human review. Cases can be (i) generated automatically by policies or analytics applied to telemetry from Managed Endpoints and Third-Party Systems, (ii) identified through Threat Hunting activities, or (iii) manually created at the discretion of the Security Services Team or at the request of the Customer/MSP.

“**Detection**” is a condition where data generated by a Managed Endpoint or Third-Party Systems is identified as an indicator of malicious or suspicious activity.

“**Health**” is the state of configurations and settings for a Managed Endpoint running Sophos Intercept X Advanced with XDR that affect the efficacy of the security of that Managed Endpoint.

“**Health Check**” is the act of reviewing Health to identify configurations and settings that may

impact the efficacy of the security of a Managed Endpoint.

“Incident” is a confirmed compromise or un-authorized access of system(s) that poses an imminent threat to Customer/MSP assets, which includes interactive attackers, data encryption or destruction, and exfiltration.

“Incident Response Lead” is a member of the Sophos Security Services Team who is identified as the primary individual responsible for assisting a Customer/MSP during Incident Response.

“Incident Response” is the technical process performed remotely by the Security Services Team to Investigate, mitigate, and neutralize an Incident.

“Investigation” is the formal process and methods used by the Security Services Team to confirm whether activity in a Case is malicious and requires Threat Response.

“Managed Endpoint(s)” is any physical or virtual endpoint device or a server system where Sophos Intercept X Advanced with XDR or Sophos XDR Sensor is installed, up-to-date, and operational in support of Service delivery.

“MDR Compatible Sophos Products” refers to any Sophos products that send security telemetry and alerts to Sophos Central that can be used in support of Service delivery.

“Response Action” is an interaction with Managed Endpoints to perform Investigation and Threat Response, including but not limited to remote query, host isolation, terminating a process, blocking an IP address, and deleting malicious artifacts. Sophos’s escalation of Cases using Customer’s/MSP’s pre-selected communication preferences shall also be deemed Response Action.

“Security Services Team” is the Sophos team conducting security Investigations, Threat Hunting, Response Actions, and Incident Response.

“Third-Party Systems” are supported non-Sophos systems (e.g., endpoints, servers, firewalls, etc.) which are configured to send security telemetry from Customers’ security tools to the Service using Sophos integrations and integration mechanisms.

“Third-Party Remediation Guidance” refers to guidance provided by Sophos regarding actions that may need to be taken by Customer/MSP on Third-Party Systems or Customer’s security tools during Threat Response, or in order to help mitigate or resolve an Incident.

“Threat Hunting” is the process of proactively and iteratively searching through data originating from Service Software and/or Third-Party Systems using a combination of manual and semi-automated activities to identify signals and indicators of malicious activity that may have bypassed existing prevention and detection controls.

“Threat Response” includes the methods, processes, communications, and Response Actions

utilized by the Security Services Team and the Customer/MSP, as applicable, to contain or disrupt malicious activity.

“Threat Response Mode” is the type of action to be taken (i.e., Collaborate, or Authorize as set forth in Article III, Section 1.2) by the Security Services Team during delivery of the Service as determined by Customer/MSP during onboarding.

Note:

Sophos Intercept X Advanced with XDR is hereinafter referred to as **"Sophos XDR,"** and Sophos XDR Sensor is hereinafter referred to as **"XDR Sensor."**

Where the term Service Software is used within this Service Description, it shall be deemed to mean Sophos XDR and/or XDR Sensor, as the context dictates.

II. TIERS OF SERVICE

There are two tiers of Service available for purchase by Customer/MSP: Managed Detection and Response (**“MDR”**) and Managed Detection and Response Complete (**“MDR Complete”**).

MDR - Includes the activities and benefits described in Article III Section 1. Customers must run Sophos XDR and/or XDR Sensor on Managed Endpoints.

MDR Complete - Includes the activities and benefits described in Article III Sections 1 and 2. Activities and benefits described in Article III Section 2 are only available on Managed Endpoints running Sophos XDR.

III. SCOPE OF SERVICE

The Service consists of the activities described below for the tier purchased by Customer/MSP.

1. The following activities are applicable to both MDR and MDR Complete Service tiers:

1.1 Onboarding. During the onboarding process, the following activities must be performed by Customer/MSP as a precondition to delivery of the Service.

a. Customer/MSP will (i) provide contact information, (ii) determine Customer/MSP communication preferences (i.e., email, phone, Sophos Central portal), and (iii) determine the Threat Response Mode. MSP must act as the contact for any Service to be provided to a Beneficiary of MSP's.

b. MSP is solely responsible for: (i) obtaining any consents or information required from its Beneficiaries in order for Sophos to perform the service, (ii) ensuring that Beneficiaries take all actions required for Customers in this Service Description, and (iii) advising Beneficiaries of the risks and potential impacts of the Service.

c. The Customer, MSP, or Partner will install either Sophos XDR or the XDR Sensor on all Managed

Endpoints to be covered by the Service. Additionally, the Customer, MSP, or Partner will configure all required Third-Party Systems.

1.2. Categories of Threat Response Modes

In accordance with 1.1, the Customer, MSP, or Partner will select the desired Threat Response Mode for the Security Services Teams' interaction with the Customer or MSP when an Investigation warrants Threat Response. Threat Response Mode choices are:

Collaborate: The Security Services Team will conduct Investigations but no Response Actions are taken without Customer/MSP's prior consent or active involvement. However, certain Response Actions such as remote query may be undertaken without Customer consent or involvement. An option exists under Collaborate, which if selected, authorizes the Security Services Team to operate in Authorize mode in the event Sophos does not receive acknowledgment from Customer/MSP after attempting to contact all Customer defined contacts.

Authorize: Security Services Team performs Threat Response independent of Customer/MSP and Customer/MSP is notified of Response Actions taken.

1.3 Sophos Account Health Check. Health Check capabilities are only available on Managed Endpoints running Sophos XDR. Security Services Team will run a Health Check on all applicable Managed Endpoints as part of the onboarding process.

Customer/MSP will be notified of any configurations that could diminish the Customer's/MSP's /Beneficiary's security posture along with the required steps to remediate the issues identified by the Health Check.

Failure of Customer/MSP/Beneficiary to implement Health Check recommendations during onboarding or during subsequent evaluations may result in diminished Service quality.

1.4 Triage, Investigation, and Threat Response. Sophos will conduct the following investigation and analysis activities for Cases originating from Managed Endpoints and Third-Party Systems:

- a. Analysis is conducted to enhance identification, aggregation, and prioritization of Detections, resulting in machine-generated Cases.
- b. Investigations are performed to confirm threats, and Threat Response is performed where appropriate. During the course of Service performance, Security Services Team may use the results of Investigations to filter out expected activity to enhance the visibility of suspicious activities in Customer's environment.
- c. Notification and information about the Case is shared with the Customer/MSP based on Customer's/MSP's pre-selected communication preferences.

1.5. Availability. All monitoring, Investigation, and Response Actions described in Section 1.4 above will be provided on a 24/7/365 basis. Customer will also have direct call-in access to the Security Services Team to review suspected Incidents on a 24/7/365 basis.

1.6 Service Level Targets. The following service level targets are utilized to provide Customers/MSPs with guidelines around timing expectations for Case creation and Response Actions resulting from Investigations but excluding Threat Hunting. These targets only apply to Investigations on Managed Endpoints and Third-Party Systems.

Target time for Case creation	2 minutes from Detection
Target time for initial Response Action	30 minutes from Case creation

1.7 Threat Hunting. Security Services Team will conduct Threat Hunting to proactively search for threats that may have evaded existing detection controls based on threat intelligence and relevant indicators of compromise observed in Incident Response engagements and Investigations. Threat Hunting is limited to data collected from Managed Endpoints and supported Third-Party Systems and will focus on identification of attacker behaviors and tactics. If Threat Hunting reveals indicators of malicious activity, a Case will be created and an Investigation will be performed.

1.8 Threat Response. Threat Response includes threat containment and disruption, and endpoint isolation on Managed Endpoints, and where possible, Sophos may provide Third-Party Remediation Guidance.

1.9 Reporting; Health Monitoring; Notification. Periodically, Sophos will provide the Customer/MSP with: (a) reports relating to Detections, Cases, and Response Actions, and (b) notification of Health issues or significant misconfigurations that can degrade real-time protection, investigation, or the ability to take Response Actions.

1.10 Threat Intelligence Webinar. Sophos will provide Customer with access to the Sophos MDR ThreatCast webinar. During the webinar, Sophos will provide Customers/MSP insight into observed global threat activity, the actions the Security Services Team has taken for such threat activity and discuss the broader threat landscape.

1.11 Remote Access Tools. To support Service delivery, the Security Services Team may utilize Sophos owned or selected remote access tools. to access or make changes to Managed Endpoints and may utilize administrative access to Customer’s/MSP’s Sophos Central environment to view or modify configurations. If Customer/MSP has selected Authorized Threat Response Mode, then such access will not require any additional approval. If Customer/MSP has selected Collaborate Threat Response Mode, Sophos will request the necessary authorization before performing any modifications. All access by the Security Services Team to Managed Endpoints and Sophos Central is recorded and logged.

CUSTOMER/MSP ACKNOWLEDGES AND AGREES THAT CUSTOMER'S AUTHORIZATION FOR SOPHOS TO MAKE ANY CHANGES TO, OR MODIFY CONFIGURATIONS IN, CUSTOMER'S/MSP'S /BENEFICIARY'S ENVIRONMENT COULD RESULT IN INTERRUPTION OR DEGRADATION OF CUSTOMER'S/MSP'S/BENEFICIARY'S SYSTEMS AND INFRASTRUCTURE. CUSTOMER/MSP FURTHER ACKNOWLEDGE THAT FAILURE TO GRANT AUTHORIZATION FOR SUCH CHANGES COULD RESULT IN NEW MALICIOUS ACTIVITY OR THE WORSENING OF EXISTING MALICIOUS ACTIVITY. SOPHOS WILL HAVE NO LIABILITY TO CUSTOMER/MSP FOR ANY DAMAGES ARISING FROM OR RELATED TO SUCH NEW OR WORSENERED MALICIOUS ACTIVITY IF THE CUSTOMER/MSP HAS DENIED SOPHOS'S REQUEST FOR AUTHORIZATION TO MAKE CHANGES OR MODIFICATIONS.

1.12 Translation Services for Customers in Japan Only. Sophos may offer translation services through a third-party service provider(s) to translate all verbal communications between Sophos and Customer ("Translation Services"). The Translation Services are provided at Customer's sole option and for Customer's convenience only. Customer acknowledges and agrees that Sophos is not responsible for the accuracy, completeness, or reliability of the Translation Services provided by such third-party service provider(s), and Sophos is not liable for any issues arising from the Translation Services.

2. The following are applicable only to MDR Complete Service tier.

2.1 Additional Scope and Benefits. MDR Complete consists of everything described in Section 1 above, plus everything listed in this Section 2.

a. Remote Incident Response in the event of a security Incident, which includes the following activities. Incident Response is only available on Managed Endpoints running Sophos XDR prior to the occurrence of the Incident. All Incident Response activities are conducted remotely on Managed Endpoints using remote access tools.

Assignment of a dedicated Incident Response Lead (one assigned per shift) to interface with the Customer.

Perform triage and Investigation to identify the scope and impact of the Incident to support containment.

Analysis of additional data sources and data provided or made available by the Customer.

Response Actions will be taken to neutralize malicious access and stop further damage to compromised assets or data.

Provide remediation guidance where Security Services Team is unable to perform Response Actions and requires Customer involvement.

Incident status reporting and action item tracking.

Proactive recommendations designed to prevent or reduce reoccurrence of the Incident.

b. Direct call-in access to the Security Services Team to review Cases and Incidents.

c. Investigation of Cases originating from other MDR Compatible Sophos Products for which the Customer has a license.

d. Service Level Agreement in accordance with Section 2.2.

e. Warranty for the Service in accordance with the terms available at www.sophos.com/legal/mdr-complete-warranty.

2.2 Service Level Agreement ("SLA"). The SLA refers to the Response Time (defined below) by the Security Services Team and is only applicable to the MDR Complete Service tier. The SLA is only available to Customers that have purchased MDR Complete subscription, and not available to MSPs. For the avoidance of doubt, those Customers that have been migrated from their existing Sophos Managed Threat Response subscription to MDR Complete ("**Existing Customers**") will not be entitled to the SLA until such Customers renew their MDR Complete subscription. For Existing customers, the SLA will apply upon the MDR Complete subscription renewal.

a. Definitions. The following defined terms apply to this Service Level Agreement:

"High Severity Case" means a case Case created from Detections generated automatically by policies or analytics applied to telemetry from Managed Endpoints and/or Third-Party Systems that is determined to be of high or critical severity after review by the Sophos Services Team.

"Response Time" means the elapsed time between the identification of a High Severity Case and the time the Security Services Team initiates: (i) contact to notify Customer of such High Severity Case either via email or phone, or (ii) Response Action for Customers that have selected "Authorize" Threat Response Mode.

b. Service Commitments. Response Time will be within sixty (60) minutes for ninety percent (90%) of High Severity Cases measured on a monthly basis, beginning on: (i) the first day of the Service subscription renewal date for Existing Customers; and (ii) the first day of the fourth month of Sophos's provision of the Service for the net new Customer. If Sophos fails to meet the foregoing Response Time more than three times in any rolling twelve (12) month period, then Sophos shall be deemed to have missed the SLA.

c. Service Credit. In the event Sophos missed the SLA as described above, Customer will be entitled to a credit in the amount of five percent (5%) of the fees paid for the Service during the previous billing cycle, or five thousand dollars (\$5,000) (the "**Service Credit**"), whichever is lesser. Service Credit will be applied towards the subscription fee for the next Service subscription term. If Customer

has earned the Service Credit and allows the subscription to lapse for any period past the prepaid subscription term, then the Service Credit will be forfeited.

d. Service Credit Request Procedure. Customer must request the Service Credit in writing and deliver such requests to SLACreditClaims@sophos.com with "MDR Service Credit" in the subject line within thirty (30) calendar days from the time Customer becomes eligible to receive a Service Credit, and Customer's Service Credit request must be supported with evidence from log or report data. If not requested during this time, the Service Credit will expire and no longer be claimable. Customer will be entitled to claim a Service Credit no more than three (3) times in any calendar year. All Service Credit requests will be subject to verification by Sophos.

e. Exclusions. Sophos shall not be responsible for meeting the SLA in whole or in part due to conditions provided in Article V Section 1 below.

IV. CUSTOMER/MSP RESPONSIBILITIES.

For either of the above tiers of the Service, Customer/MSP acknowledges and agrees that, in addition to the actions required of Customer/MSP in Article II above, Customer/MSP must take the following actions to facilitate and enable delivery of the Service, and Sophos shall have no liability for any degraded, incomplete, or failed Service delivery which may result from Customer/MSP's failure to take the required actions. Sophos reserves the right to suspend Service delivery until such time as Customer/MSP performs the required actions. Failure to complete the required actions after written notice from Sophos (including email notice from the Security Services Team to the Customer/MSP designated contacts) shall constitute a material breach by Customer/MSP of the Agreement.

1. Onboarding. Customer/MSP will perform all required activities during the onboarding process.

2. Installation Requirements. Customer/MSP/Beneficiary must: a) have a valid, active Sophos Central account, b) deploy and configure the applicable Service Software to Managed Endpoints, and c) maintain compliance with all the requirements identified in Health Checks, and d) meet minimum system requirements to install Service Software, e) setup and configure all required Third-Party Systems to enable transmission of all applicable security telemetry to Sophos in a format that is compatible with the Service; and f) run only supported versions of Service Software and/or third-party security tools. Customer/MSP acknowledges and agrees that Service Software must be deployed on at least eighty percent (80%) of licensed volume as this is necessary to provide Security Services Team with sufficient visibility into Customer's/MSP's environment for Service delivery.

3. Remediating Known Threats. Customer/MSP must make reasonable efforts to timely remediate any compromises reported by Sophos or by other third-party technologies that Customer/MSP/Beneficiary utilizes for cybersecurity detection and protection. Sophos will not be responsible or liable for any issues caused by Customer's/MSP's failure to take remediation steps in a

timely manner. Additionally, the Security Services Team has no obligation to notify Customer/MSP or generate new Cases from Detections for which Sophos has already provided recommended remediation steps.

4. Time and Date Settings. Customer/MSP must ensure that all Managed Endpoints have accurate time and date settings. Sophos will not be responsible for errors, issues, and residual risk experienced or incurred by Customer/MSP for Detections generated by Managed Endpoints with inaccurate time and date settings.

5. Customer/MSP Personnel. Customer/MSP must identify an appropriate number of suitably skilled personnel who will work with Sophos during the provision of the Service. Customer/MSP's identified personnel must have the necessary technical and business knowledge and authority to make decisions concerning the Service.

6. Timely Response. Customer/MSP must promptly acknowledge receipt of Sophos communications in writing (via email or other agreed method) and must timely respond to Sophos's requests.

7. Actions Outside the Scope of Service. All activities that are not expressly provided in this Service Description are outside of the scope of the Service. Customer/MSP is solely responsible and liable for: (i) taking any actions that are outside of the scope of the Service (e.g., Sophos's suggestions regarding on-site response; all litigation and e-Discovery support; and collaboration with law enforcement); and (ii) for any actions undertaken by Sophos that are not provided in this Service Description under Customer's/MSP's specific direction. Customer/MSP acknowledge and agree Sophos is not responsible for any security incidents, threats or compromises that occurred or existed prior to Service subscription start date. In addition, Customer/MSP is responsible for neutralizing any Incidents and/or confirmed threats in Third-Party Systems that cannot be resolved by Sophos.

8. Non-Sophos Systems. Customer/MSP acknowledges and agrees that: (i) Sophos is not responsible for any changes made to any non-Sophos systems by their vendors or any party that impact either the integration with Service or Sophos's ability to provide the Service; and (ii) Sophos, at its discretion, may add, remove, and modify supported non-Sophos systems. It is the responsibility of Customer/MSP to check the list of non-Sophos system then currently supported by Sophos. Additionally, Customer/MSP must ensure all Third-Party Systems integrations function and continue to function properly throughout the Term. Customer/MSP must contact Sophos immediately in the event the Third-Party Systems have not been properly configured or if the Third-Party Systems do not support transmission of security telemetry to Sophos, in which case, Sophos will reasonably work with Customer/MSP to enable security telemetry transmission.

9. Actions Taken by Partners. Customer may allow Partners to take certain actions within the scope of the Service on Customer's behalf, in which case Customer is responsible for all actions or

omissions of such Partner. Sophos will not be liable for Partners' actions or omissions.

10. MSP Additional Responsibilities. MSP is solely responsible for: ensuring that any Beneficiary for which MSP performs this Service has agreed to accept all risks described in this Service Description or otherwise inherent in the Service. MSP will indemnify and hold Sophos harmless for any claim brought against Sophos by a Beneficiary if such claim results, in whole or in part, from MSP's failure to fully perform its obligations under this Service Description or the Agreement with respect to the Service.

V. ADDITIONAL TERMS.

1. Service Exclusion. Customer/MSP agrees and acknowledges that Sophos will not be liable or be considered in breach of this Service Description or the Agreement (including any applicable SLA): (i) due to any delay or failure to perform its obligations hereunder as a result of industry or infrastructure wide ransomware, cyberwarfare or other cyberattacks that causes Security Services Team to be unable to provide resources to address an Incident in a timely manner; (ii) due to unforeseen circumstances or to causes beyond Sophos reasonable control including but not limited war, strike, riot, crime, acts of God, or shortage of resources; (iii) due to legal prohibition, including but not limited to, passing of a statute, decree, regulation, or order; (iv) during any period of Service suspension by Sophos in accordance with the terms of the Agreement; (v) if Customer/MSP is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (vi) during any scheduled maintenance windows.

2. Service Capabilities. Customer/MSP agrees and acknowledges while Sophos has implemented commercially reasonable technologies and process as part of the Service, Sophos makes no guarantee that the Service will detect, prevent, or mitigate all Incidents. Customer/MSP agrees not to represent to anyone that Sophos has provided such a guarantee or warranty.

Revision Date: 8 June 2023

Cybersecurity as a Service Delivered | Sophos

Sophos provides this limited warranty (“**Warranty**”), on the terms and conditions outlined herein, for Customers that have a current, fully paid-up subscription for MDR Complete (“**Subscription**”) and have a currently supported version of the Product (as defined below) correctly installed and fully operational on their endpoint(s). Customer hereby agrees to have read, to have understood, and to be bound by this Warranty.

This Warranty is part of the Service Description for Sophos Managed Detection and Response offering (“**MDR Service Description**”) and is subject to the Agreement (as defined in the MDR Service Description). In the case of a conflict between these documents in respect of the Warranty, then the terms of this Warranty shall prevail to the extent of such conflict.

Capitalized terms not defined in this Warranty shall have the meaning given to them in the MDR Service Description or the Agreement, as applicable, but for the purposes of this Warranty, the following definitions shall apply:

“**Breach Incident**” means a confirmed ransomware attack from external sources through malware or a virus that denies, by encryption, Customer’s access to a material portion of its confidential information, files and data located on one or more of its Managed Endpoints and demands a ransom payment for its release or return. For clarification, where individual impacts on multiple endpoints are related to the same underlying malware, virus, threat actor, threat campaign, or series of threat campaigns, the multiple impacts shall be considered one Breach Incident and will be limited to one claim under the Warranty.

“**Healthy Environment**” means Customer’s endpoint environment using a current supported operating system that is free of known malware and/or viruses at the time immediately prior to the Breach Incident, and such environment has an overall health score of 100 as indicated by the Account Health Check in Sophos Central. Notwithstanding the foregoing, a Managed Endpoint shall not cease to be a Healthy Environment if Sophos has instructed Customer in writing to disable a feature or otherwise change a setting in Sophos Central and such guidance is current (i.e. has not been revoked) at the time of the Breach Incident.

“**Product**” means, as applicable, (i) Sophos Intercept X Advanced with XDR and MDR, and/or (ii) Sophos Intercept X Advanced for Server with XDR and MDR and, in each case, with all three components fully installed.

“**Warranty Term**” means the time period in which Customer (i) has a current, fully paid-up Subscription and (ii) runs a currently supported version of the Product correctly installed, configured

and enabled to the recommended settings on all of the Managed Endpoints in compliance with the MDR Service Description, the relevant Documentation and the terms and conditions of this Warranty.

“**Year**” means a year beginning on the start date of the Customer’s Subscription (or renewal in the case of an Existing Customer), or anniversary of such date, as applicable.

A. WARRANTY

Sophos warrants that if, during the Warranty Term, the Customer suffers a Breach Incident on a Healthy Environment that results in the irretrievable loss of Customer’s data, Sophos will pay an amount up to the limits specified in this Warranty in respect of that Breach Incident. All claims are subject to the terms, conditions, limitations, disclaimers and exclusions of this Warranty.

B. WARRANTY CONDITIONS, DISCLAIMERS & EXCLUSIONS

1. GENERAL

1.1 The Warranty is only available for a Customer in respect of its Managed Endpoints. The Warranty does not apply to Managed Service Providers (MSPs) (or customers of MSPs) and is non-transferrable.

1.2 The Warranty is only available to a current subscriber of MDR Complete where the Customer has purchased a Subscription. For the avoidance of doubt, a Customer that was migrated from its existing Managed Threat Response subscription to MDR Complete (“**Existing Customer**”) will not be entitled to the Warranty until such Customer renews its Subscription unless B1.3 applies.

1.3 If, prior to the scheduled renewal date, an Existing Customer (a) increases the Use Level of its Subscription license for MDR Complete by 20% or more of the number of Users or Servers (each as defined in the Licensing Guidelines) comprising its current Subscription, or (b) purchases a: (i) chargeable MDR integration add-on; (ii) Central Data Storage – 1 yr Pack; or (iii) Central Network Detection and Response virtual appliance, for its existing Subscription, then the Warranty will apply to their entire augmented Subscription.

1.4 The Warranty is provided AS IS and may be modified at any time at the sole discretion of Sophos, and only the then current version of the Warranty as published at www.sophos.com/legal/MDR-Complete-Warranty shall apply.

1.5 This Warranty is not intended to and shall not be construed to give any third party any interest or rights (including, without limitation, any third party beneficiary rights) with respect to or in connection with any agreement or provision contained herein or contemplated hereby. Only the Customer has the right to enforce this Warranty.

1.6 THIS WARRANTY MAY BE CANCELLED, SUSPENDED OR REVISED BY SOPHOS

BY REASONABLE WRITTEN NOTICE AT ANY TIME AND AT SOPHOS' SOLE DISCRETION. SUCH NOTICE MAY INCLUDE A POSTING TO SOPHOS.COM OR A BANNER ON THE CENTRAL CONSOLE.

1.7 THIS WARRANTY DOES NOT, AND SHALL NOT BE DEEMED TO PROVIDE A CONTRACT OF INSURANCE UNDER ANY LAWS OR REGULATIONS AND SHALL BE NULL AND VOID IN ANY COUNTRY OR JURISDICTION IN WHICH IT IS DEEMED TO BE A CONTRACT OF INSURANCE OR AN OFFERING OF INSURANCE.

2. REQUIREMENTS & CONDITIONS

The benefits of this Warranty will only be available to an MDR Complete Customer that meets all of the conditions of this Section B.2.

2.1 Customer has the Product correctly installed, configured and enabled on its Managed Endpoints in compliance with the MDR Service Description, relevant Documentation and these terms and conditions.

2.2 Customer has a fully paid-up Subscription for a minimum subscription of 12 months, and that Subscription has not lapsed and/or payment is not pending or subject to any grace/hold period.

2.3 At the time of the Breach Incident the affected Managed Endpoints must:

have been running the currently supported release of the Product, including all updates, patches and bug fixes;

have a Healthy Environment;

be using a current supported operating system on each of its Managed Endpoints from either:

(i) Microsoft Windows <https://learn.microsoft.com/en-us/windows/release-health/supported-versions-windows-client> and <https://learn.microsoft.com/en-us/windows/release-health/windows-server-release-info>, and the Product continues to support the operating system; or

(ii) Apple, in which case either the current macOS release or a prior release is used, and for so long as Apple continues to support and provide updates for it, and the Product continues to support the operating system;

An operating system that is under a period of extended support shall not be considered current, and a claim will not be honored under the Warranty; and

not be in breach/default of any terms of the Agreement (as defined in the MDR Services Description) or of the MDR Services Description.

2.4 Throughout the Warranty Period, Customer must :

not turn off or disable any functionality for the Products that permits the Managed Endpoints to be scanned for malware and viruses;

allow Sophos to conduct an “on demand” scan of the Managed Endpoint at Sophos’ discretion to determine the health of the Managed Endpoints;

routinely backed up its data in accordance with industry best practice; and

provided sufficient training to those accessing its data on basic precautionary steps to be taken to avoid phishing or the inadvertent installation of malware and viruses.

2.5 Any Customer remote management of its endpoints and servers must be securely managed and protected using industry best practices, employing at a minimum: multi-factor authentication (which must be enabled and enforced), and enforcing complex passwords containing alphanumeric and special characters and automatic time-outs.

2.6 Customers that are in a regulated industry (e.g., banking, energy, healthcare) must comply with all laws and regulations applicable to its industry.

2.7 Customer reasonably cooperates with Sophos in the investigation of the Breach Incident and any Warranty claim.

3. DISCLAIMERS/LIMITATIONS

A claim made under this Warranty will be denied by Sophos if any of the following apply:

3.1 A Breach Incident occurs after Sophos reports to, or otherwise notifies, Customer in relation to: (a) an Incident, Detection, Case or Response Action, or (b) (i) a non-Healthy Environment, (ii) gaps in Customer’s system or significant misconfigurations of the Products that could degrade real-time protection, (iii) investigation or the inability of Customer to follow up to take Response Actions, or (iv) matters that are likely to lead to a potential Breach Incident, but Customer fails to remediate any identified issues promptly, as reasonably determined by Sophos, and in accordance with good security practice commensurate with the level of security threat.

3.2 Customer fails to notify Sophos of a Breach Incident by opening an MDR case/ticket via email to mdr-ops@sophos.com and / or by calling the relevant number listed at <https://docs.sophos.com/support/help/en-us/active-threat/mtr/open/index.html> as soon as reasonably practicable, and in any event, within 24 hours of becoming aware of a potential breach occurring.

3.3 Customer fails to state their intent to claim under this Warranty, within 5 days of a Breach Incident, by providing a written request to Sophos at breachclaims@sophos.com to commence the approval process for the claim in conformance with Section D (Filing a Claim) of this Warranty.

3.4 Customer does not complete the form at www.sophos.com/claim within 15 days from the

occurrence of a Breach Incident.

3.4 A review of the Account Health Check in Sophos Central shows that the Customer's Managed Endpoint was not a Healthy Environment at the time of the Breach Incident.

3.5 The Incident Response determined that the Breach Incident occurred because of the following:

Customer failed to install bug fixes, patches and/or updates relating to any security vulnerability issued by a vendor/developer from time-to-time for any application and/or operating system running on the Managed Endpoints within the timeframe for the Common Vulnerability Scoring System (CVSS) outlined below, each such timeframe beginning from the date the fix is made available:

Critical (score 8.5+) within 7 days;

High (score 7-8.5) within 30 days; and

Medium and lower (score < 7.0) within 90 days.

If a reboot of the system or application was required in connection with any of the above, the application/system will not be considered to have fulfilled this requirement unless and until completion of the applicable reboot.

an introduction of an active threat through an unprotected endpoint within the Customer network (i.e., the Breach Incident did not originate from a Managed Endpoint but was introduced from another end point on the Customer network).

the Breach Incident occurred before the Warranty Term.

the Customer failed to identify or remediate issues where the Product was improperly installed on a Managed Endpoint or was not performing in accordance with the Documentation. (It is the Customer's responsibility to identify and remediate issues arising during installation.)

3.6 The Customer fails to provide sufficient evidence of its compliance with its obligations and requirements set forth under this Warranty.

3.7 Customer is requesting that a ransomware payment or reimbursement under the Warranty be paid to any person or entity that: (i) would be a violation of the local laws of the country where the Breach Incident occurred; or (ii) resides in or is subject to economic sanctions administered or enforced by the U.S. Treasury Department Office of Foreign Assets Control (OFAC), including (a) any persons or entities listed on OFAC's Specially Designated Nationals and Blocked Persons (SDN) list, (b) persons or entities otherwise prohibited under relevant U.S. law, or (c) persons or entities prohibited by laws of other countries. Customer must provide to Sophos evidence, to Sophos' reasonable satisfaction, that any ransomware payment to be provided by Sophos shall not violate the above.

4. EXCLUSIONS

The following types of claims are expressly excluded from the Warranty and a payment reimbursement will not be made:

4.1 Any claims related to a Breach Incident occurring within a virtual desktop infrastructure (e.g. Citrix, VMware, and other virtual desktop infrastructure environments).

4.2 A claim made by a Customer where either (i) the data is *not* irretrievable (i.e., Customer can get access to back-up data and is capable of restoring the majority of the deleted or encrypted data with the back-up); or (ii) where the data was not on the Managed Endpoints affected by the Breach Incident.

4.3 A claim for a Breach Incident caused by a third party product and/or service which directly or indirectly causes the malfunction or nonperformance of the Product or the Subscription.

4.4 A claim resulting from a systemic failure of third party software impacting customers on a significant, large scale basis.

4.5 A claim resulting from a systemic failure affecting the Sophos infrastructure.

4.6 A claim related to any Breach Incident that arises out of or is caused by, directly or indirectly, acts of God, including but not limited to earthquakes, hurricanes, tsunamis, natural disasters, wildfires, solar flares, solar winds, etc., acts of war or terrorism, or reasonably believed to be related to state sponsored cyberattacks, civil or military disturbances, nuclear, and interruptions, loss or malfunctions of utilities, communications, or the systemic failures of the same.

4.7 A claim related to a Breach Incident arising directly or indirectly from the intentional or willful misconduct, collusion, or the negligence of the Customer, its Affiliates, or its or their directors, officers, agents, employees, non-employee workers, agents, representatives, contractors or consultants (“**Customer Representatives**”).

4.8 A claim related to a Breach Incident arising as a result of an infection, compromise, malware, virus or other unauthorized access of asset(s) or credentials that attempts to circumvent controls in an effort to compromise an endpoint that was introduced to Customer’s internal systems (which could be an unprotected endpoint within the Customer network or a Managed Endpoint) by a Customer Representative, whether intentionally or unintentionally (e.g. malware or virus testing).

4.9 A claim filed by the Customer is not in good faith or is considered non-meritorious or frivolous, as reasonably determined by Sophos.

C: LIMITS OF REIMBURSEMENT PAYMENT

To initiate a claim under the Warranty, Customer must have anticipated demonstrable out of pocket expenses of at least \$5,000 (US) spent in direct response to a Breach Incident.

Sophos will not be liable to pay more than \$1,000 (US) for the lesser of: (i) each fully paid up license acquired by Customer, or (ii) each breached Managed Endpoint. For the avoidance of doubt, if Customer has purchased 25 licenses for use, the maximum reimbursable claim is limited to \$25,000 (provided that the conditions in Section B.2 are met).

Subject to the limitations set forth in Sections C.1 and C.2 above, Sophos will reimburse Customer for pre-approved actual, documented out of pocket Expenses, not to exceed \$1,000,000 (US) in any Year. Such aggregate limit shall apply regardless of the number of Subscriptions held by the Customer, the number of Managed Endpoints covered, or the number of Breach Incidents which could be reimbursable under this Warranty.

For the purposes of C.3 above “Expenses” shall constitute, and be limited to, any of the following costs that are incurred in order to remediate a Breach Incident: (i) reasonable legal fees; (ii) expenses relating to providing notices to affected individuals; (iii) reasonable costs and expenses for public relations; (iv) fines assessed by a regulatory agency; and (v) payment of a ransom to the party causing the Breach Incident to retrieve encrypted data (subject to Section C.5 below and Customer confirming compliance with Section B.2.6 above). Expenses shall not include any value added tax (or similar taxes), any other federal, state, municipal, or other governmental taxes, duties, licenses, fees, excises, or tariffs incurred by Customer that are recoverable, creditable, or in any other way are not a cost to Customer under applicable laws by any reasonable means or endeavours of Customer.

A claim for a ransomware payment shall be limited to a maximum payment of \$100,000 (US) in any one claim (and remains subject to any further limitation pursuant to the maximum amount payable per affected Managed Endpoint as specified in Section C.2 above).

If a Customer makes multiple purchases of the Product on different orders and/or dates, and/or has multiple Subscriptions, the customer is only entitled to receive reimbursement on 1 claim; not 1 claim per order/Subscription.

Sophos shall have no obligation to make any payments that are prohibited by applicable law.

The payment reimbursements provided by this Warranty is Customer’s sole and exclusive remedy for any claims arising from a Breach Incident. To the maximum extent permitted by applicable law, Sophos and its Affiliates disclaim all other warranties, whether express, implied or statutory or otherwise, including but not limited to, warranties of merchantability and fitness for a particular purpose and warranties against hidden or latent defects. In no event will Sophos, its Affiliates or their respective suppliers be liable (under any theory of liability, whether in contract, statute, tort or otherwise) for any lost profits, lost business opportunities, business interruption, lost data, data restoration, or special, incidental, consequential, or punitive damages, even if such party has been advised of the possibility of such damages or losses or such damages or losses were reasonably foreseeable; and in no event shall Sophos’ liability under or arising from this Warranty exceed the

limits set out above.

IN CASE ANY OF THE LIMITS SET OUT ABOVE ARE DETERMINED TO BE INVALID UNDER APPLICABLE LAW IN ANY COUNTRY OR JURISDICTION, THIS WARRANTY SHALL BE DEEMED NULL AND VOID.

D: FILING A CLAIM

A claim under the Warranty must first be approved in writing by Sophos, including the preapproval of qualified vendor(s) selected to remediate a Breach Incident and the costs to be paid for such services. Sophos reserves the right, at its sole discretion, to exclude the use of a competitor of Sophos.

Customer shall reasonably cooperate with Sophos in the investigation of the Breach Incident and Warranty claim.

Customer will, within 72 hours of a Breach Incident, state their intent to claim under this Warranty by providing a written request to Sophos at breachclaims@sophos.com to commence the approval process for the claim.

Within 15 days from the Breach Incident, Customer must submit full claim details via www.sophos.com/claim. All invoices for costs incurred by Customer must be submitted to Sophos within 2 months of the Breach Incident.

E. GOVERNING LAW & DISPUTES

All disputes arising from or in connection with this Warranty shall be governed by the laws of England and Wales.

Any dispute arising out of or in connection with this Warranty, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration under the London Court of International Arbitration (LCIA) Rules, which Rules are deemed to be incorporated by reference into this clause.

The seat, or legal place, of arbitration shall be London, England. The language to be used in the arbitral proceedings shall be English.

Become A **Participant**

OMNIA[®]

PARTNERS

MASTER INTERGOVERNMENTAL COOPERATIVE PURCHASING AGREEMENT

This Master Intergovernmental Cooperative Purchasing Agreement (this "**Agreement**") is entered into by and between those certain government agencies that execute a Principal Procurement Agency Certificate ("**Principal Procurement Agencies**") with National Intergovernmental Purchasing Alliance Company, a Delaware corporation d/b/a OMNIA Partners, Public Sector, Communities Program Management, LLC, a California limited liability company d/b/a U.S. Communities, and/or NCPA LLC, a Texas limited liability company d/b/a National Cooperative Purchasing Alliance (collectively, "**OMNIA Partners**"), in its capacity as the cooperative administrator, to be appended and made a part hereof and such other agencies ("**Participating Public Agencies**"), as defined in each Master Agreement (as defined below), who register to participate in the cooperative purchasing programs administered by OMNIA Partners and its affiliates and subsidiaries (collectively, the "**OMNIA Partners Parties**") by either registering on the OMNIA Partners website (www.omniapartners.com/publicsector (<https://www.omniapartners.com/publicsector?hsLang=en>) or any successor website), or by executing a copy of this Agreement.

RECITALS

WHEREAS, after a competitive solicitation and selection process by Principal Procurement Agencies, in compliance with their own policies, procedures, rules and regulations, a number of suppliers have entered into "**Master Agreements**" (herein so called) to provide a variety of goods, products and services ("**Products**") to the applicable Principal Procurement Agency and the Participating Public Agencies;

WHEREAS, Master Agreements are made available by Principal Procurement Agencies through the OMNIA Partners Parties and provide that Participating Public Agencies may purchase Products on the same terms, conditions and pricing as the Principal Procurement Agency, subject to any applicable federal and/or local purchasing ordinances and the laws of the State of purchase; and

WHEREAS, in addition to Master Agreements, the OMNIA Partners Parties may from time to time offer Participating Public Agencies the opportunity to acquire Products through other group purchasing agreements.

NOW, THEREFORE, in consideration of the mutual promises contained in this Agreement, and of the mutual benefits to result, the parties hereby agree as follows:

1. Each party will facilitate the cooperative procurement of Products.
2. The Participating Public Agencies shall procure Products in accordance with and subject to the relevant federal, state and local statutes, ordinances, rules and regulations that govern Participating Public Agency's procurement practices. The Participating Public Agencies hereby acknowledge and agree that it is the intent of the parties that all provisions of this Agreement and that Principal Procurement Agencies' participation in the program described herein comply with all applicable laws, including but not limited to the requirements of 42 C.F.R. § 1001.952(j), as may be amended from time to time. The Participating Public Agencies further acknowledge and agree that they are solely responsible for their compliance with all applicable "safe harbor" regulations, including but not limited to any and all obligations to fully and accurately report discounts and incentives.
3. The Participating Public Agency represents and warrants that the Participating Public Agency is not a hospital or other healthcare provider and is not purchasing Products on behalf of a hospital or healthcare provider; provided that the foregoing shall not prohibit Participating Public Agency from furnishing health care services so long as the furnishing of health care services is not in furtherance of a primary purpose of the Participating Public Agency.
4. The cooperative use of Master Agreements shall be in accordance with the terms and conditions of the Master Agreements, except as modification of those terms and conditions is otherwise required by applicable federal, state or local law, policies or procedures.
5. The Principal Procurement Agencies will make available, upon reasonable request, Master Agreement information which may assist in improving the procurement of Products by the Participating Public Agencies.
6. The Participating Public Agency agrees the OMNIA Partners Parties may provide access to group purchasing organization ("**GPO**") agreements directly or indirectly by enrolling the Participating Public Agency in another GPO's purchasing program, provided that the purchase of Products through the OMNIA Partners Parties or any other GPO shall be at the Participating Public Agency's sole discretion.
7. The Participating Public Agencies (each a "**Procuring Party**") that procure Products through any Master Agreement or GPO Product supply agreement (each a "**GPO Contract**") will make timely payments to the distributor, manufacturer or other vendor (collectively, "**Supplier**") for Products received in accordance with the terms and conditions of the Master Agreement or GPO Contract, as applicable. Payment for Products and inspections and acceptance of Products ordered by the Procuring Party shall be the exclusive obligation of such Procuring Party. Disputes between Procuring Party and any Supplier shall be resolved in accordance with the law and venue rules of the State of purchase unless otherwise agreed to by the Procuring Party and Supplier.
8. The Procuring Party shall not use this Agreement as a method for obtaining additional concessions or reduced prices for purchase of similar products or services outside of the Master Agreement. Master Agreements may be structured with not-to-exceed pricing, in which cases the Supplier may offer the Procuring Party and the Procuring Party may accept lower pricing or additional concessions for purchase of Products through a Master Agreement.
9. The Procuring Party shall be responsible for the ordering of Products under this Agreement. A non-procuring party shall not be liable in any fashion for any violation by a Procuring Party, and, to the extent permitted by applicable law, the Procuring Party shall hold non-procuring party harmless from any liability that may arise from the acts or omissions of the Procuring Party.
10. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, THE OMNIA PARTNERS PARTIES

EXPRESSLY DISCLAIM ALL EXPRESS OR IMPLIED REPRESENTATIONS AND WARRANTIES REGARDING ANY PRODUCT, MASTER AGREEMENT AND GPO CONTRACT. THE OMNIA PARTNERS PARTIES SHALL NOT BE LIABLE IN ANY WAY FOR ANY SPECIAL, INCIDENTAL, INDIRECT, CONSEQUENTIAL, EXEMPLARY, PUNITIVE, OR RELIANCE DAMAGES, EVEN IF THE OMNIA PARTNERS PARTIES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, THE PROCURING PARTY ACKNOWLEDGES AND AGREES THAT THE OMNIA PARTNERS PARTIES SHALL HAVE NO LIABILITY FOR ANY ACT OR OMISSION BY A SUPPLIER OR OTHER PARTY UNDER A MASTER AGREEMENT OR GPO CONTRACT.

11. This Agreement shall remain in effect until termination by either party giving thirty (30) days' written notice to the other party. The provisions of Paragraphs 6 - 10 hereof shall survive any such termination.
12. This Agreement shall take effect upon (i) execution of the Principal Procurement Agency Certificate, or (ii) registration on the OMNIA Partners website or the execution of this Agreement by a Participating Public Agency, as applicable.

By checking this box, I indicate that I have read and agree to the Terms and Conditions

By checking this box, I indicate that I have read and understand our [Privacy Notice](#)

(<https://info.omniapartners.com/hubfs/Policies/OMNIA-Partners-Website-Privacy-Notice.pdf?hsLang=en>) and accept and agree to be bound by these [Terms of Use](#) (<https://info.omniapartners.com/hubfs/Policies/OMNIA-Partners-Terms-of-Use.pdf?hsLang=en>)

CONTINUE



TD SYNEX
Public Sector



NCPA Contract #01-97 - Advanced Technology Solutions Aggregator - Terms & Conditions

About NCPA

NCPA (National Cooperative Purchasing Alliance) is a leading national government purchasing cooperative working to reduce the cost of goods and services by leveraging the purchasing power of public agencies in all 50 states. For more information, go to www.ncpa.us.

Who Can Use NCPA's Contracts?

There are over 90,000 agencies nationwide from both the public and nonprofit sectors that are eligible to utilize NCPA's cooperative purchasing contracts. These include, but are not limited to the following agency types:

- School Districts (including K-12, Charter schools, and Private K-12)
- Higher Education (including Universities, Community Colleges, Private Colleges & Technical / Vocational Schools)
- Cities, Counties, and any Local Government
- State Agencies
- Healthcare Organizations
- Church/Religious
- Nonprofit Corporations

State Statutes

This contract is accessible nationally to public agencies whose state laws allow for intergovernmental contract use. Click here to view [your state's laws on cooperative purchasing](#).

Contract Name

TD SYNEX NCPA #01-97 - Advanced Technology Solutions Aggregator

Term

August 1, 2019 thru July 31, 2024 with no additional optional years.

Awarded Manufacturers

NCPA Contract #01-97 covers all vendor product lines available at TD SYNEX. TD SYNEX and manufacturers' standard commercial certifications/authorizations are required for participation, in addition to any requirements specific to Public Sector or this contract.

Freight

All deliveries to NCPA members shall be freight prepaid, FOB Destination for CONUS delivery. For authorized Dealers, all standard commercial freight policies will apply. Possible assistance with freight will be determined on a case by case basis. Additional freight costs may apply for OCONUS delivery, white glove, special and expedited delivery requirements.

<https://www.synnecorp.com/us/govsol/ncpa/>



TD SYNnex

Public Sector



NTE (Not-to-Exceed) Contract Pricing

- 4% Discount from MSRP applicable to all manufacturing lines, (unless noted in Exceptions below)
- 2% Discount from MSRP for the following:
 - Chromebooks, HP Smartbuys, Lenovo TopSeller Products and all other promotionally priced products.
 - Manufacturers: APC, Asus, Avaya, Cisco, Crucial, Google, Global Knowledge Training, Microsoft Software, NEC, Netmotion, Seagate, and F5
- 0% Discount for:
 - Non-Discountable SKUs
- **Services:** Please refer to the Services line card for a complete breakdown of specific costs associated with our services. Please email fieldservices@TDSYNNEX.com with any questions.
- **Dealer is encouraged to offer additional discounts** from the established contract price when possible.

Authorized Dealer Program

TD SYNnex offers a Dealer Program that provides select reseller partners the ability to sell to NCPA members using this contract. The Dealer is authorized to invoice the NCPA member and accept payment on behalf of TD SYNnex, subject to the following requirements:

- Dealer must obtain a quote from TD SYNnex Sales Rep or Team. TD SYNnex NCPA Team will include the NCPA contract NTE price to the quote.
- End-user pricing can NOT exceed the NCPA Contract Price but can be discounted by the Dealer.
- Dealer must identify all NCPA quotes and orders to TD SYNnex. Quotes can be obtained at NCPA@TDSYNNEX.com.
- Both the End-user and Dealer POs should reference the NCPA Contract number (NCPA 01-97). Dealer is responsible for maintaining a copy of these POs for audit purposes for up to 3 years following the date of that sale.
- Reseller must have a current account in good standing at TD SYNnex and signed Dealer Agreement. To participate, please send request to NCPA@TDSYNNEX.com.
- TD SYNnex and manufacturers' standard commercial certifications/authorizations are required for participation.



TD SYNEX

Public Sector



Reporting

Authorized Dealers must provide a Report of their sales under this contract no later than the 5th day following the end of the preceding month using the template provided. Use the contract sales report portal to download the most recent template and upload your report each month. Reach out to ContractsSupportTeam@TDSYNEX.com for help if you need to correct a submitted report or adjust a recent entry online.

Submit Sales Reports: <https://www.synnecorp.com/us/govsolv/monthly-contract-reporting/>

Contract Fees

Authorized Dealer Is responsible for the payment of the Contract Fee to TD SYNEX. The contract admin fees are due 10 days following the reporting due date. Or due by the 15th of the month following the sales report submission.

**Contract fee: 0.80% or 80 Bps for Commodity Products
2.00% or 200 Bps for Enterprise Products**

- The Contract Fee is calculated off the Dealer's combined monthly sales based on the total pricing charged to the NCPA members. Participating manufacturers are encouraged to provide special pricing that offsets this Contract Fee.
- Payment Method: ACH Payment is preferred, reach out to Contracts@TDSYNEX.com for ACH instructions
- Payment by check is also accepted.
 - Mail to:
TD SYNEX Corporation
c/o Public Sector Contracts NCPA SCM5551293
39 Pelham Ridge Drive
Greenville, SC 29615

Marketing

There are no restrictions in the marketing of this contract directly to the cooperative membership. The NCPA Program Office can assist TD SYNEX and our participating Dealers with their marketing efforts, training and attendance at industry events and TD SYNEX Public Sector shows.

NCPA has provided a membership list to assist our dealer organization in the marketing of this contract. TD SYNEX will send all Authorized Resellers the membership list on a monthly basis. Reach out to NCPA@TDSYNEX.com for contact information.

NCPA Contact below available to connect w/ end-user/agencies, qualify them & answer any questions.

Jonathan Applegate, Director, Operations

Tele: 832-477-3475

E-Mail: japplegate@ncpa.us



TD SYNnex
Public Sector



Public Sector Contract Specialists, Reseller Support

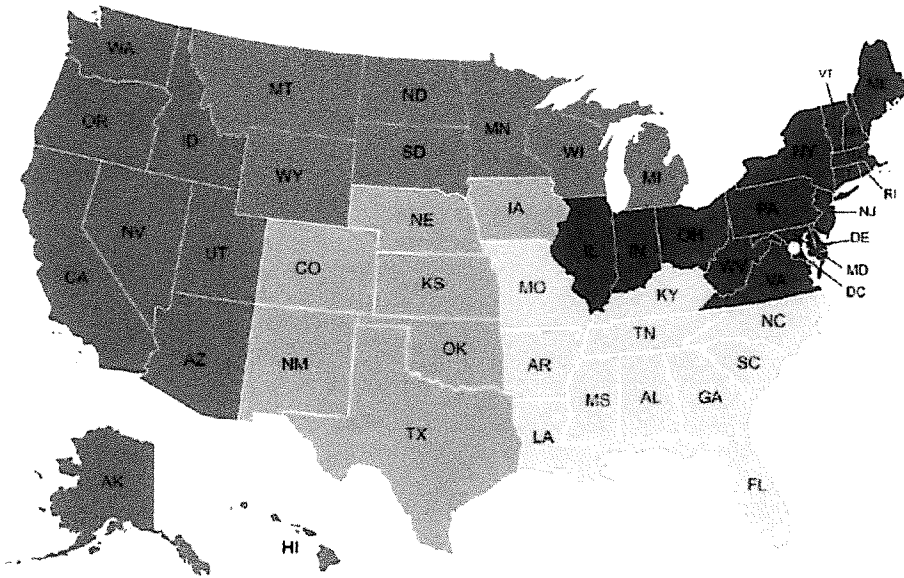


TD SYNnex

Public Sector Specialist Coverage Map



TD SYNnex



Legend

Please select the BD rep based on the state in which your HQ is located.

Nicholas Coperine

Sr. Public Sector Specialist, South East
(914) 618-1524 | Nicholas.Coperine@tdsynnex.com

Caroline Tremblay

Public Sector Specialist, North Central
(864) 293-3406 | Caroline.Tremblay@tdsynnex.com

Lisa McElroy

Public Sector Specialist, North East
(703) 254-6907 | Lisa.McElroy@tdsynnex.com

Travis Matthews

Public Sector Specialist, South Central
(864) 908-9312 | Travis.Matthews@tdsynnex.com

Ian Nix

Public Sector Specialist, West Coast
(202) 688-9978 | Ian.Nix@tdsynnex.com

Jamie Grimm

Public Sector Business Development, Supervisor
(864) 373-7589 | Jamie.Grimm@tdsynnex.com

Randy Finley

Public Sector Business Development, Director
(864) 349-4390 | Randy.Finley@tdsynnex.com



Region XIV Education Service Center

1850 Highway 351
Abilene, TX 79601-4750
325-675-8600
FAX 325-675-8659

Wednesday, September 1st, 2021

**SYNNEX Corporation
ATTN: Daniel T. Brennan
39 Pelham Ridge Drive
Greenville, SC 29615**

Re: Annual Renewal of NCPA contract #01-97

Dear David:

Region XIV Education Service Center is happy to announce that SYNNEX Corporation has been awarded an annual contract renewal for Advanced Technology Solutions Aggregator based on the proposal submitted to Region XIV ESC.

The contract will expire on July 31st, 2024, completing the fifth year of a possible five-year term. If your company is not in agreement, please contact me immediately.

If you have any questions or concerns, feel free to contact me at 325-675-8600.

Sincerely,

A handwritten signature in cursive script, appearing to read 'Shane', is written in black ink.

**Shane Fields
Region XIV, Executive Director**

**CITY COUNCIL
OF THE CITY OF SEDALIA, MISSOURI**

RESOLUTION NO. _____

**A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF SEDALIA, MISSOURI,
STATING FACTS AND REASONS FOR THE NECESSITY TO AMEND AND INCREASE
THE CITY'S ANNUAL BUDGET FOR FISCAL YEAR 2024.**

WHEREAS, Section 67.010 of the Revised Statutes of Missouri requires each political subdivision of the State of Missouri ("State") to prepare an annual budget and establishes the requirements for that budget; and

WHEREAS, the City of Sedalia, Missouri ("City"), is a city of the third classification created pursuant to Chapter 77, RSMo, and is a political subdivision of the State of Missouri; and

WHEREAS, the City Council of the City adopted and approved the City's annual budget for Fiscal Year 2023 in accordance with the requirements of Section 67.010, RSMo, by Ordinance No. 11535 on March 21, 2022, and

WHEREAS, Sections 67.030 and 67.040 authorize and provide a procedure for the City Council to amend the City's annual budget to increase expenditures in any fund; and

WHEREAS, expenses for City's operations for Fiscal Year 2024 have been higher than budgeted, but do not exceed revenues plus the City's unencumbered balance brought forward from previous years; and

WHEREAS, the City Council of the City desire to state the facts and reasons necessitating an amendment to increase certain expenditures in the Fiscal Year 2024 annual budget.

**NOW THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY
OF SEDALIA, MISSOURI, AS FOLLOWS:**

Section 1. Expenditures from the City's General Fund must be increased by a total of \$35,425 above the amount authorized in the adopted annual budget for Fiscal Year 2024. An amendment to increase said budget is necessary for the following facts and reasons:

A. Harding Street Ground Testing.

Section 2. This Resolution shall take effect immediately upon its execution by the Mayor or otherwise as provided by law.

PASSED by the City Council of the City of Sedalia, Missouri, on November 20, 2023

Presiding Officer of the Council

ATTEST: _____
Jason S. Myers, City Clerk

BILL NO. _____

ORDINANCE NO. _____

**AN ORDINANCE AMENDING THE BUDGET FOR THE FISCAL YEAR 2023-2024
REGARDING HARDING STREET GROUND TESTING.**

**NOW THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE CITY OF
SEDALIA, MISSOURI** as follows:

Section 1. The 2023-2024 fiscal year budget beginning April 1, 2023 and ending March 31, 2024 is hereby amended to modify certain budgeted line items as they appear on the attached schedule and made a part hereof as Exhibit A as if fully set out herein.

Section 2. This ordinance shall be in full force and effect from and after its passage and approval.

Read two times by title, copies of the proposed ordinance having been made available for public inspection prior to the time the bill is under consideration by the Council and passed by the Council of the City of Sedalia, Missouri this 20th day of November 2023.

Presiding Officer of the Council

Approved by the Mayor of said City this 20th day of November 2023.

Andrew L. Dawson, Mayor

ATTEST:

Jason S. Myers
City Clerk

Exhibit A
 City of Sedalia
 FY24 Budget Amendment 11/20/2023 Admin Harding Street Ground Testing

Account / Description	Current Budget	Change	Amended Budget	Comments
-----------------------	----------------	--------	----------------	----------

Expenditures / Uses of Funds				
Capital Expenditures				
15-32-353-41 Other Capital Projects	44,650.00	35,425.00	80,075.00	Harding Street Ground Testing Related to Economic Development
	-			
	-			
	-			

Total Expenditure Change

35,425.00

(35,425.00)

Net Increase (Decrease) in Projected Fund Balance

BILL NO. _____

ORDINANCE NO. _____

AN ORDINANCE APPROVING AND ACCEPTING A QUOTE FOR THE PURCHASE OF AN RC MOWER TO BE UTILIZED BY THE STREET DEPARTMENT.

WHEREAS, The City of Sedalia, Missouri, has received a quote from Red Equipment for the purchase of an RC Mower mower to be utilized by the Street Department, Street Division; and

WHEREAS, under the terms of the quote, the City of Sedalia shall pay the sum and amount of Sixty-Seven Thousand Seven Hundred Sixty-Two Dollars and Fifty Cents (\$67,762.50) to Red Equipment for the purchase of said mower as more fully described in the quote attached to this ordinance and incorporated by reference herein.

NOW THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE CITY OF SEDALIA, MISSOURI, as follows:

Section 1. The Council of the City of Sedalia, Missouri, hereby approves and accepts the quote from Red Equipment in substantively the same form and content as the quote has been proposed.

Section 2. The Mayor or City Administrator are authorized and directed to execute and the City Clerk is hereby authorized and directed to attest and fix the seal of the City of Sedalia, Missouri, on any other documentation, if necessary, in substantively the same form and content as the quote has been proposed.

Section 3. The City Clerk is hereby directed to file in his office a duplicate or copy of the quote and any other subsequent documentation after it has been executed by the parties or their duly authorized representatives.

Section 4. This ordinance shall take effect and be in full force and effect from and after its passage and approval.

Read two times by title, copies of the proposed ordinance having been made available for public inspection prior to the time the bill is under consideration by the Council and passed by the Council of the City of Sedalia, Missouri this 20th of November, 2023.

Presiding Officer of the Council

Approved by the Mayor of said City this 20th of November, 2023.

ATTEST:

Andrew Dawson, Mayor

Jason S. Myers, City Clerk



Let's Cross Paths


City of Sedalia

200 S. Osage

Sedalia, MO 65301

(660) 827-3000 www.sedalia.com

To: Kelvin Shaw, City Administrator
 Jessica Pyle, Finance Director

Through: Chris Davies, Public Works Director 

From: Justin Bray, Operations Manager

Date: November 8, 2023

Subject: Purchase of RC Mower Street Division

The Public Works Department, Street Division, is requesting approval to purchase a RC Mower for \$67,762.50 from Red Equipment, 1150 South Sterling Avenue, Independence, MO 64054. The funds for the purchase would be out of budget line item 20-64-351-00. While the mower was not budgeted in the original FY24 budget Public Works has to date purchased two items out of the FY24 budget under the original budgeted amount and would like to use the remaining funds to purchase this mower.

<u>Item</u>	<u>Budget Amount</u>	<u>Purchase Amount</u>	<u>Savings</u>
Dump Truck	\$225,000.00	\$130,000.00	\$95,000.00
Steel Wheel Roller	\$195,100.00	\$184,500.00	\$10,600.00

The unit is an unmanned slope mower designed to mow steep slopes and difficult terrain safely and efficiently. This remote control unit will allow staff to mow and maintain several City owned properties such as equalization basins, drainage ditches, Springfork Dam, Rail Spur as well as overgrown lots turned over from Code Enforcement violations.



2158 Deerfield Avenue E, Suamico, WI 54173
 (920) 634-2227
 RCMOWERSUSA.COM

QUOTE

BILLING

Bill To Name Red Equipment
 Bill To 1150 South Sterling Avenue
 Independence, MO 64054
 United States
 Contact Name Justin Bray
 Contact Phone • 660-620-5527

SHIPPING

Ship To Name Red Equipment
 Ship To 1150 South Sterling Avenue
 Independence, MO 64054
 Delivery Contact Justin Bray
 Delivery Phone • 660-620-5527

Customer Name City of Sedalia (MO)
 Order Notes Discounts applied are valid if PO is issued on
 12-31-23 or before

FCA Suamico, WI
 Lead Time 4-6 Weeks

Product Code	Product	Sales Price	Quantity	Total Price
226045	R-60 - Tracked 60" Rotary Mower, 38.5hp Kawasaki EFI Engine, 50° Max Slope, HSA	\$66,950.00	1.00	\$66,950.00
401918	4500 LB Winch Kit - Synthetic Rope, Receiver Mounted, Storage Bracket, 1 Year Warranty	\$985.00	1.00	\$985.00
401918-01	4500 LB Winch Installation	\$130.00	1.00	\$130.00
700010	Light Kit - [R-52, R-60]	\$560.00	1.00	\$560.00
700010-01	Light Kit Installation (Includes wiring and mounting)	\$187.50	1.00	\$187.50
790133	Replacement Blade Kits - 6 Blades & Hardware [R-52 & R-60]	\$0.00	2.00	\$0.00
790132	Replacement Belt Kit (All Belts) - [R-60]	\$0.00	2.00	\$0.00
790102	200 Hour Maintenance Kit - [R-60]	\$0.00	1.00	\$0.00
DISCOUNT	Discount	-\$2,000.00	1.00	-\$2,000.00

Subtotal \$66,812.50
 Freight \$950.00
 Tax Due \$0.00
 Total \$67,762.50

Prepared By Bill Tharrington
 Phone (515) 520-9599
 Email btharrington@rcmowersusa.com

Quote Number 00001328
 Created Date 11/1/2023

LOVE IT OR LEAVE IT

Our 30-day buy-back guarantee provides you peace-of-mind in case you change yours. This quote is valid for 60 days.



November 2, 2023

RE: RC Mowers – Single Source

To Whom it May Concern:

Thank you for your interest in RC Mowers. Our products are designed to mow steep slopes and difficult terrain safely and efficiently, solving age-old grounds maintenance problems with a high-tech and innovative solution.

Our products are unique from others in the slope mowing industry in that:

- ▶ Our products are designed, built and supported right here in the USA.
- ▶ We offer a 30-day money back guarantee. If for any reason you are not satisfied with the product, we will buy it back – no questions asked.
- ▶ We offer a 72-hour parts shipping guarantee. If the parts you order are not shipped from our factory within 72 hours of placing the order, they are free.

RC Mowers holds US Patent numbers D898,778 S, US D898,779 S, and US D898,780.

RC Mowers has patents pending for the following:

- Automatically adjusting settings based on slope angle
- Automatic warnings and shutdown based on slope angles
- Safety interlock for PTO and speed switches
- Automatic safety timeout mode (Enable button feature)
- Automatic adjustment of drive speed based on PTO settings

Please note that Red Equipment is the sole authorized dealer for RC Mowers equipment in the Kansas and Missouri region.

Should you have any questions, please feel free to reach out to us.

Sincerely,

Cori Triest

[Executive Administrator, Sales]

RCMOWERSUSA.COM

906-241-0780 direct

920-634-2227 office

**CITY COUNCIL
OF THE CITY OF SEDALIA, MISSOURI**

RESOLUTION NO. _____

**A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF SEDALIA, MISSOURI,
STATING FACTS AND REASONS FOR THE NECESSITY TO AMEND AND INCREASE
THE CITY'S ANNUAL BUDGET FOR FISCAL YEAR 2024.**

WHEREAS, Section 67.010 of the Revised Statutes of Missouri requires each political subdivision of the State of Missouri ("State") to prepare an annual budget and establishes the requirements for that budget; and

WHEREAS, the City of Sedalia, Missouri ("City"), is a city of the third classification created pursuant to Chapter 77, RSMo, and is a political subdivision of the State of Missouri; and

WHEREAS, the City Council of the City adopted and approved the City's annual budget for Fiscal Year 2023 in accordance with the requirements of Section 67.010, RSMo, by Ordinance No. 11535 on March 21, 2022, and

WHEREAS, Sections 67.030 and 67.040 authorize and provide a procedure for the City Council to amend the City's annual budget to increase expenditures in any fund; and

WHEREAS, expenses for City's operations for Fiscal Year 2024 have been higher than budgeted, but do not exceed revenues plus the City's unencumbered balance brought forward from previous years; and

WHEREAS, the City Council of the City desire to state the facts and reasons necessitating an amendment to increase certain expenditures in the Fiscal Year 2024 annual budget.

NOW THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF SEDALIA, MISSOURI, AS FOLLOWS:

Section 1. Expenditures from the City's Water Fund must be increased by a total of \$67,000 above the amount authorized in the adopted annual budget for Fiscal Year 2024. An amendment to increase said budget is necessary for the following facts and reasons:

- A. Purchase two trucks due to addition of staff members.

Section 2. This Resolution shall take effect immediately upon its execution by the Mayor or otherwise as provided by law.

PASSED by the City Council of the City of Sedalia, Missouri, on November 20, 2023

Presiding Officer of the Council

ATTEST: _____
Jason S. Myers, City Clerk

BILL NO. _____

ORDINANCE NO. _____

**AN ORDINANCE AMENDING THE BUDGET FOR THE FISCAL YEAR 2023-2024
REGARDING WATER DEPARTMENT TRUCK PURCHASES.**

**NOW THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE CITY OF
SEDALIA, MISSOURI** as follows:

Section 1. The 2023-2024 fiscal year budget beginning April 1, 2023 and ending March 31, 2024 is hereby amended to modify certain budgeted line items as they appear on the attached schedule and made a part hereof as Exhibit A as if fully set out herein.

Section 2. This ordinance shall be in full force and effect from and after its passage and approval.

Read two times by title, copies of the proposed ordinance having been made available for public inspection prior to the time the bill is under consideration by the Council and passed by the Council of the City of Sedalia, Missouri this 20th day of November 2023.

Presiding Officer of the Council

Approved by the Mayor of said City this 20th day of November 2023.

Andrew L. Dawson, Mayor

ATTEST:

Jason S. Myers
City Clerk

Exhibit A
 City of Sedalia
 FY24 Budget Amendment 11/20/2023 Water Truck Purchases

Account / Description	Current Budget	Change	Amended Budget	Comments
Revenues / Source of Funds				
Expenditures / Uses of Funds				
62-73-351-00 Water - Capital Expenditures - Equipment	596,634.00	67,000.00	663,634.00	Purchase Two Chevy Trucks
	-	-	-	
	-	-	-	
	-	-	-	
Total Expenditure Change		<u>67,000.00</u>		
		<u>(67,000.00)</u>		Net Increase (Decrease) In Projected Fund Balance



Let's Cross Paths

City of Sedalia

200 S. Osage

Sedalia, MO 65301

(660) 827-3000 www.sedalia.com

To: Kelvin Shaw, City Administrator
Jessica Pyle, Finance Director

Through: Chris Davies, Public Works Director *CD*

From: David Murray, Senior Operations Technician

Date: November 16, 2023

Subject: Budget Amendment to Purchase of Two Chevy 2500 Trucks for Public Works Water Division

The Public Works Department, Water Division, is requesting an increase of \$67,000 in line item 62-73-351-00 to purchase two Chevy 2500 trucks. The Water Division has added two positions (Utility Locator and Service Technician for Lead/Copper Compliance) that will need vehicles not currently in the Division.

The Missouri State Highway Patrol currently has a 2018 Chevrolet 2500 Crew Cab for \$34,000 and a 2018 Chevrolet 2500 Crew Cab for \$33,000. We are requesting the approval for this increase prior to final purchase of the vehicles. They will be inspected to be sure they meet our needs.

From: Diehl, Todd
To: Matthew Wirt
Subject: Truck Info
Date: Thursday, November 16, 2023 10:50:04 AM
Attachments: image001.png

11/16/2023

MISC VEHICLES

P#	YEAR	MAKE	MODEL	MILES	PRICE	COLOR	CONDITION/COMMENTS	STATUS
18225	2018	Chevrolet	Truck	89,228	\$34,000.00	SILVER	2500 4X4 Crew Cab	
18224	2018	Chevrolet	Truck	125,675	\$33,000.00	WHITE	2500 4X4 Crew Cab	

Todd Diehl
Fleet Control Coordinator
Missouri State Highway Patrol
573-526-6147
573-418-3088 – Cell









City of Sedalia
Council Agenda Work Flow

Council Meeting Date:

Agenda Item:

Department:

Department Head:

Legal Review Needed – If So Attorney Assigned:

Documents Required

Date Required

Memo

(To Clerk 10 Business Days Before Council Meeting)

Employee Bio

(To Clerk 3 Business Days Before Council Meeting)

Ordinance

(Clerk Prepare 8 Business Days Before Council Meeting)

Resolution

(Clerk Prepare 8 Business Days Before Council Meeting)

Contract

(Legal Review Completed and to Clerk 10 Business Days Before Council Meeting) (Note Templates Allow Quicker Turn Around)

Hearing Ad

(To Clerk 5 Business Days Before The Ad Has To Run)

Petition

(To Clerk 10 Business Days Before Council Meeting)

Process Completed / Ready For Packet

(City Clerk Verified)

Janeice Dodick

From: Elizabeth Nations <ENations@sedalia.com>
Sent: Thursday, November 16, 2023 2:07 PM
To: Kelvin L. Shaw; Jessica Pyle
Cc: Jason Myers; Janeice Dodick; Thomas Oldham; Chris Davies
Subject: Council Memo-Water Division Truck Purchase
Attachments: Agenda Work Flow-Trucks Water Division.pdf; Council Memo-Budget Amendment Two Trucks Water Division.docx; Truck Info.pdf; PB161042.JPG; PB161043.JPG

Please see attached. If possible Chris would like this added to the Council Agenda for the 20th to insure the trucks are still available.

*Elizabeth Nations
Executive Administrative Assistant
Public Works Department
City of Sedalia
200 S. Osage Avenue
Sedalia, MO 65301
660-827-3000 Ext. 1166
enations@sedalia.com*

BILL NO. _____

ORDINANCE NO. _____

AN ORDINANCE GRANTING A SPECIAL USE PERMIT TO NICHOLAS A. DILTHEY FOR A CAR DEALERSHIP BUSINESS ON PROPERTY LOCATED AT 204 EAST 24TH STREET IN THE CITY OF SEDALIA, MISSOURI.

NOW THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE CITY OF SEDALIA, MISSOURI, AS FOLLOWS:

Section 1. The Planning and Zoning Commission of the City of Sedalia, Missouri, upon the application, hereinafter described of Nicholas A. Dilthey has recommended by a vote of 7 Yes 0-No and one Abstaining with 2 members absent, that his Special Use Permit application be granted for a car dealership business on said location. This recommendation was made after publication of notice on August 17, 2023 in The Sedalia Democrat as required by the ordinances of the City of Sedalia, Missouri and the laws of the State of Missouri, a full public hearing on October 4, 2023 to consider the application, and upon the hearing and examination of the application by the said Planning and Zoning Commission on October 4, 2023 and November 8, 2023.

Section 2. The said real estate mentioned in Section 1 hereof is described as follows:

SEE ATTACHED EXHIBIT A

Section 3. The Council determines that the proposed use is compatible with the surrounding neighborhood and authorizes the applicant to proceed with obtaining necessary licenses and documentations as needed to place said car detail business on said site.

Section 4. This ordinance shall take effect and be in full force from and after its passage by the City Council and approval by the Mayor.

Read two times by title, copies of the proposed ordinance having been made available for public inspection prior to the time the bill is under consideration by the Council and passed by the Council of the City of Sedalia, Missouri this 20th day of November, 2023.

Presiding Officer of the Council

Approved by the Mayor of said City this 20th day of November, 2023.

Andrew L. Dawson, Mayor

Attest:

Jason S. Myers
City Clerk

EXHIBIT A

LEGAL DESCRIPTIONS

204 East 24th:

LOTS TWENTY-TWO (22), TWENTY-THREE (23), TWENTY-FOUR (24) AND TWENTY-FIVE (25) IN LAWNDALE ADDITION, AN ADDITION TO THE CITY OF SEDALIA, PETTIS COUNTY, MISSOURI.

**APPLICATION FOR AN
AMENDMENT TO THE ZONING DISTRICT MAP**

Sedalia City Planning & Zoning Commission
200 S. Osage Avenue
Sedalia, Missouri 65301

Special Use Permit

DO NOT WRITE IN THIS SPACE	
Date of Public Hearing	
Date Submitted	<u>7-21-23</u>
Date Advertised	
Date of Mailing	
Checked By	
Commission Action	
Council Action	

1. Applicant's Name Nicholas A. Dilthey 660-287-6069 *ND*
2. Applicant's Address 204 East 24th Street, Sedalia
3. Telephone Number (Home) (660) ~~473-3555~~ (Business) (660) 826-6907
4. Present Zoning C-1 Requested Zoning C-3 *ND*
5. Legal Description of property requested to be rezoned, with street address or location:
LOTS TWENTY TWO (22), TWENTY THREE (23), TWENTY FOUR (24) AND TWENTY FIVE (25) IN LAWNDALE ADDITION, AN ADDITION TO THE CITY OF SEDALIA, PETTIS COUNTY, MISSOURI.

6. Area of subject property, square feet and/or acres 0.54 acres
7. Present Use of subject property Used Car Dealership
8. Desired use of subject property Used Car Dealership
9. What is the present use of the adjoining properties? North Residential
South Residential East Residential West Residential
10. How can you justify the proposed zoning change? (To answer this question, see Page 1, Item 2)
11. Time schedule for development N/A
12. Is property in a flood plain district? If yes, please indicate applicable FEMA Map applicable zone No Has base flood elevation been established? _____
If yes, please explain how such elevation was determined. _____

13. Public Utilities available at site: Sewer _____ " at _____
Water _____
at _____
Natural Gas _____ " at _____
Electric _____
at _____

14. Exhibits furnished _____
15. *[Signature]* 204 E 24th St
Signature of Applicant Address of Applicant

16. Relationship of applicant to property: Owner Agent _____
17. Other _____
(Explain)



BAKER LEGAL SERVICES

412 South Ohio, Suite D, Sedalia, Missouri 65301
bakerlegalservices@gmail.com—660.287.3098

July 18, 2023

City of Sedalia
Planning & Zoning Commission
200 South Osage Avenue
Sedalia, Missouri 65301

Re: Request for Rezoning
204 East 24th Street

To whom it may concern,

Twilight Motors LLC has operated as a used car dealership at 204 East 24th Street since its formation in January 2019. When it purchased its current lot, it did so with the understanding that it would be permitted to operate a used car dealership at this address. For the next several years, it has in fact operated a used car dealership here without any issue. Twilight Motors first discovered that its lot was not properly zoned when it received a citation in May of this year. I have been hired by Twilight Motors to help address its issues with zoning.

With this letter, please find enclosed a zoning application and payment in the amount of \$350 to process the application. Twilight Motors LLC is currently on a lot zoned as a C-1 district and requests its lot to be rezoned as a C-2 district.

Twilight Motors over the past several years has enriched the City of Sedalia both in the tax revenue it generates and in the service it provides to the local community. For a business to succeed, it must provide a value to its customers over and above the amount it takes from its customers. If I

buy a used car for \$5,000, I am buying this car because I believe the car is worth more to me than the \$5,000 I am giving up for it. A business that takes more from its customers than it provides in value cannot survive for very long. If I find out the car I paid \$5,000 for is only worth \$3,000, then I will feel cheated and will not go back.

By selling used cars, Twilight Motors doesn't just serve its own customers, but the community as a whole. Saving money on a used car allows a person to spend more money elsewhere. Extending the life of vehicles by repairing and reselling the vehicles helps put a downward pressure on the price tag of all vehicles. Conversely, restricting the market for used vehicles by closing down used car dealerships would drive up vehicle prices and would make it harder to buy and sell cars in Sedalia.

Among a segment of our community, the lack of reliable transportation is a significant impediment towards employment and self-sufficiency. It may not be the only reason a person cannot work, but it may be a significant factor in some cases. Our community can only benefit by businesses helping to provide a robust market for used cars.

In requesting a zoning change, Twilight Motors is not proposing to fundamentally change how it conducts its business. The character of the neighborhood and the flow of traffic on the roads should not change in any meaningful way. Changing the zoning of the lot on which Twilight Motors conducts its business will not have any visible impact on the community. Before the zoning change, Twilight Motors operated a used car dealership and after the zoning change it will continue to do so.

Indeed, the character of this neighborhood would only change if this zoning request is denied. A once productive lot will be vacant if Twilight Motors is prohibited from operating its business. Moreover, this property contains a large gravel lot with a small building. It is set up as a car dealership. If Twilight Motor's zoning application is denied, not only would the lot be vacant, but it would require a significant amount of work

to make the property marketable again. Whoever purchases this property would have to change it from a used car lot to some other purpose.

Finally, Twilight Motors is located on a street that hosts a number of other large parking lots and other public accommodations. Twilight Motors is located in between Katy Park and Centennial Park on 24th Street. In between these parks are: New Covenant Baptist Church, Antioch Fellowship, Evangelic Word, Real Life Church, Sedalia Bible Church, Freedom House, Read Memorial Christian Center, Bristol Manor, Loving Arms Assisted Living and the Sedalia Housing Authority. In addition, traffic from the Sedalia Middle School naturally feeds into 24th Street by way of Collins Street.

The impact Twilight Motors may have on the traffic on 24th Street is nominal by comparison.

Thank you for taking the time to review this application. Please do not hesitate to let me know if there is anything you may need from me or my client.

Sincerely,



Daniel Baker

I, Nicholas Dilthey, am the person applying to amend the zoning classification of 204 East 24th Street. I am the owner and operator of Twilight Motors LLC. I have hired Daniel Baker to help me with the zoning application process. Please feel free to discuss any matters concerning the rezoning of this property with him as if you were talking directly with me.



Nicholas Dilthey



City of Sedalia
200 S. Osage
Sedalia, MO 65301
(660)827-3000 www.cityofsedalia.com

September 21, 2023

NOTIFICATION LETTER

To Whom It May Concern:

This is to notify you that a public hearing will be held in the City of Sedalia's Council Chambers of the Municipal Building, 2nd Street & Osage Avenue, Sedalia, Missouri to consider a Special Use Permit for the following purpose and described tract of land:

PURPOSE OF SPECIAL USE PERMIT:
Used Car Dealership

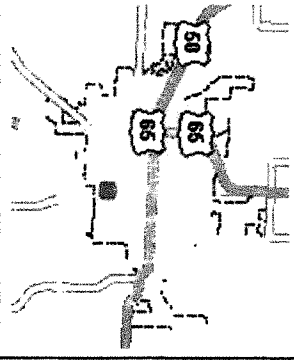
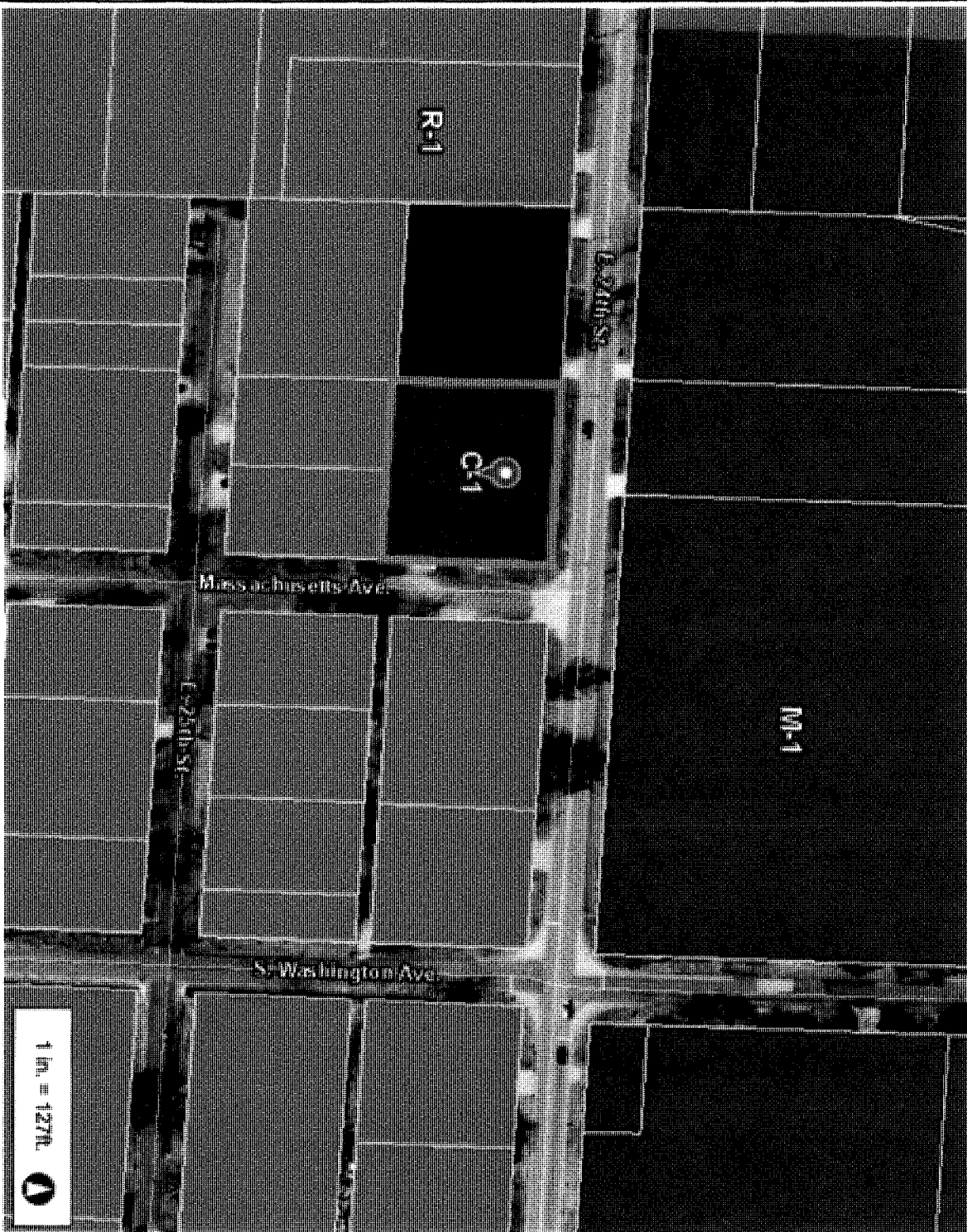
PROPERTY ADDRESS:
204 E 24TH, SEDALIA, MO – LOTS TWENTY TWO (22), TWENTY THREE (23), TWENTY FOUR (24) AND TWENTY FIVE (25) IN LAWNSDALE ADDITION, AN ADDITION TO THE CITY OF SEDALIA, PETTIS COUNTY, MISSOURI.

The public hearing will be held to consider the Special Use Permit for the above-described tract. Hearing will begin at 5:30 pm on Wednesday, October 4, 2023, any interested persons or property owners are invited to attend. For any additional information regarding this special use permit, please contact the undersigned at the Municipal Building.

Respectfully,

John Simmons
Community Development Director
City of Sedalia
jsimmons@sedalia.com
(660) 827-3000 x1115

Sedalia, MO



Legend

- Parcel
- Roads
 - Other
 - State Hwy
 - US Hwy
- Corporate Limit Line
- Zoning
 - C-0
 - C-1
 - C-2
 - C-3
 - M-1
 - M-2
 - PUD
 - Parks and Open Space
 - R-1
 - R-2
 - R-3
 - leftover lines

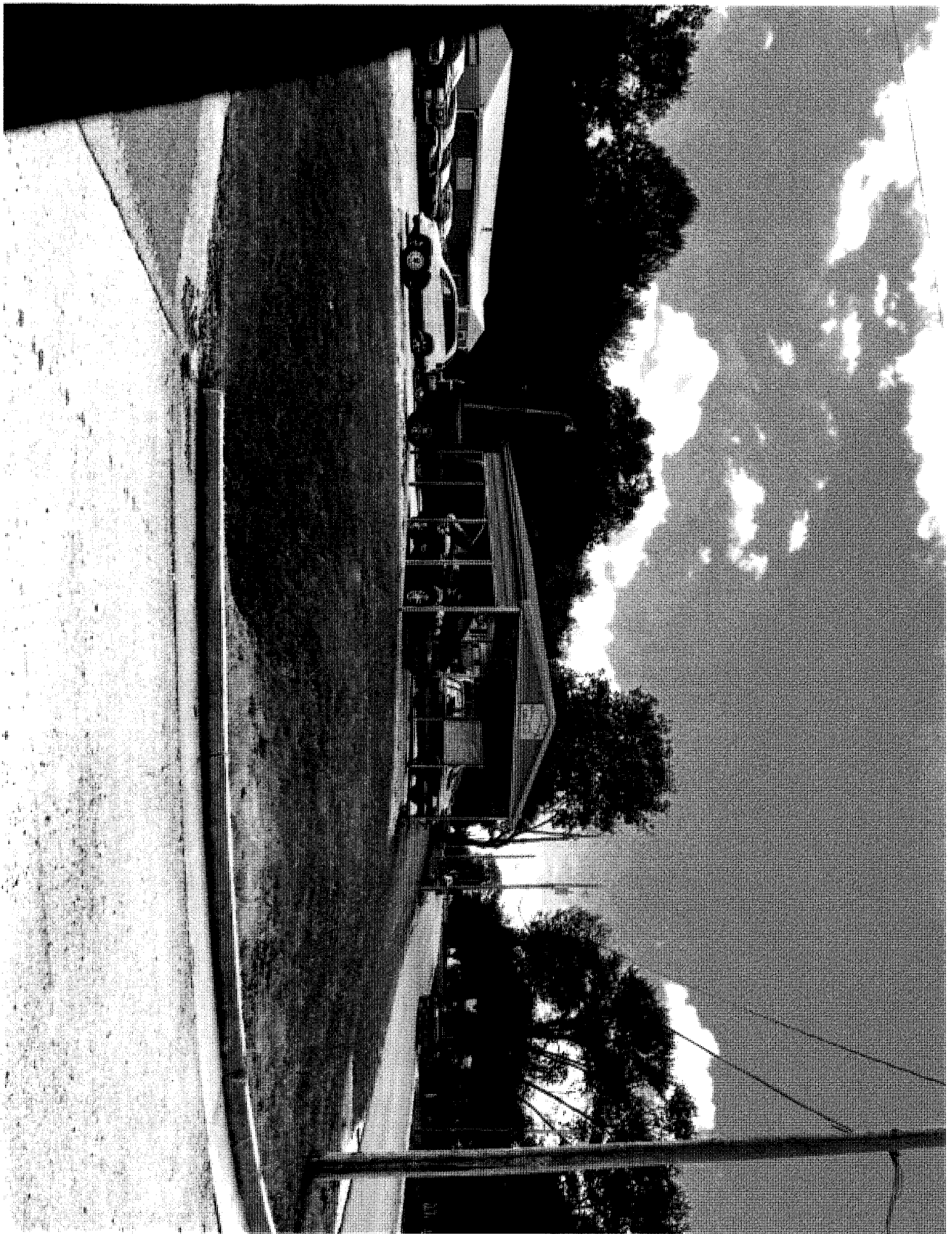
Notes

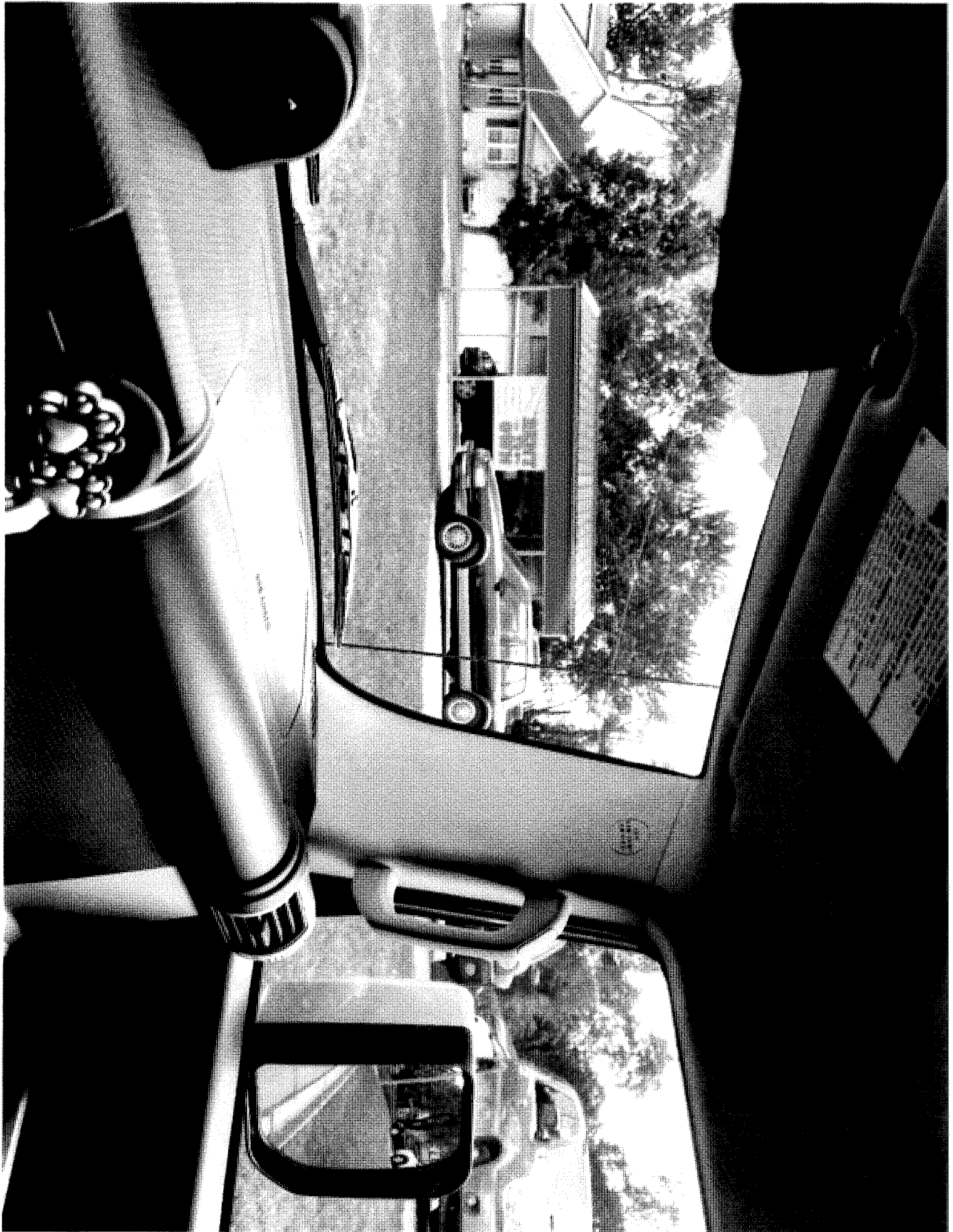
This Cadastral Map is for informational purposes only. It does not purport to represent a property boundary survey of the parcels shown and shall not be used for conveyances or the establishment of property boundaries.

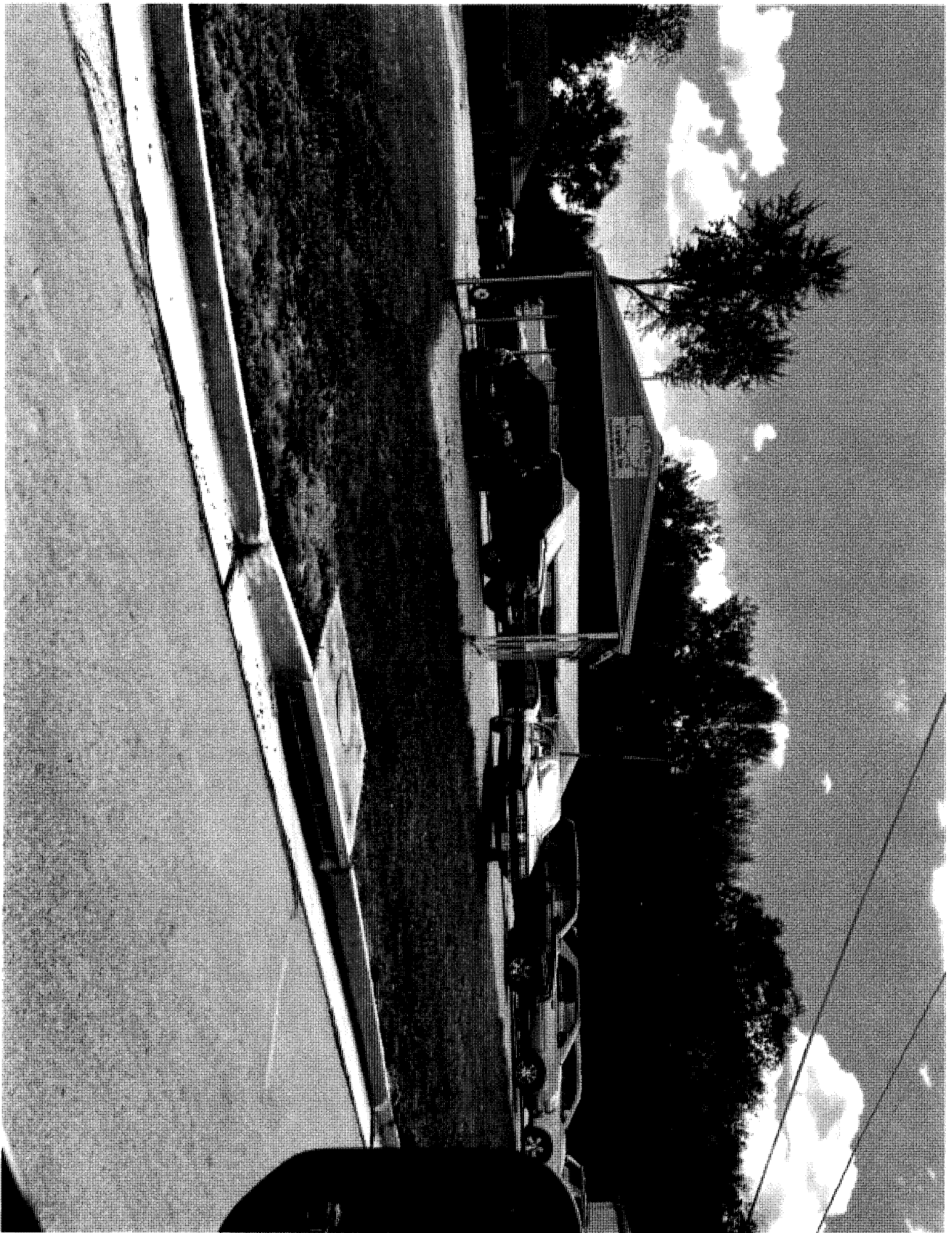
THIS MAP IS NOT TO BE USED FOR NAVIGATION

1 in. = 127ft

254.9 0 127.43 254.9 Feet







MEMO

To: Planning & Zoning Commission
From: John Simmons, Community Development Director
Date: September 27, 2023
Subject: 204 East 24th Street
Applicant: Nicholas A. Dilthey

Description of Request: Applicant requests a special use permit for the property located at 204 East 24th Street. Current zoning of the properties is C-1 Local Business. The applicant is requesting a special use permit to continue the use of the property for automobile sales.

Land Use Review:

The property located at 204 East 24th Street 0.539 acres and is currently used for the sale of used automobiles and carport structures. This use is in conflict with the zoning and the applicant has received notice of violation of the city code.

In reviewing the ownership and use history of the property, it was revealed that a commercial buildings was erected in 1977 and housed an automobile/implement service. The current property owner had been selling used automobiles at this location since 2019 until code enforcement inspection revealed that this was in violation of the zoning code. At that time, a violation letter was sent to the property owner and their business license was suspended.

Applicant submitted a rezoning application for the September Planning and Zoning meeting, but the meeting was canceled due to lack of a quorum. The staff recommendation at that time was to deny the rezoning to C-3 Commercial that zoning class is too broad and is not compatible with the single family composition of the surrounding land uses. Staff recommended that a special use permit be applied for instead at the October 2 meeting as the special use permit is tied to the applicant and not the land. Should the land change hands, the special use ceases.

The property to the north is zoned M-1 Light Industrial with a single family dwelling. The property to the east, south and west is zoned R-1 Single Family Residential with single family dwellings.

Staff Recommendation: Staff recommends the application for a special use permit be approved for the following reasons:

1. The used car lot is not obtrusive to the neighborhood and the use does not increase traffic or intensify land use when compared to previous uses of the C-1 Local Business property. The proposed use is not an intensive use of the property. Although the auto sales use is typically a C-3 Commercial use, it is not a heavy traffic creator, particularly due to the size of the operations.

2. The City of Sedalia Comprehensive Plans of 2021 and 2013 indicate that this Urban Development Area is designated as a conservation/stabilization area.
“Conservation/Stabilization areas are the most dominant areas in Sedalia” and as such “need to be sustained in the current manner as well as protected from physical and economic deterioration.”
3. The use would be attached to the applicant and not the land. Should the applicant ever sell the property the use would be invalidated whereas with a rezoning to C-3 Commercial, other uses intrusive to residential neighborhoods would be allowed.

Under Article V of the City of Sedalia’s zoning code, “automobile or trailer sales rooms or yards, other than premises where used vehicles are dismantled” are eligible to apply for a Special Use Permit.

Staff makes this recommendation based on including the following stipulations in the special use permit:

1. Applicant must maintain the property in compliance with the International Property Maintenance Code;
2. City may revoke special use permit upon violation of the IPMC.
3. Sale of goods on the lot is limited to used vehicles. Any other use of the exterior of the property is prohibited.
4. Preparation of sale of vehicles must be conducted inside the building and not on the exterior.

Should you have any questions or concerns regarding anything outlined in this advisory, please do not hesitate to contact me at 827-3000 or jsimmons@sedalia.com.

MEMO

To: Planning & Zoning Commission
From: John Simmons, Community Development Director
Date: September 27, 2023
Subject: 204 East 24th Street
Applicant: Nicholas A. Dilthey

Description of Request: Applicant requests a special use permit for the property located at 204 East 24th Street. Current zoning of the properties is C-1 Local Business. The applicant is requesting a special use permit to continue the use of the property for automobile sales.

Land Use Review:

The property located at 204 East 24th Street 0.539 acres and is currently used for the sale of used automobiles and carport structures. This use is in conflict with the zoning and the applicant has received notice of violation of the city code.

In reviewing the ownership and use history of the property, it was revealed that a commercial buildings was erected in 1977 and housed an automobile/implement service. The current property owner had been selling used automobiles at this location since 2019 until code enforcement inspection revealed that this was in violation of the zoning code. At that time, a violation letter was sent to the property owner and their business license was suspended.

Applicant submitted a rezoning application for the September Planning and Zoning meeting, but the meeting was canceled due to lack of a quorum. The staff recommendation at that time was to deny the rezoning to C-3 Commercial that zoning class is too broad and is not compatible with the single family composition of the surrounding land uses. Staff recommended that a special use permit be applied for instead at the October 2 meeting as the special use permit is tied to the applicant and not the land. Should the land change hands, the special use ceases.

The property to the north is zoned M-1 Light Industrial with a single family dwelling. The property to the east, south and west is zoned R-1 Single Family Residential with single family dwellings.

Staff Recommendation: Staff recommends the application for a special use permit be approved for the following reasons:

1. The used car lot is not obtrusive to the neighborhood and the use does not increase traffic or intensify land use when compared to previous uses of the C-1 Local Business property. The proposed use is not an intensive use of the property. Although the auto sales use is typically a C-3 Commercial use, it is not a heavy traffic creator, particularly due to the size of the operations.

MEMO

To: Mayor Andrew Dawson and Sedalia City Council
From: John Simmons, Community Development Director
Date: November 14, 2023
Subject: Special Use Permit Application
204 East 24th Street
Nicholas Dilthey

Description of request: Special use permit application for automobile sales in C-1 Local Business Zoning located at 204 East 24th Street by Nicholas Dilthey

Please see the attached minutes (labeled “P&Z Meeting Minutes”) from the September 1, October 4 and November 8, 2023 Planning and Zoning Commission meetings. These minutes show the progression of the case from a rezoning request to a special use permit application at the September 1 meeting, the tabling of the request at the October 4 meeting for more information and the recommendation of approval of the request at the November 8 meeting.

I have also included the staff recommendations (labeled “P&Z Staff Recommendations”) for the rezoning and special use permit applications as the case progressed.

At the November 8, 2023 Planning and Zoning Commission meeting the Commission recommended the approval of the special use permit application for council consideration at the November 20, 2023 council meeting by a vote of seven in favor, one abstention and two absent.

Should you have any questions or concerns regarding anything outlined in this memo please do not hesitate to contact me at 827-3000.



Let's Cross Paths

PLANNING & ZONING COMMISSION

Wednesday, November 8, 2023

Council Chambers

5:30 pm

Planning & Zoning Commission

Tolbert Rowe	Present	Andrew Dawson	Absent
Ann Richardson	Present	Teresa McDermott	Present
Rhonda Ahern	Present	Mike Privitt	Absent
Valerie Bloess	Present	Ann Graff	Present
Jerry Ross	Present		
Chris Marshall	Present		

STAFF:

Kelvin Shaw

John Simmons

Devin Lake

- Tolbert Rowe, Chairman, called the meeting to order at 5:30 pm.
- Roll Call

The minutes from the October 4th meeting were presented for approval. Amendments were made to indicate that both Anne and Teresa were present. Anne Richardson made a motion to accept the minutes with changes, which was unanimously approved

➤ **New Business**

- **Rezoning Code Amendment (Animal Control):** The commission discussed the necessity to remove a remnant in zoning related to animal control, not addressed in the recent city council update. A motion was made to remove the provisions for "private stable" from section 6437-B11C, aligning with Chapter 8 of the Animal Code. This motion was put forward by Jerry Ross, seconded by Anne Richardson and subsequently unanimously approved.

➤ **Old Business**

- **Rezoning Application for 204 E 24th:** The commission revisited a tabled public hearing from October 4th regarding a special use permit application for automobile sales at 204 East 24th Street. CBO Devin Lake provided an update on compliance issues, including a permit for a carport and zoning setbacks. Michael Comer of 305 West Cooper addressed the commission

regarding a personal vehicle on the property. Further public commentary was provided by a resident, Vaughn Loomis of 300 East 24th Street, advocating for future residential zoning considerations in the area.

The motion to approve the special use permit for 204 East 24th Street was made by Jerry Ross and seconded by Anne Richardson. The vote was conducted with one abstention from Chris Marshall, citing a personal connection. The motion passed 7 (seven) in favor, 1 (one) abstaining and will proceed to the City Council for final approval on November 20th.

➤ **Announcements**

- The commission noted that no further applications are pending, indicating a potentially quiet December meeting. The deadlines for rezoning applications for the December meeting have passed. Season's greetings were extended, and a reminder was given for the next City Council meeting.

➤ **Adjournment**

- The meeting was adjourned with a motion from Jerry Ross and a Second from Teresa McDermott, with members reminded to attend the upcoming City Council meeting for further discussions on the special use permit.

EXCERPT FROM THE OCTOBER 4, 2023 PLANNING AND ZONING COMMISSION MEETING

Open Public Hearing- 204 E 24th Street. Special Use Permit application from Nicholas Dilthey.

Public Hearing opened at 6:27 p.m. John Simmons indicated the property is currently zoned C-1. Applicant had originally requested rezoning to C-3, staff recommended after the cancelled September meeting, that this would be better served as a Special Use Permit. C-3 is too broad of a category to allow that zoning in that area.

Nicholas Dilthey, owner was present for the meeting. He purchased this property in 2017 and has been selling cars ever since. Hasn't had any problems, no complaints. Ever since he was growing up there has always been a car business there. Just purchased the property knowing he could sell cars there and now all of a sudden it's become a problem. That business is what supports his family and supports Sedalia by the revenue it brings in. Val wanted to know if he's had the license to sell cars there. Nick said he's had city license there for the last five years. He bought the property knowing he could sell vehicles there.

Gary Lahmeyer of 201 E 24th Street spoke and he has two properties across the street and have been there for probably 70 years. This property has always been a car lot or retail lot. He has no complaints or problems with the place and to his knowledge none of his neighbors have any complaints.

John said he did receive one phone call before the September meeting for the rezoning application, property owner across the street to the north was opposed to it.

The public hearing closed at 6:32. John said in the packet was a letter from Baker Legal Services, Daniel Baker, on behalf of the applicant. John also drove past the property in mid-September & took some pictures of the property. Applicant requests Special Use Permit to continue the use of the property for automobile sales. Currently used for the sale of used automobiles and carport structures. This use is in conflict with the zoning and applicant has received a notice of violation of the city code. In the last few years have changed the way of communication between departments. He was issued a business license before code enforcement noticed was in conflict of zoning ordinance. Commercial building was erected in 1977 and housed an automobile implement service. Current owner has been selling automobiles since 2019 until code enforcement revealed this was in violation of the zoning code. Applicant submitted rezoning application for the September Planning & Zoning meeting but that meeting was cancelled due to lack of quorum. The recommendation at that time was to deny the rezoning to C-3 commercial. Staff recommended that a Special Use Permit be applied for as a special use permit is tied to the applicant and not the land. Should the land change hands, the special use permit ceases. The new owner has the opportunity to approach the board for another special use permit. Staff recommends the application for the Special Use Permit be approved due to the used car lot is not obtrusive to the neighborhood and does not increase traffic; the use would be attached to the applicant and not the land. Should the applicant ever sell the property the use would be invalidated whereas with rezoning to C-3 Commercial, other uses intrusive to residential neighborhoods would be allowed. Under Article V of the City of Sedalia's zoning code, "automobile or trailer sales rooms or yards, other than premises where used vehicles are dismantled" are eligible to apply for a Special Use permit. Making this recommendation with some stipulations. Building Official, Devin Lake explained the conditions she's concerned with. Code Enforcement issued a violation letter for motor vehicles in February 2023, accumulation of trash & rubbish & zoning violation. To date the motor vehicles & zoning is still not

compliant. The trash & rubbish has been taken care of. Also realized the carport constructed there did not obtain a building permit to be constructed there so a new violation letter was sent out last week. He has appeared in municipal court for these violations so seeing that the property is still in violation of the International Property Maintenance Code staff has made the recommendation of stipulations of this special use permit including: occupant must maintain the property in compliance with the International Property Maintenance Code; City may revoke special use permit upon violation of that code; sale of goods on that lot is limited to used vehicles, any other use of the exterior of the property is prohibited and preparation of sale of vehicles must be conducted inside the building and not on the exterior: Devin's recommendation all of these must be in compliance within 30 days. Mayor Dawson asked if there is any type of notice if found in violation or does the revocation happen automatically?

Devin said if found in violation again they would be issued another violation letter & per code they have 10 days to take care of the issue. Rhonda said he's selling carports as well. Devin said the sale of carports would be prohibited. Devin said there would be an appeals process for the revoking of the business license because of the revoking of the special use permit from having violations. John said the case of the carport is there was no building permit for it. Nick said he didn't know he had to have a permit. Devin said since this violation has been open since February that's why her recommendation would be that all those violations need to be corrected within 30 days. Ann said she doesn't feel comfortable having all these questions.

Terry said her question is that he has to maintain his property according to the International Property Maintenance Code is the owner aware of everything entailed in this IPMC? Devin said it's available on our City's website. John said the violations he received in the past are what the concern is. Terry said she just didn't know if there is anything else in there that he may not be aware of that might just pop up. Nick said the carport is just for display. It is anchored to the ground. Nick sells the carports for Coast to Coast. He didn't know you had to have a permit for this carport. Mr. Saker asked if it's possible to get a carport to keep it. Devin said as long as a sale isn't occurring and as long as it meets all the setbacks that would have been addressed during the building permit process. Not moving carports in & out, used as a display building only. Jerry Ross made a motion to table for 30 days, seconded by Rhonda Ahern for Mr. Diltney to come into compliance with these issues.



**City of Sedalia
Council Agenda Work Flow**

Council Meeting Date:

Agenda Item:

Department: Department Head:

Legal Review Needed – If So Attorney Assigned:

<u>Documents Required</u>	<u>Date Required</u>	
<input checked="" type="checkbox"/> Memo	<input type="text" value="11/10/23"/>	(To Clerk 10 Business Days Before Council Meeting)
<input type="checkbox"/> Employee Bio	<input type="text"/>	(To Clerk 3 Business Days Before Council Meeting)
<input checked="" type="checkbox"/> Ordinance	<input type="text" value="11/10/23"/>	(Clerk Prepare 8 Business Days Before Council Meeting)
<input type="checkbox"/> Resolution	<input type="text"/>	(Clerk Prepare 8 Business Days Before Council Meeting)
<input type="checkbox"/> Contract	<input type="text"/>	(Legal Review Completed and to Clerk 10 Business Days Before Council Meeting) (Note Templates Allow Quicker Turn Around)
<input type="checkbox"/> Hearing Ad	<input type="text"/>	(To Clerk 5 Business Days Before The Ad Has To Run)
<input type="checkbox"/> Petition	<input type="text"/>	(To Clerk 10 Business Days Before Council Meeting)

Process Completed / Ready For Packet

(City Clerk Verified)

BILL NO. _____

ORDINANCE NO. _____

AN ORDINANCE AUTHORIZING A MASTER SERVICES AGREEMENT FOR AERIAL PHOTOGRAPHY SERVICES.

WHEREAS, the City of Sedalia, Missouri has received a Master Services agreement from Pictometry International Corp., dba Eagleview for aerial photography services; and

WHEREAS, under the agreement, the City of Sedalia, Missouri shall pay the sum and amount not to exceed Three Hundred Five Thousand One Hundred Ninety-Nine Dollars (\$305,199.00) spread over three separate projects as follows and more fully described in the agreement attached to this Ordinance and incorporated by reference herein.

First Project - \$101,733.00
Second Project - \$101,733.00
Third Project - \$101,733.00

NOW THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE CITY OF SEDALIA, MISSOURI as follows:

Section 1. Ordinance number 11884 is hereby repealed.

Section 2. The Council of the City of Sedalia, Missouri hereby authorizes the Master Services agreement by and between the City of Sedalia, and Pictometry International Corp., dba Eagleview as the agreement has been proposed.

Section 3. The Mayor or City Administrator are authorized and directed to execute and the City Clerk is hereby authorized and directed to attest and fix the seal of the City of Sedalia, Missouri on the agreement in substantively the same form and content as the agreement has been proposed.

Section 4. The City Clerk is hereby directed to file in his office a duplicate or copy of the agreement after it has been executed by the parties or their duly authorized representatives.

Section 5. This ordinance shall be in full force and effect from and after its passage and approval.

Read two times by title, copies of the proposed ordinance having been made available for public inspection prior to the time the bill is under consideration by the Council and passed by the Council of the City of Sedalia, Missouri this 6th day of November 2023.

Presiding Officer of the Council

Approved by the Mayor of said City this 6th day of November 2023.

Andrew L. Dawson, Mayor

ATTEST:

Jason S. Myers, City Clerk



CUSTOMER NAME: City of Sedalia, MO
Attn: Devin Lake
CUSTOMER ADDRESS: 200 S. Osage
Sedalia, Missouri 65301
CUSTOMER PHONE: (660) 827-3000
CUSTOMER E-MAIL: dlake@cityofsedalia.com

MASTER SERVICES AGREEMENT

This Master Service Agreement (“Agreement”) is entered into by and between the Customer identified above (“Customer”) and Pictometry International Corp. dba EagleView, a corporation formed under the laws of the State of Delaware, with its principal place of business at 25 Methodist Hill Drive, Rochester, NY 14623 (“EagleView”). This Agreement is effective as of the date Customer signs the Order Form and will remain in effect during the Term, as defined below or until terminated as provided in this Agreement. In the event of a conflict between the terms of this Agreement and an Order Form, the Order Form shall prevail. Customer and EagleView may be referred to individually as “Party” and/or collectively as “Parties”. EagleView shall provide the Product(s) and/or Service(s) in accordance with and subject to the conditions of this Agreement during the applicable Term as defined below.

GENERAL TERMS AND CONDITIONS

1. DEFINITIONS

- 1.1. **“Account”** means an account created for Customer by EagleView for the purpose of providing access to the Product(s) and/or Service(s).
- 1.2. **“Activation”** means the point in time where Customer has access to an Account and the Products and/or Services are available to Customer.
- 1.3. **“Authorized User”** means: (i) any employee or elected or appointed official of the Customer authorized by Customer to use the Service; (ii) any additional users as may be defined in an Order Form (such as governmental subdivisions and their employees or elected or appointed officials if the Order Form indicates that governmental subdivisions are included) all of whom are considered to be agents of Customer for the purposes of Section 1.3; or (iii) a contractor of Customer (so long as Customer gives written notice of its intent to use such contractor to EagleView prior to being granted access to the Service and, unless EagleView expressly waives such requirement for any individual, has entered into a written agreement with EagleView authorizing such access).
- 1.4. **“Confidential Information”** means any non-public information that is identified as or would be reasonably understood to be confidential and/or proprietary as disclosed by a Party (“Discloser”) to another Party (“Recipient”). Confidential Information of EagleView includes, but is not limited to: (a) the Product(s) and/or Service(s) including any related software code and Documentation; (b) the terms of this Agreement including all Order Forms and statements of work as applicable and related pricing, to the extent Customer is not required to disclose this information under a Freedom of Information Act type obligation, and (c) EagleView’s roadmaps, product plans, product designs, architecture, technology and technical information, security audit reviews, business and marketing plans, and business processes, however disclosed. Confidential Information shall not include information that was (a) at the time of disclosure, through no fault of the Recipient, already known and generally available to the public; (b) at the time of disclosure to Recipient already rightfully known to the Recipient without any obligation of confidentiality; (c) disclosed to the Recipient by a third party who had the right to make the disclosure without any confidentiality restrictions; or (d) independently developed by the Recipient without access to or use of the Discloser’s Confidential Information.
- 1.5. **“Documentation”** means the materials describing the features and functions of the Product(s) and/or Service(s) as may be updated from time to time by EagleView.



- 1.6. **“Fee”** means the fees charged by EagleView for the Product(s) and/or Service(s) as identified in an Order Form or an invoice issued by EagleView.
- 1.7. **“Intellectual Property Rights”** means all worldwide intellectual property rights whether registered or unregistered including copyrights, patents, patent applications, trademarks, service marks, trade secrets, and all other proprietary rights.
- 1.8. **“Malware”** means any software program or code intended to harm, destroy, interfere with, corrupt, or cause undesired effects on program files, data, or other information, executable code, or application software macros.
- 1.9. **“Order Form”** means a mutually agreeable order describing the Product(s) and/or Service(s) purchased by Customer. The Parties may enter into several Order Forms with each Order Form made part of this Agreement.
- 1.10. **“Products and/or Services”** means EagleView’s proprietary products and/or services and/or content identified in an Order Form and developed and owned by EagleView, its Affiliates (its directors, officers, employees, agents, representatives, advisors, and persons or entities which are controlled by or are under common control with EagleView) and/or their licensors.

2. ACCESS AND USE OF THE PRODUCT(S) AND/OR SERVICE(S)

- 2.1. **Access to the Product(s) and/or Service(s).** Subject to Customer’s compliance with the terms of this Agreement, EagleView hereby grants to Customer the right to access and use the Product(s) and/or Service(s) identified on an Order Form(s) for its internal business purpose on a limited, revocable, non-exclusive, non-transferable basis in accordance with the scope of use identified in the Order Form. Unless a different term of the license grant to a Product is set forth in an Order Form, the right to access and use the Product(s) and Service(s) for its internal business purpose during the term of any Order Form(s) is the only right granted to Customer under this Agreement and any Order Form(s). EagleView will have no liability for any loss or damage arising from Customer’s failure to comply with the terms of this Agreement. EagleView will provide Customer a primary Administrator Account for managing and granting access to its Authorized Users. Customer shall be responsible for activating Authorized Users through use of the Account. Customer and its Authorized Users are responsible for maintaining the confidentiality of all passwords.
- 2.2. **Access Restrictions.** Access by Customer and its Authorized Users to the Service is subject to the following conditions:
- 2.2.1. Customer shall not access the Product(s), Service(s) or Confidential Information of EagleView in a way that might adversely affect the security, stability, performance, or functions of the Service.
- 2.2.2. Customer will not directly or indirectly: (a) resell or sublicense the Product(s) and/or Service(s), (b) modify, disassemble, decompress, reverse compile, reverse assemble, reverse engineer, or translate any portion of the software related to the Product(s) and/or Service(s); (c) create derivative works from the Product(s) or Service(s); (d) use the Product(s) and/or Service(s) in violation of applicable law or the rights of others; (e) perform any vulnerability or penetration testing of the Service; (f) cause harm in any way to the Product(s) and/or Service(s) or cause Malware to harm the Products and/or Service(s); (g) work around the Product(s) and/or Service(s) technical limitations; (h) remove any proprietary notices from the Application, documentation or any other EagleView materials furnished or made available hereunder; (i) access the Application in order to build a competitive product or service; or (j) copy any features, functions or graphics of the Application.
- 2.2.3. Customer will not use the Product(s) and/or Service(s) in connection with any data that: (a) may create a risk of harm or loss to any person or property; (b) constitutes or contributes to a crime or tort; (c) is illegal, unlawful, harmful, pornographic, defamatory, infringing, or invasive of personal privacy or publicity



rights; (d) contains any information that Customer does not have the right to use; or (e) use the Application or associated documentation or Data Products in violation of export control laws and regulations.

2.2.4. EagleView may suspend the Product(s) and/or Service(s) if EagleView determines, in its reasonable discretion, that suspension is necessary to protect Customer or the Service from operational, security, or other material risk, or if the suspension is ordered by a court or other tribunal. In such event(s), EagleView will provide notice of suspension to Customer as soon as reasonably practicable.

2.3. Account Use. Customer is responsible for maintaining and keeping confidential its Account information, including passwords, usernames, and email addresses. If Customer becomes aware of: (i) any violation of the terms of this Agreement by an Authorized User or unauthorized access to an Account, or (ii) any compromise to an Account including unauthorized access to or disclosure of any Account information, passwords, usernames or login credentials, Customer must promptly suspend such access or Authorized User and notify EagleView.

2.4. Reservation of Rights. Except for the limited rights expressly granted herein, EagleView and its Affiliates retain all right, title and interest in all Intellectual Property Rights and technology related to EagleView's proprietary Products and Services. Customer shall preserve and keep intact all EagleView copyright, patent, and/or trademark notices presented in connection with the Products and Services. Customer shall not assert any implied rights in or to any of EagleView's Intellectual Property Rights. From time to time, Customer may provide suggestions, ideas, enhancement requests, or other information on their use of the Products or Services ("Feedback"). Customer agrees that EagleView shall have all right, title, and interest to use such Feedback without any restrictions and without any payment to Customer.

3. PAYMENT

3.1. Fees. Customer shall pay the Fees within thirty (30) days of receipt of invoice. EagleView shall have the right to assess a late payment charge on any overdue amounts equal to the higher of: (i) one and one-half percent (1.5%) per month; or (ii) the rate allowed by applicable law. Additional payment terms may be set forth in the Order Form. All Fees paid pursuant to this Agreement and any applicable Order Form are non-refundable and all Product(s) and/or Service(s) ordered pursuant to an Order Form are non-cancelable, unless expressly stated to the contrary. In the event that EagleView seeks legal recourse for the collection of any unpaid Fees from Customer, Customer shall be responsible for all of EagleView's costs of such collection action if EagleView is the prevailing party. If any Fees are overdue by more than thirty (30) days, EagleView may, without limiting its other rights and remedies, suspend the Product(s) and/or Service(s) until such amounts are paid in full, provided that, EagleView will give Customer at least ten (10) days' prior notice that its account is overdue.

3.2. Pricing Changes. EagleView shall have the option to adjust the pricing for any Products and/or Services upon any renewal or extension of an Order Form by providing one hundred and eighty (180) days' notice of such pricing change to Customer prior to the date for such renewal or extension.

3.3. Taxes. The Fees do not include any levies, duties excise, sales, use, value added or other taxes, tariffs, or duties that may apply to the Product(s) and/or Service(s) ("Taxes"). Customer is responsible for paying all Taxes associated with its purchases hereunder. If EagleView has the legal obligation to collect Taxes from Customer, Customer will pay that amount to EagleView unless Customer provides EagleView with a valid tax exemption certificate authorized by the applicable taxing authority prior to billing. For clarity, EagleView is solely responsible for taxes assessable against it based on its income, property, and employees.

4. TERM AND TERMINATION

4.1. Term. The term of this Agreement will commence on the date Customer signs an Order Form under this Agreement and will end upon the expiration date of the Order Form, or upon the expiration date of any subsequent or renewal Order Form(s) ("Term"). After expiration Customer shall not have any access to content, Product(s) or Service(s). Unless either Party gives notice of its intent not to renew the Product(s) and/or Service(s) and/or Content at least one hundred and twenty (120) days prior to the end of the then current Term, access to the Services will automatically renew.



4.2. Termination. Either Party may terminate this Agreement upon written notice to the other Party if: (i) the non-terminating Party materially breaches this Agreement and fails to cure such breach within thirty (30) days of delivery of written notice; or (ii) if the other Party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation, or assignment for the benefit of creditors. EagleView may suspend the Product(s) and/or Service(s) in the event Customer is in material breach of this Agreement and such breach has not been cured within thirty (30) days' written notice to Customer. In the event of suspension due to Customer's material breach of this Agreement, Customer will remain liable for all Fees applicable to the Term that would have been paid had the Product(s) and/or Service(s) not been suspended.

4.3. Effect of Termination on Fees: EagleView Breach. In the event this Agreement is terminated by Customer for a material breach by EagleView, (a) where EagleView has fully delivered imagery to Customer, no refund of fees shall be made, or (b) where customer is accessing on-line imagery and data access and/or an application, EagleView will refund any unused prorated, prepaid fees for the Product(s) and/or Service(s).

4.4. Effect of Termination on Fees: Customer Breach. In the event this Agreement is terminated by EagleView for a material breach by Customer, Customer shall be responsible for all fees under any current Order Form(s).

4.5. Survival. Upon any expiration of the Product(s) and/or Services or termination of this Agreement, the following sections shall survive: 2.4 (Reservation of Rights), 3 (Payment), 5 (Confidentiality), 7 (Indemnification), 8 (Limitation of Liability), and 9 (General Provisions).

5. CONFIDENTIALITY

5.1. Obligations. Each Party will hold the other Party's Confidential Information in confidence with at least as much care as it holds its own Confidential Information, and neither Party will disclose any of the other Party's Confidential Information to any third party. Each Party may use the Confidential Information solely for purposes of its performance under this Agreement, and may disclose such information to its employees, subcontractors and professional advisors only on a need-to-know basis, provided that such employees, subcontractors and professional advisors are bound by obligations of confidentiality at least as restrictive as those set forth in this Agreement.

5.2. Required Disclosure. The Recipient may disclose Confidential Information as required by court order or otherwise by law, provided that it gives the Discloser prior written notice of such disclosure (to the extent legally permitted) as well as reasonable assistance if Discloser seeks a protective order to prevent the disclosure. Any disclosure pursuant to this Section 5.2 shall be restricted to include the least amount of Confidential Information necessary to comply with the order. All costs incurred by the Recipient in connection with complying with such order shall be reimbursed by the Discloser.

6. WARRANTIES

6.1. Mutual Warranties. Each Party represents and warrants to the other Party that: (i) it is a organization duly organized, validly existing and in good standing under the laws of the jurisdiction of its formation, has all requisite power and authority to carry on its business and to own and operate its properties and assets; and (ii) the individual signing this Master Services Agreement and/or the Order Form(s) has the requisite authority to bind the party to this Agreement.

6.2. EagleView Warranty. EagleView warrants that (i) it will provide the Product(s) and/or Service(s) with commercially reasonable care and skill; and (ii) the Product(s) and/or Service(s) will conform to the then-current Documentation in all material respects. In the event of a breach of this warranty, Customer's sole and exclusive remedy shall be as described in Section 4.3 Payments Upon Termination.

6.3. Disclaimer. EXCEPT FOR EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, EAGLEVIEW MAKES NO ADDITIONAL REPRESENTATION OR WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED IN FACT OR BY OPERATION OF LAW, OR STATUTORY, AS TO ANY MATTER WHATSOEVER. EAGLEVIEW EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. EAGLEVIEW DOES NOT



WARRANT THAT THE PRODUCT(S) AND/OR SERVICE(S) (INCLUDING ANY SUPPORT SERVICES) WILL BE ERROR FREE, WILL MEET CUSTOMER'S REQUIREMENTS, OR WILL BE TIMELY OR SECURE. CUSTOMER WILL NOT HAVE THE RIGHT TO MAKE OR PASS ON ANY REPRESENTATIONS OR WARRANTY ON BEHALF OF CUSTOMER TO ANY THIRD PARTY. TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE SERVICES AND SUPPORT SERVICES ARE PROVIDED "AS IS."

7. INDEMNIFICATION

7.1. EagleView Indemnification. EagleView will defend Customer against any claim, demand, suit or proceeding made by a third party alleging that the Product(s) and/or Service(s) infringes the intellectual property rights of such third party and will pay all costs or damages that are finally awarded by a court of competent jurisdiction (including reasonable attorneys' fees) or agreed to in a written settlement signed by EagleView. Customer will: (i) notify EagleView in writing within ten (10) calendar days of its receipt of notice of the claim, (ii) give EagleView sole control of the defense and settlement of the claim (except that EagleView will not settle any claim that results in liability or an admission of liability by Customer without Customer's prior written consent), and (iii) provide EagleView with all reasonable assistance, information, and authority necessary to perform EagleView's obligations under this paragraph. Notwithstanding the foregoing, EagleView will have no liability for any claim of infringement or misappropriation to the extent such claim arises from: (i) use of the Product(s) and/or Service(s) in combination with materials including software, hardware, or content not furnished by EagleView; or (ii) Customer's breach of this Agreement.

7.2. Remedies. In the event the Product(s) and/or Service(s) is held or is believed by EagleView to infringe or misappropriate any Intellectual Property Right of a third party, EagleView will have the option, at its expense, to: (i) replace the Product and/or Service with a non-infringing equivalent, (ii) modify the Product(s) and/or Service(s) to be non-infringing, (iii) obtain for Customer a license to continue using the Product(s) and/or Service(s); or (iv) terminate the Agreement and refund any prepaid, prorated fees for the remainder of the Term. The foregoing remedies constitute Customer's sole and exclusive remedies and EagleView's sole liability with respect to any third-party infringement claim.

7.3. Customer Indemnification. Customer will, at its expense, defend EagleView from and against all third party claims and will pay any costs, losses or damages that are finally awarded (including reasonable attorneys' fees) or agreed to in settlement to the extent arising out of Customer's breach of this Agreement, provided that (i) EagleView notifies Customer in writing within ten (10) calendar days of its receipt of written notice of the claim, (ii) Customer has sole control of the defense and settlement of the claim (except that Customer will not settle any claim that results in liability or an admission of liability by EagleView without EagleView's prior written consent), and (iii) EagleView provides Customer with all reasonable assistance, information, and authority necessary to perform Customer's obligations under this paragraph.

8. LIMITATION OF LIABILITY

8.1. Consequential Damages. TO THE EXTENT PERMITTED BY LAW, IN NO EVENT SHALL EITHER PARTY OR ITS AFFILIATES BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, COVER, BUSINESS INTERRUPTION, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND OR NATURE, INCLUDING, BUT NOT LIMITED TO, LOSS OF USE, DATA, PROFITS, REVENUE, OR GOODWILL, WHETHER AN ACTION IS BASED IN CONTRACT, TORT, OR OTHERWISE, REGARDLESS OF WHETHER EITHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

8.2. Limitation of Liability. EXCLUDING EITHER PARTY'S INDEMNIFICATION OBLIGATIONS PURSUANT TO SECTION 7, TO THE EXTENT PERMITTED BY LAW, THE AGGREGATE AND CUMULATIVE LIABILITY OF EITHER PARTY INCLUDING ALL THEIR AFFILIATES REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT OR TORT (INCLUDING BUT NOT LIMITED TO NEGLIGENCE) SHALL IN NO EVENT EXCEED THE AMOUNT OF FEES PAID OR PAYABLE BY CUSTOMER IN THE TWELVE MONTHS PRECEDING THE ACTIONS GIVING RISE TO THE CLAIM.

9. GENERAL PROVISIONS



9.1. Export Laws. The Product(s) and/or Services and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. EagleView and Customer each represent that it is not named on any U.S. government denied-party list. Customer will not permit any user to access or use any Product(s) and/or Service(s) or Content in a U.S.-embargoed country or region (including but not limited to Cuba, Iran, North Korea, Sudan, Syria, Crimea, or Russia) or in violation of any U.S. export law or regulation.

9.2. No Third-Party Beneficiaries. Except as specifically identified in this Agreement, nothing in this Agreement is intended to confer upon any person other than the parties and their respective successors or permitted assigns, any rights, remedies, obligations, or liabilities whatsoever.

9.3. Independent Contractors. Nothing contained in this Agreement shall be deemed or construed as creating a joint venture or partnership between any of the Parties hereto. Neither Party shall have the power nor authority to control the activities or operations of the other. At all times, the status of the Parties shall be that of independent contractors.

9.4. Force Majeure. Except with respect to Customer's payment obligations for services delivered, reports delivered, or any ongoing payment obligation, each party will be excused from performance under this Agreement, will not be deemed to be in breach hereof, and will have no liability to the other party whatsoever if either party is prevented from performing any of its obligations hereunder, in whole or in part, as a result of a Force Majeure Event. A "Force Majeure Event" means an event or occurrence beyond the control of the nonperforming party, such as an act of God or of the public enemy, embargo or other act of government in either its sovereign or contractual capacity, government regulation, travel ban or request, court order, civil disturbance, terrorism, war, quarantine restriction, epidemic, virus, fire, weather, flood, accident, strike, slowdown, delay in transportation, electrical power outage, interruption or degradation in electronic communications systems, inability to obtain necessary labor, materials or manufacturing facilities, and other similar events. In the event of any delay resulting from a Force Majeure Event, any date of delivery hereunder will be extended for a period equal to the time lost because of the delay.

9.5. Security Assessment. Upon reasonable request, EagleView will assist Customer in its EagleView security risk assessments by completing forms and/or providing reports that provide Customer with generally available information relating to EagleView's security practices, policies and procedures used to protect its systems. Such information will include high level overviews of implemented security measures, such as access controls, encryption, or other means, where appropriate, and will provide details relating to how Customer's Confidential Information is disclosed, accessed, processed, and stored (as applicable).

9.6. Assignment. Neither Party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the other Party's prior written consent (not to be unreasonably withheld); provided, however, either Party may assign this Agreement in its entirety (including all Order Forms), without the other Party's consent to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets. Subject to the foregoing, this Agreement will bind and inure to the benefit of the Parties, their respective successors, and permitted assigns.

9.7. Governing Law. This Agreement will be governed by the laws of the State of Customer, without regard to conflict of law principles. The Parties agree that any claims, legal proceedings, or disputes and/or litigation arising out of or in connection with this Agreement, will be brought solely in the state or federal courts located in the jurisdiction the Customer is based in, and the Parties irrevocably consent to the exclusive personal jurisdiction of such courts.

9.8. Severability & Waiver. The failure of either Party to exercise any right or the waiver by either Party of any breach, shall not prevent a subsequent exercise of such right or be deemed a waiver of any subsequent breach of the same, or any other provision of this Agreement. All waivers must be in writing and signed by the Party waiving its rights. If any section of this Agreement is held to be invalid or unenforceable, the remain sections of this Agreement will remain in force to the extent feasible.

9.9. Notices. Notwithstanding anything to the contrary in this Agreement, notices and other communications may be given or made pursuant to this Agreement via electronic mail. Notwithstanding the foregoing, any notice concerning a material breach, violation, or termination hereof must be in writing and will be delivered: (a) by certified or registered mail; or (b) by an internationally recognized express courier or overnight delivery service. All written notices or other written communications to EagleView shall be provided to the address first listed above and



addressed to: ATTENTION: LEGAL DEPARTMENT. All written notices to Customer shall be sent to the address identified on the Order Form and addressed to the individual signing said Order Form, and shall be deemed to have been duly given when delivered personally, when deposited in the U.S. mail, postage prepaid, or when deposited with an overnight courier or delivery service. With respect to notices and other communications regarding EagleView’s privacy policy, Support Plan, or other similar provisions, such notices shall be deemed given when posted to EagleView’s website (www.eagleview.com) or e-mailed to the Customer’s Account administrator(s).

9.10. Execution in Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed to be an original and all of which together shall constitute only one agreement. The execution and delivery of counterparts of this Agreement by electronic mail, electronic form (including execution by way of an electronic or other signature stamp), website submission, facsimile, or by original manual signature, regardless of the means or any such variation in pagination or appearance shall be binding upon the Parties executing this Agreement.

9.11. Entire Agreement. This Agreement, along with the Order Form(s) and Exhibit(s), contains the entire understanding of the Parties with respect to the subject matter hereof and supersedes all prior agreements, oral or written, and all other communications between the Parties relating to such subject matter. The Parties agree that any term or condition stated in a Customer purchase order is null and void. This Agreement may not be amended or modified except by mutual written agreement. In the event that any court holds any provision of this Agreement as null, void, or otherwise ineffective or invalid, such provision shall be deemed to be restated to reflect as nearly as possible the original intentions of the Parties in accordance with applicable law, and the remaining provisions shall remain in full force and effect. The unenforceability of any provision of this Agreement shall not affect the validity of the remaining provisions hereof. A waiver by either Party of a breach or failure to perform hereunder shall not constitute a waiver of any subsequent breach or failure.

Pictometry International Corp. dba EagleView

Customer

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____



EXHIBIT A

ORDER FORM

EFFECTIVE DATE (MONTH/DAY/YEAR): _____

TERM (DURATION): Six years

ORDER #
LC-10004728

BILL TO
City of Sedalia, MO
Devin Lake
200 S. Osage
Sedalia, Missouri 65301
(660) 827-3000
dlake@cityofsedalia.com

SHIP TO
City of Sedalia, MO
Devin Lake
200 S. Osage
Sedalia, Missouri 65301
(660) 827-3000
dlake@cityofsedalia.com

CUSTOMER ID	SALES REP	REFRESH FREQUENCY
A1216347	A. Stark	Biennial

QTY	PRODUCT NAME	PRODUCT DESCRIPTION
57	EagleView Cloud - Imagery GSD: 1in Refresh Frequency: 2-Year Refresh	Provides entitlement to the EagleView Platform, a secure hosted infrastructure and access to EagleView enabled workflow, analytics, and high-resolution imagery to dramatically improve efficiency for government agencies. Includes regular refreshes of ortho and oblique imagery at the GSD and frequency specified. Target capture season subject to weather and airspace permissions. Services term commences on date of activation.
658	EagleView Cloud - Imagery GSD: 6in Refresh Frequency: 2-Year Refresh	Provides entitlement to the EagleView Platform, a secure hosted infrastructure and access to EagleView enabled workflow, analytics, and high-resolution imagery to dramatically improve efficiency for government agencies. Includes regular refreshes of ortho and oblique imagery at the GSD and frequency specified. Target capture season subject to weather and airspace permissions. Services term commences on date of activation.
1	EagleView Cloud - Physical Delivery - Ortho	Provides an offline copy of the orthomosaic tiles and mosaics at the GSD specified in the EagleView Cloud - Imagery product once per refresh. Files to be provided in industry standard formats selectable by the customer with delivery made physically via hard drive media.
1	EagleView Cloud - Software	Provides an unlimited number of authorized users the ability to login and access the EagleView Cloud software and analytics via the web-based EagleView Cloud platform. This software provides a robust compliment of tools for engaging with imagery as well as additional project and collaboration tools, and access to mobile application. Requires the purchase of an EagleView - Imagery entitlement.
1	EagleView Cloud - Comprehensive Integration Bundle	Provides activation of integrations between the EagleView Cloud platform and compatible customer environments (including compatible CAMA providers, 911/PSAP, Cityworks, and ESRI/GIS) and via the Integrated Web Application.
1	EagleView Cloud - Authorized Subdivisions	Extends the ability for a contracting county or non-state consortium of counties the ability to authorize access to their EagleView Cloud organization to any political unit or subdivision located totally or substantially within their boundary.
1	EagleView Cloud - Early Access	Provides entitlement to imagery from counties neighboring the imagery AOI as part of EagleView Cloud. Also provides entitlement to Early Access to refreshed imagery captures which allows authorized users to use new imagery immediately following its preliminary processing and quality control checks and prior to its final processing. Early Access imagery will become available incrementally as it is processed, and it will remain available until final, fully processed imagery is made available through other means.



1	EagleView Cloud - Disaster Response Program	Includes eligibility for the Disaster Response Program.
9	EagleView Cloud - Years Capture History	Includes access to historical ortho and oblique frame imagery from the EagleView archive. Quantity represents the number of calendar years of archive imagery available in EagleView Cloud.

FEES

Due at Initial Activation of Services	\$50,866.50
Due at First Anniversary of Initial Activation of Services	\$50,866.50
Due at Second Anniversary of Initial Activation of Services	\$50,866.50
Due at Third Anniversary of Initial Activation of Services	\$50,866.50
Due at Fourth Anniversary of Initial Activation of Services	\$50,866.50
Due at Fifth Anniversary of Initial Activation of Services	\$50,866.50

The LiDAR products listed below shall be produced in conjunction with the 1st image capture refresh of the initial term of this Agreement.

QTY	PRODUCT NAME	PRODUCT DESCRIPTION
57	LIDAR-DEM and 1ft Contours (sq mi)	Available with qualifying LiDAR purchase. Gridded bare earth DEM in ArcGIS GRID format and tiled contours at a 1-foot interval in ESRI Polyline Feature Class format. Refer to attached terms and conditions.
57	LiDAR-PURCHASED-0.5m postings (sq mi) Custom Area	LiDAR data delivered in tiled LAS format, nominal raw post spacing of 0.5m, vertical accuracy sufficient to support optional generation of 1-ft contours (available separately). Customer shall own the copy of this LiDAR product delivered to Customer pursuant to this Agreement. EagleView shall retain copies of said LiDAR product and shall own those copies.

FEES - LIDAR

Due at Delivery/Activation	\$ 64,740.60
----------------------------	--------------

PRODUCT PARAMETERS

Disaster Response Program (“DRP”)

Agreement includes eligibility for the DRP described below so long as the customer remains under an active services agreement and in good standing with EagleView. Imagery captured through DRP will be captured “as-is”.

A. Disaster Coverage Imagery at No Additional Charge – EagleView will, upon request of Customer and at no additional charge, provide standard quality imagery of up to 200 square miles of affected areas (as determined by EagleView) upon the occurrence of any of the following events during any period Customer is eligible for DRP:

- Hurricane: areas affected by hurricanes of Category 2 and higher.
- Tornado: areas affected by tornados rated EF4 and higher.
- Terrorist: areas affected by damage from terrorist attack.
- Earthquake: areas affected by damage to critical infrastructure resulting from earthquakes measured at 6.0 or higher on the Richter scale.
- Tsunami: areas affected by damage to critical infrastructure resulting from tsunamis.

B. Discounted Rate – Coverage for areas affected by the events set forth above exceeding 200 square miles will be, subject to EagleView resource availability, offered to Customer at the then-current DRP rates. Also, coverage for areas affected by hurricanes below Category II, tornadoes below EF4 or earthquakes rated below 6.0 on the Richter scale, flooding meeting or exceeding the major flood stage, wildfires impacting population centers, or other disasters as agreed to between the customer and EagleView, will be, subject to EagleView resource availability, offered to Customer at the then current DRP rates.

LiDAR 0.5 m



Actual collection parameters may vary due to weather conditions and/or air traffic control (ATC) restrictions. EagleView stipulates the final accuracy of the dataset regardless of actual capture parameters.

Capture Parameters (nominal) – 0.5 m postings

Flight Altitude:	500m/1600ft
Point Spacing:	0.5m
Point Density:	4 points per square meter
Pulse Repetition Freq.:	50kHz
Scan Angle (+/-):	10.1 degrees
Scan Frequency:	70.1Hz
Swath Width:	177m
Overlap:	N/A
Vertical Accuracy:	9.25 cm RMSE _z bare earth 18.2 cm NSSDA Vertical Accuracy (95% confidence) – bare earth
Horizontal Accuracy:	35cm; RMSE
Returns:	Up to four per pulse
Intensity records:	Recorded for each return
Coordinate System:	Customer preferred system and units (must be specified and approved in advance of start of work).
Filtering:	Automated methods with manual review and clean up with the following minimum performance specifications: <ul style="list-style-type: none">• 95% of outliers removed• 95% of vegetation removed• 98% of buildings removed
Contour Interval	Meets or exceeds FEMA requirements to generate contours at a 1' interval. NOTE: While EagleView stipulates this accuracy, independent verification of this accuracy as well as additional independent reporting is usually required to qualify for FEMA funding. EagleView offers these services through an independent subcontractor for additional cost.

Deliverables:

- LiDAR Data
 - Tiled* LAS v1.2 files including Return Number and intensity attribute for each return
 - Duplicate points and 95% of outliers removed
 - Ground points classified via automated methods with manual review and clean up
 - 95% of vegetation features removed
 - 98% of buildings removed
 - Buildings and vegetation not classified separately
 - **NOTE:** LiDAR data deliverables will extend approximately 200m beyond the specified project area
- Raw GPS/INS data and laser range files with supporting information
- FGDC compliant metadata
- Estimated Data Sizes: 40-50 GB per 100 square miles (approximate)

DEM Bare Earth

ESRI Terrain

EagleView will convert the Bare Earth classified data contained in the LAS files to ESRI Terrain data as a fundamental step toward deriving subsequent bare earth terrain products. Developing the data in this manner will significantly enhance the delivery of data to the Customer and provide maximum flexibility for future use, updates, and edits. **Standard Hydrographic Breaklines (described below) will be incorporated into all terrain deliverables.** Additional breaklines may be developed and incorporated into the terrain at any time.

Digital Elevation Models (DEMs)

The standard DEM deliverable will be assumed to have a 10-foot grid cell size unless otherwise specified by the customer. EagleView will also develop a Hillshade from the DEM for visualization and cartographic mapping purposes.

Standard Hydrographic Breaklines

Breaklines are linear features that describe a change in the smoothness or continuity of a surface. As part of the baseline effort to create a DEM, EagleView will develop limited 3D breaklines for water feature boundaries and wide rivers and incorporate those into the ESRI Terrain data prior to generating any derived products. Hydrographic breaklines will be delineated using the LiDAR data with elevation values assigned from the LiDAR data, using best available aerial photography and the National Hydrography Dataset (NHD) as references.

Water bodies will be defined for the purposes of this task as being larger than 5m across, or greater than one (1) acre. Breaklines delineating the edge of water will be created for all such water bodies. Breaklines will not be developed for streams less than 5m across, also referred to in NHD as 'single line streams'.



The standard for water bodies in the USGS Specification is 100ft and two (2) acres respectively. 'Hydro-flattening', as defined in the USGS Specification, will be completed at a minimum on all water bodies meeting the USGS definition. This task is intended to meet or exceed the requirements for 'Hydro-flattening' in the USGS Specification.

For flat and level water bodies (ponds, lakes), a single elevation value will be assigned to the entire polygon and/or to every bank vertex. The entire water surface edge will be at or just below the immediately surrounding terrain. For streams and rivers, breaklines indicating flat and level bank-to-bank conditions (perpendicular to the apparent flow centerline) will be created, with the gradient along the bank to follow the immediately surrounding terrain. Monotonicity will be enforced on breaklines meeting the USGS Specification. Stream and river breaklines delineating the edge of water will stop at road crossings (i.e., culvert locations).

Bare earth LiDAR points that are within the design Nominal Point Spacing (NPS) of a breakline will be re-classified as 'Ignored Ground' once the breaklines have been completed. The design NPS of a LiDAR collection is typically between 1 and 2 meters, but may be greater or less depending on the collection specifications of the project.

The identification and prioritization of additional breaklines beyond those minimally described here represents a wide range of expectations and detail depending on specific project/customer needs and intended uses. Most customized uses of breaklines are appropriate for project specific purposes, such as hydraulic modeling, construction site design or transportation engineering. As such, additional breakline development options are offered below. Additional detailed breaklines can be developed and incorporated into the terrain data at any time.

Deliverables:

- Collection-wide point data (bare earth only) in ESRI multi-point format
- Collection-wide Terrain Data Model (bare earth) in ArcGIS TERRAIN format
- Collection-wide Digital Elevation Model (bare earth) in ArcGIS GRID format
- Collection-wide polyline files in ESRI Polyline Feature Class format
- Collection-wide Hillshade of the Bare earth DEM in ArcGIS format

Contours

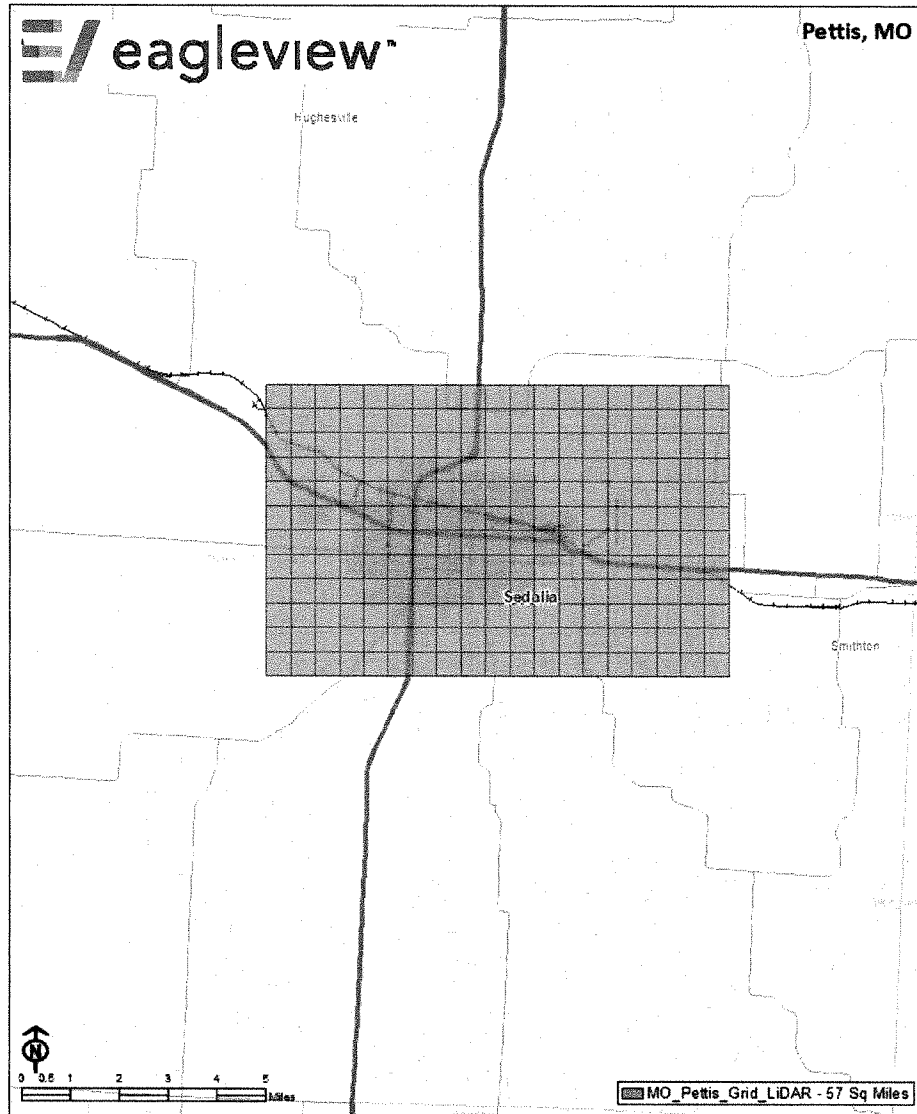
The range of available algorithms can result in significant differences in cartographic output quality for the generation of topographic contours. Some methods more accurately represent the point data, but result in a more angular and less cartographically pleasing output. Other methods will smooth the data to varying degrees but produce a much higher quality cartographic output. The customer will be given options, based on demo data, for having their collection area contours created from smoothed data or not-smoothed data.

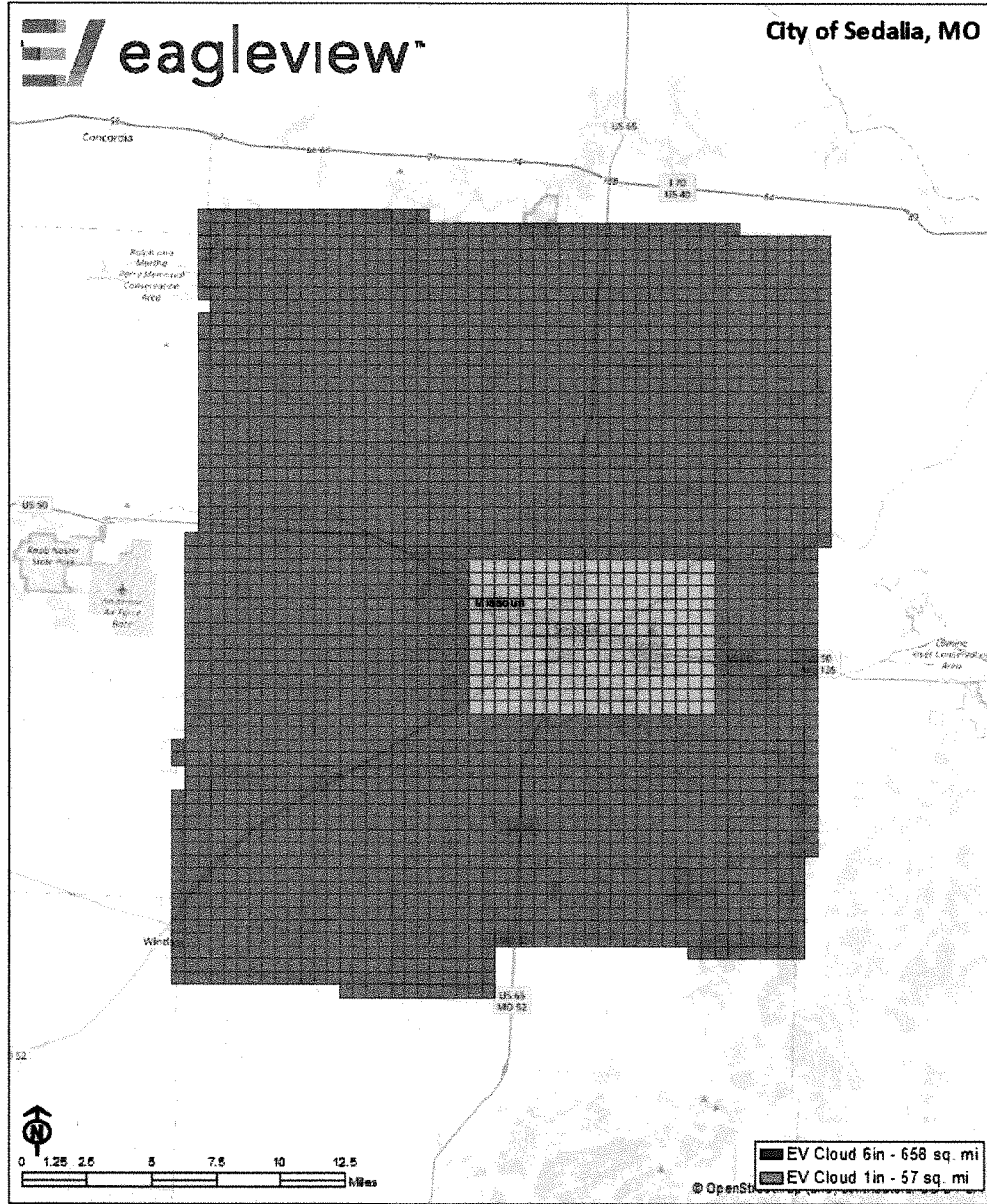
This task will result in vector (line) data and as such, tiling the data will be required because the vector files can be quite large. The output tiling scheme will correspond to the LiDAR tiles unless the customer requests a different tiling scheme in advance. Final tiled vector data will be seamless and free of edge effects. EagleView will establish elevation attributes to each contour line and identify 10, 20, and 50 ft. index contours unless otherwise specified by the Customer.

Deliverables:

- Tiled 1-foot or 2-foot* contour files in ESRI Polyline Feature Class format. (*NOTE: Contours will be created at maximum resolution supported by the collection as specified in Section A.)

AOI(S)





Contains information from OpenStreetMap, which is made available here under the Open Database License (ODbL): openstreetmap.org/copyright

[Signature page follows]



This Order Form is incorporated by reference into the Master Services Agreement between Pictometry International Corp. dba EagleView and Customer.

Pictometry International Corp. dba EagleView

Customer

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____



EXHIBIT B

SECURITY

1. Definitions.

- 1.1 “**Critical Issue**” means an issue that does, or has the potential to, compromise the confidentiality, integrity, availability, security, or privacy of Customer Confidential Information.
- 1.2 “**Security Incident**” means any (a) access to Customer’s Confidential Information in the possession or control of EagleView or any Subcontractors, by an unauthorized party or by an authorized party for unauthorized purposes; (b) unauthorized use of any such Confidential Information; or (c) event involving data or information that results in a material impact to EagleView’s services or to Customer.
- 1.3 “**Standards Body**” means any commercially recognized technology and or auditing standards organization, including but not limited to AICPA, ISO, ITIL, and NIST.
- 1.4 “**Subcontractor**” means a subcontractor of EagleView.

2. Payment Card Security Compliance. EagleView will meet the security requirements set forth in this Agreement or, alternatively, demonstrate and implement to Customer’s reasonable satisfaction appropriate compensating controls.

- 2.1 To the extent applicable, EagleView will: (a) take all steps necessary to maintain its status as a PCI DSS compliant; (b) promptly notify Customer if EagleView ceases to be PCI DSS compliant, explaining the cause for non-compliance and the target date for becoming compliant; and (c) annually provide to Customer its current PCI DSS Attestation of Compliance report upon request.
- 2.2 EagleView may elect to use an alternative to PCI DSS, should a commercially accepted framework approved by major credit card processors become available.
- 2.3 If EagleView learns of any Critical Issues, EagleView will use all reasonable efforts to remediate such Critical Issues promptly.

3. Data Security. EagleView will:

- 3.1 Upon request, provide to Customer a report identifying where Customer Confidential Information is processed and stored, and how access is controlled. For any material changes in data center hosting, including, without limitation, outsourcing of data center hosting, such report will be accompanied by the most recent report for such data center.
- 3.2 Not allow Customer Confidential Information to be disclosed, accessed, processed, or stored outside the United States, its territories, and possessions (“U.S.”) without notice to Customer, and will cooperate with Customer’s security assessment of such non-U.S. based activities. EagleView will be responsible for any such non-U.S. based activities and will ensure that such non-U.S. based activities are in compliance with applicable law and this Agreement, including, without limitation, all security requirements.
- 3.3 When transmitting and storing Customer Confidential Information, encrypt such information using encryption at rest and encryption in transit that is applied to such Customer Confidential Information and maintains its protection throughout the lifecycle of such Customer Confidential Information. Use encryption keys and key management techniques that comply with security industry standards published by a Standards Body.
- 3.4 Where practicable, store Customer Confidential Information in a manner that logically or physically separates the data from other EagleView customer data.
- 3.5 Ensure that Customer Confidential Information is not stored on any portable removable media (such as USB mass storage, external hard drives, and CD/DVDs), except as necessary to support the services provided under this Agreement and provided that such Customer Confidential Information is encrypted as described in Section 3.3.
- 3.6 Remove all Customer Confidential Information from any media taken out of service and destroy or securely erase such media to make it unreadable, undecipherable, and unrecoverable by any means consistent with data destruction practices recommended by a Standards Body.
- 3.7 Conduct a security risk assessment, based upon a Standards Body framework, of all EagleView’s Subcontractors. Ensure Subcontractors have and follow appropriate security processes and remediate any Critical Issues Promptly.



- 3.8 From time to time, EagleView may update its practices as described herein, but will not materially decrease the overall security of the Products and Services during the Term.
4. **Penetration Testing.**
- 4.1 No more than once per year while this Exhibit is in effect and with no less than thirty (30) days prior written notice to EagleView, and prior written approval by EagleView, Customer will be permitted to conduct a penetration test at Customer's expense, and targeted at sites or services directed by EagleView, in order to verify that EagleView has and continues to comply with the security and data requirements set forth in this Agreement. Customer may elect to use a qualified third-party vendor to conduct such penetration test. In no event will any such test exceed ten (10) business days in duration. Upon completion of such test, Customer will provide EagleView with a copy of the results of such test.
5. **Information Security Program.** Without limiting EagleView's obligation of confidentiality under this Agreement, EagleView will establish and maintain a written Information Security Program, together with adequate administrative, technical, and physical safeguards, to:
- 5.1 Ensure the confidentiality, integrity, and availability of all Customer Confidential Information that is accessed, processed, stored, or controlled by EagleView;
- 5.2 Take commercially reasonable efforts to protect against anticipated threats or hazards to the confidentiality, integrity, and availability of such Customer Confidential Information;
- 5.3 Maintain a vulnerability management program to protect hardware and software assets from known exploitable vulnerabilities that have an approved vendor/supplier patch or mitigation strategy;
- 5.4 Engage a third-party vendor to perform an annual penetration test. EagleView will also ensure all Critical Issues identified by such testing are remediated and retested promptly. Upon request, EagleView will provide Customer with a letter from the third-party stating that testing was performed, and all Critical Issues were addressed;
- 5.5 Protect against unauthorized access to or use of such Customer Confidential Information; and
- 5.6 Such written Information Security Program and administrative, technical, and physical safeguards must be no less rigorous than accepted industry practices (such as applicable security standards published by a Standards Body), and will ensure that all such safeguards, including the manner in which Customer Confidential Information is collected, accessed, used, stored, processed, disposed of, and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Agreement.
6. **Disaster Recovery and Business Continuity.** EagleView will maintain a backup of Customer Confidential Information, for an orderly and timely recovery thereof if access to or use of the services hereunder may be interrupted. EagleView will maintain a Restore Point Objective ("RPO") of one business day prior.
7. **Security Incident Process.** EagleView will use commercially reasonable efforts to notify Customer, whose data is known to be or suspected to be impacted, of any Security Incident within 72 hours of confirming that a Security Incident has occurred. Unless otherwise agreed to in writing, EagleView will remediate the cause of such Security Incident immediately.
- 7.1 Customer is responsible for providing EagleView with updated and accurate contact information.
- 7.2 EagleView agrees to fully cooperate with Customer in responding to the Security Incident, including, without limitation, by: (a) designating an employee to serve as primary point of contact and a backup who will maintain reasonable communication with Customer; and (b) assisting with any investigation of the nature or cause of such Security Incident.
- 7.3 If Customer determines that applicable law or regulation requires notification to any person of a Security Incident, such notification will be carried out by EagleView at EagleView's cost, including any costs for credit monitoring or other mitigation services, unless otherwise directed by Customer in writing; provided, however, that in all cases Customer will have sole control over the content, timing, and method of any such notification to persons affected by a Security Incident involving Customer's Confidential Information.
- 7.4 EagleView will maintain Security Incident handling and reporting processes that ensure: (a) relevant logs or other digital records related to the Security Incident are maintained until the Security Incident is declared fully remediated; (b) all Security Incidents are appropriately logged; (c) all such logs and information are appropriately protected to ensure the integrity of such logs and information.



- 8. Human Resources Security.** EagleView will: (a) unless agreed otherwise in the Agreement, perform criminal background checks covering charges and convictions of any felony or any misdemeanor involving violence, dishonesty, or breach of trust for all employees of EagleView and any Subcontractors who perform services at Customer facilities and/or access or process Customer Confidential Information and/or access Customer information systems; (b) ensure that physical and logical access for each employee of EagleView and of any Subcontractors are deactivated within twenty-four (24) hours of such employee's termination of employment or such Subcontractor's termination of engagement; and (c) provide regular security awareness training to all EagleView employees and require Subcontractors to provide such training for their employees.
- 9. Facility Requirements.** EagleView will employ physical security procedures to ensure that only authorized individuals have access to corporate facilities. Such procedures will include, but not be limited to, the use of video surveillance, cardkey access, and visitor authorization and supervision processes. Surveillance records will be maintained for at least 30 days.
- 10. Record Retention.** EagleView will retain Customer Confidential Information as long as EagleView is required to by applicable law.

Janeice Dodick

From: Jason Myers
Sent: Tuesday, October 31, 2023 8:21 AM
To: Janeice Dodick
Subject: FW: Eagleview Imagery Contract
Attachments: MO City of Sedalia_EV Cloud MSA_10-30-23.pdf

From: Devin Lake <dlake@sedalia.com>
Sent: Monday, October 30, 2023 4:53 PM
To: Jason Myers <JMyers@sedalia.com>; 'Joe Lauber' <jlauber@laubermunicipal.com>; 'Todd Smith' <tsmith@laubermunicipal.com>
Subject: FW: Eagleview Imagery Contract

Joe/Todd, could you review this contract for Monday's agenda?

Jason, can we please get this added to the Council Agenda for Monday?

Thanks!!

Devin Lake, CBO
Chief Building Official
dlake@sedalia.com
660-851-7637 – office
660-473-1623 – cell



From: Alexandra Stark <alexandra.stark@eagleview.com>
Sent: Monday, October 30, 2023 3:33 PM
To: Devin Lake <dlake@sedalia.com>
Subject: RE: Eagleview Imagery Contract

Devin,

Attached is the agreement for 1" and 6" with the updated payment terms. Signatures are required on pages 7 and 14. Please let me know if you have any questions.

Have a good afternoon.
Alex

Alexandra Stark
District Manager – Arkansas, Missouri, Oklahoma



M 660.322.0153
alexandra.stark@eagleview.com

From: Devin Lake <dlake@sedalia.com>
Sent: Tuesday, October 10, 2023 3:21 PM
To: Alexandra Stark <alexandra.stark@eagleview.com>
Subject: RE: Eagleview Imagery Contract

Yes, upstairs on the 2nd floor.

Devin Lake, CBO
Chief Building Official
dlake@sedalia.com
660-851-7637 – office
660-473-1623 – cell



From: Alexandra Stark <alexandra.stark@eagleview.com>
Sent: Tuesday, October 10, 2023 2:13 PM
To: Devin Lake <dlake@sedalia.com>
Subject: RE: Eagleview Imagery Contract

Absolutely, I will send a meeting invite shortly feel free to forward on.

Should I come to city hall?



Alexandra Stark
District Manager – Arkansas, Missouri, Oklahoma
M 660.322.0153
alexandra.stark@eagleview.com

From: Devin Lake <dlake@sedalia.com>
Sent: Tuesday, October 10, 2023 2:11 PM
To: Alexandra Stark <alexandra.stark@eagleview.com>
Subject: RE: Eagleview Imagery Contract

Sure, that will work!! If you don't mind, I will invite James Theisen from Pettis County to also join us?

Thanks!!

Devin Lake, CBO

Chief Building Official
dlake@sedalia.com
660-851-7637 – office
660-473-1623 – cell



SEDALIA
Let's Cross Paths

From: Alexandra Stark <alexandra.stark@eagleview.com>
Sent: Tuesday, October 10, 2023 2:06 PM
To: Devin Lake <dlake@sedalia.com>
Subject: RE: Eagleview Imagery Contract

Let's do this Friday at 10:30?



eagleview

Alexandra Stark
District Manager – Arkansas, Missouri, Oklahoma
M 660.322.0153
alexandra.stark@eagleview.com

From: Devin Lake <dlake@sedalia.com>
Sent: Tuesday, October 10, 2023 2:03 PM
To: Alexandra Stark <alexandra.stark@eagleview.com>
Subject: RE: Eagleview Imagery Contract

Yes, that would work. I am available most anytime, however, I will be out of the office next week starting at noon on Tuesday. I could meet anytime the rest of this week, next Monday or sometime before noon on Tuesday.

Thanks!!

Devin Lake, CBO
Chief Building Official
dlake@sedalia.com
660-851-7637 – office
660-473-1623 – cell



SEDALIA
Let's Cross Paths

From: Alexandra Stark <alexandra.stark@eagleview.com>
Sent: Tuesday, October 10, 2023 1:56 PM
To: Devin Lake <dlake@sedalia.com>
Subject: RE: Eagleview Imagery Contract

Hey Devin,

There are a lot of details that go into the explanation of the pricing. I feel that an in-person meeting would best suit both parties in figuring out how to move forward. Do you have any time this week or next for me to make an in person visit?



Alexandra Stark
District Manager – Arkansas, Missouri, Oklahoma
M 660.322.0153
alexandra.stark@eagleview.com

From: Devin Lake <dlake@sedalia.com>
Sent: Tuesday, October 10, 2023 1:03 PM
To: Alexandra Stark <alexandra.stark@eagleview.com>
Subject: RE: Eagleview Imagery Contract

Alex,

The base bid for this RFP was for a 6-year contract for a total of 3 flights. The base bid amount was \$225,624 so that should be spread out over the 3 flights.

What you are saying below is significantly more than we have paid in the past. Our last contract was for \$45,625 per year. This is over double that amount for the same quality of imagery that we received for the 2022 flight. Maybe there is some confusion?

Thanks!!

Devin Lake, CBO
Chief Building Official
dlake@sedalia.com
660-851-7637 – office
660-473-1623 – cell



From: Alexandra Stark <alexandra.stark@eagleview.com>
Sent: Tuesday, October 10, 2023 12:52 PM
To: Devin Lake <dlake@sedalia.com>
Subject: RE: Eagleview Imagery Contract

Hey Devin,

Nice catch on the payment terms, they aren't correct on the agreement. My apologies. However, the \$225,624 would be for one Project 1, if the county wanted to move forward with project 2 and 3 it would be an additional \$225,624/project.

Payment terms should be:

Year 1: \$112,812+ \$64,740.60 LiDAR = \$177,552
Year 2: \$112,812
Year 3: \$112,812 – Project 2
Year 4: \$112,812

Year 5: \$112,812 – Project 3

Year 6: \$112,812

I can request the April 1st invoice date as well.



Alexandra Stark
District Manager – Arkansas, Missouri, Oklahoma
M 660.322.0153
alexandra.stark@eagleview.com

From: Devin Lake <dlake@sedalia.com>
Sent: Tuesday, October 10, 2023 12:38 PM
To: Alexandra Stark <alexandra.stark@eagleview.com>
Subject: RE: Eagleview Imagery Contract

Hi Alex,

I just want to clarify with you that the total contract for all 6 years is \$225,624.00? In our previous contracts we paid ½ of each flight yearly so it broke it out by year.

Year 1: \$37,604 + \$64,740.60 LiDAR = \$102,344.60

Year 2: \$37,604

Year 3: \$37,604

Year 4: \$37,604

Year 5: \$37,604

Year 6: \$37,604

We received the invoices for each year on April 1 which is the beginning of our fiscal year. Could you have the contract reflect these amounts? And yes, we will be doing the imagery and LiDAR in March 2024.

Thanks!!

Devin Lake, CBO

Chief Building Official

dlake@sedalia.com

660-851-7637 – office

660-473-1623 – cell



SEDALIA
Let's Cross Paths

From: Alexandra Stark <alexandra.stark@eagleview.com>
Sent: Tuesday, October 10, 2023 10:58 AM
To: Devin Lake <dlake@sedalia.com>
Subject: Eagleview Imagery Contract

Good Morning, Devin!

Attached is the long awaited imagery agreement. Please let me know if you have any questions.

I also want to confirm that county would like the Imagery and LiDAR flown in March of 2024?

Thank you!
Alex



Alexandra Stark
District Manager – Arkansas, Missouri, Oklahoma
M 660.322.0153
alexandra.stark@eagleview.com

AFFIDAVIT

**COMPLIANCE WITH THE WORK AUTHORIZATION LAW
(as required by Section 285.530, Revised Statutes of Missouri)**

As used in this Affidavit, the following terms shall have the following meanings:

EMPLOYEE:

Any person performing work or service of any kind or character for hire within the State of Missouri.

FEDERAL WORK AUTHORIZATION PROGRAM:

Any of the electronic verification of work authorization programs operated by the United States Department of Homeland Security or an equivalent federal work authorization program operated by the United States Department of Homeland Security to verify information of newly hired employee, under the Immigration Reform and Control Act of 1986 (IRCA), P.L. 99-603.

KNOWINGLY:

A person acts knowingly or with knowledge,

- (a) with respect to the person's conduct or to attendant circumstances when the person is aware of the nature of the person's conduct or that those circumstances exist; or
- (b) with respect to a result of the person's conduct when the person is aware that the person's conduct is practically certain to cause that result.

UNAUTHORIZED ALIEN:

An alien who does not have the legal right or authorization under federal law to work in the United States, as defined in 8 U.S.C. 1324a(h)(3).

Before me, the undersigned Notary Public, in and for the County of Monroe, State of New York, personally came and appeared Robert Locke
(Name)
President, of the Pictometry International Corp., dba Eagleview
(Position) (Name of the Company)

(a corporation) and after being duly sworn did depose and say that all provisions and requirements set out in Chapter 285.530 (2) Missouri Revised Statutes, have been fully satisfied and there has been no exception to the full and complete compliance with said provisions and requirements.

Contractor is enrolled in and participates in a federal work authorization program with respect to the employees working in connection with the following services contracted between Contractor and the City of Sedalia for geospatial software, aerial imagery, contours and analytics.

Contractor does not knowingly employ any person who is an unauthorized alien in connection with the contracted services set forth above.

Attached hereto is documentation affirming Contractor's enrollment and participation in a federal work authorization program with respect to the employees working in connection with the contracted services as reflected in the EagleView Master Services Agreement Order # LC-10004728.

RW Locke

(Signature)

Subscribed and sworn to me this 16th day of November, 2023.

My Commission expires: February 14, 2027

JAMIE L ANTHONY
NOTARY PUBLIC-STATE OF NEW YORK
No. 01AN0001505
Qualified in Monroe County
My Commission Expires 02-14-2027

Jamie Anthony
Notary Public