SECOND AMENDATORY AGREEMENT

THIS SECOND AMENDATORY AGREEMENT is made and entered into by and between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the "City"), and **RUNBECK ELECTION SERVICES INC.**, an Arizona corporation, registered to do business in Colorado, whose address is 2800 S. 36th Street, Phoenix, Arizona 85034 (the "Contractor").

W I T N E S S E T H:

WHEREAS, the City and the Contractor previously entered into an Agreement dated September 6, 2022 relating to the acquisition of elections software, hardware, and related maintenance services, and a first Amendatory Agreement dated October 27, 2022 (collectively, the "Agreement"); and

WHEREAS, the City has determined to purchase additional equipment, to extend the term of the Agreement, and to make such other amendments as are set forth below;

NOW, THEREFORE, in consideration of the premises and the mutual covenants and obligations herein set forth, the parties agree as follows:

1. The revised Scope of Work is attached hereto and incorporated herein as **Exhibit A-2** and all references to "Exhibit A and A-1" are hereby amended to read "**Exhibit A-2**".

2. The revised Software License is attached hereto and incorporated herein as **Exhibit B-2** and all references to "Exhibit B" are hereby amended to read "**Exhibit B-2**".

3. The revised Equipment List and Prices is attached hereto and incorporated herein as **Exhibit D-2** and all references to "Exhibit D" and "Exhibit D-1" are hereby amended to read "**Exhibit D-2**".

4. Paragraph 4 of the Agreement, entitled "TERM", is hereby amended to read as follows:

"**4. <u>TERM</u>:** The term of this Agreement shall commence on August 1, 2022, and shall expire on December 31, 2027 (the "Term"). The Contractor shall complete the corresponding annual work and any work in progress as of the expiration date unless the work is earlier terminated by the Clerk."

5. Paragraph 5 of the Agreement, entitled "COMPENSATION AND PAYMENT," is amended to read as follows:

"5. COMPENSATION AND PAYMENT:

A. Fee: The fee for the software, hardware, services, and maintenance services described in Exhibits A-2, B-2, C, and D-2 is not to exceed One Million Two Hundred Ten Thousand Five Hundred Thirty-Six Dollars and no cents ($1,210,536.00) (the "Fees"). The Fees shall be paid pursuant to the City's Prompt Payment Ordinance and in accordance with the Payment Milestones in Exhibits A-2, B-2, and D-2 and as invoiced for services provided at the rates in Exhibit C. Invoicing and payment thereon may not exceed either the rates or the budgets in Exhibits A-2, B-2, C, and D-2.

B. Reimbursement Expenses: The Fees specified above include all expenses, and no other expenses shall be separately reimbursed hereunder.

C. Invoicing: Contractor must submit an invoice which shall include the City contract number, clear identification of the deliverable that has been completed, and other information reasonably requested by the City. Payment on all uncontested amounts shall be made in accordance with the City's Prompt Payment Ordinance.

D. Maximum Contract Liability:

(i) Notwithstanding any other provision of the Agreement, the City's maximum payment obligation for the goods and services under this Agreement will not exceed One Million Two Hundred Ten Thousand Five Hundred Thirty-Six Dollars and no cents ($1,210,536.00) (the "Maximum Contract Amount"). The City is not obligated to execute an Agreement or any amendments for any further services, including any services performed by Contractor beyond that specifically described in **Exhibits A-2, B-2, C, and D-2.** Any services performed beyond those in Exhibits A-2, B-2, C, and D-2 are performed at Contractor's risk and without authorization under the Agreement.

(ii) The City's payment obligation, whether direct or contingent, extends only to funds appropriated annually by the Denver City Council, paid into the Treasury of the City, and encumbered for the purpose of the Agreement. The City does not by the Agreement irrevocably pledge present cash reserves for payment or performance in future fiscal years. The Agreement does not and is not intended to create a multiple-fiscal year direct or indirect debt or financial obligation of the City."

6. Paragraph 39 of the agreement, entitled "NO EMPLOYMENT OF A WORKER WITHOUT AUTHORIZATION TO PERFORM WORK UNDER THE AGREEMENT" is hereby deleted in its entirety and replaced with:

"**39. [RESCINDED].**"

7. Except as herein amended, the Agreement is affirmed and ratified in each and every particular.

Remainder of page left intentionally blank.

Contract Control Number: CLERK-202369075-02
Contractor Name: RUNBECK ELECTION SERVICES INC

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of:

SEAL

CITY AND COUNTY OF DENVER:

ATTEST:

By: _____

_____

APPROVED AS TO FORM:

Attorney for the City and County of Denver

By: _____

REGISTERED AND COUNTERSIGNED:

By: _____

By: _____

Contract Control Number: CLERK-202369075-02
Contractor Name: RUNBECK ELECTION SERVICES INC

By: DocuSigned by: _____
894F17320B0C4D2...

Name: Rizwan Fidai
(please print)

Title: Vice President of Sales
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)

EXHIBIT A-2

STATEMENT OF WORK AGREEMENT TO UPDATE SECURITY ON AGILIS SYSTEMS

Services Performed by: Runbeck Election Services
2800 S 36th St
Phoenix, AZ 85034

Client Name: Denver Elections Division, Office of the Clerk & Recorder
200 W 14th Ave
Denver, CO 80204

This Statement of Work (SOW) is issued pursuant to the Purchase Order and Service Contract for the Agilis Ballot Sorting Machine between the Denver Election Division ("Client") and Runbeck Elections Services ("Contractor") effective October 1, 2022 (the "Agreement").

This SOW is subject to the terms and conditions contained in in the Agreement between the parties and is made a part thereof. Any term not otherwise defined herein shall have the meaning specified in the Agreement.

The Exhibit to this SOW, if any, shall be deemed to be a part of hereof. In the event in of any inconsistencies between the terms of the body of this SOW and the terms of the Exhibit hereto, the terms of the body of this SOW shall prevail.

Scope of Work

The Contractor shall bring Agilis hardware and software to comply with the City and County of Denver's Internet of Things policy (attachment Exhibit A-2, part 2) prior to December 31, 2026.

Expenses/Fees

All expenses related to improvements to the hardware and software shall be considering part of the purchase price. The client shall not be charged additional amounts over those that are agreed upon in the purchase price and the contract price for the service agreements and warrantee.

In the case of non-conformance to this Agreement, the Agilis unit will be removed from the City and County system.

Internet of Things (IoT) Device Policy	
What:	To provide direction and governance to City Departments and Agencies and their vendor partners to successfully manage operation of IoT Devices and their associated risks throughout the devices' Lifecycles.
Why:	IoT Devices are advancing how the City operates using smart or smarter technologies. These devices are changing the cybersecurity and privacy risk landscape for the City. These risks can be mitigated in three ways: (1) protect device security, (2) protect data security, and (3) protect individuals' privacy.
How do we communicate/implement:	Communications plan jointly developed by the IGC and Technology Services. Plan implemented by Technology Services.
How do we measure success/compliance:	Success of this program can be indirectly measured through: (1) the ability of the City to innovate and increase performance using smart or smarter devices, and (2) through audit and policy compliance.
IGC Reviewers:	IoT IGC Working Group and Committee *en banc*

Policy Control Information	
Executive Sponsorship	Information Governance Committee
Related Policies	
Effective Date	June 5, 2020

Purpose

The Internet of Things (IoT) is an umbrella term for the rapidly evolving and expanding collection of diverse technologies that both connect to a network or the Internet and interact with the physical world. IoT Devices are the logical progression of combining the worlds of Information Technology (IT) and Operational Technology (OT). Many IoT Devices are the result of the convergence of mobile computing, cloud computing, embedded systems, industrial controls, low-priced hardware, and other technological advances. IoT Devices provide functionality, data storage, and network connectivity to devices that previously lacked them, fostering innovation through general efficiencies and economies; real-time or near-time control of systems and their environment; and the ability to better anticipate future events.

The City is already using large number of IoT Devices. It is necessary to consider how these current devices and any future IoT Devices will affect the City's cybersecurity, privacy, and infrastructure risks, and how those risks might differ from conventional information technology. Additionally, IoT

Devices may have unforeseen and unintended consequences upon the City's continuity of government, business operations, and critical infrastructure programs; incident management and operational coordination; public information and warning; emergency planning; as well as community preparedness and post-disaster recovery coordination. The purpose of this policy is to provide direction and governance to City Agencies and Departments and their vendor partners to successfully manage the operation of IoT Devices and associated risks.

Scope

This policy applies to all City Agencies and Departments, including auxiliary units and external business or organizations, that use or provide IoT Devices to the City and County of Denver.

Executive Sponsorship

Executive sponsorship for this document comes from Information Governance Committee and City and County of Denver Executive Order 143, as amended.

Policy

1. Vendors or contractors that provide an IoT Device to the City shall ensure and provide attestation that the IoT Devices provided:
    1.1. do not knowingly contain any Hardware, Software, or Firmware component with any restriction, known Security Vulnerability, or other exploitable defects as listed in:
        1.1.1. Federal Acquisition Regulations (FAR) or active FAR Circulars (Code of Federal Regulations, 48 C.F.R.);
        1.1.2. the National Vulnerability Database (NVD) of NIST;
        1.1.3. any additional database selected by Technology Services that tracks Security Vulnerabilities, defects, or restrictions, that is credible, and is similar to the FAR and NVD; and
    1.2. ensure that data is properly protected while in-transit and at-rest on the device using Strong Cryptography by default; and
    1.3. are only capable of accepting Properly Authenticated Updates from the vendor to the exclusion of all other methods (for all Software or Firmware components of the devices); and
    1.4. use only non-deprecated and current industry-standard protocols and technologies for functions including, but are not limited to:
        1.4.1. communications, such as standard ports for network traffic;
        1.4.2. Strong Cryptography;
        1.4.3. interconnection with other devices or peripherals; and

1.5. do not include any Fixed or Hard-Coded Credentials used for remote administration, the delivery of updates, or communication; and

1.6. have mechanisms to prevent unauthorized and improper physical and logical access to, usage of, and administration of the device by people, processes, and other computing devices; and

1.7. have mechanisms to monitor and analyze the device activity for signs of incidents involving security and improper use; and

1.8. have mechanisms to maintain a current, accurate inventory of all IoT Devices and their relevant characteristics throughout the devices' Lifecycle.

2. Vendors or contractors that provide an IoT Device to the City shall promptly notify the City of any known Security Vulnerabilities or other defects subsequently disclosed to the vendor by a security researcher or of which the vendor or contractor becomes aware for the duration of the agreement.

3. IoT Device Software or Firmware components shall be promptly updated or replaced, consistent with other provisions of the governing terms of support, in a manner that allows for any future Security Vulnerability or other defect in any part of the Software or Firmware to be patched in order to fix or remove a vulnerability or defect in the Software or Firmware component as a Properly Authenticated Update.

4. Vendors or contractors that provide an IoT Device to the City shall provide a patch, repair, or replacement in a timely manner in respect to any new Security Vulnerability or other defect discovered through any of the databases as described in §1.1 or from notifications in §2 in the event the vulnerability cannot be remediated through an update as described in §3.

5. Vendors or contractors that provide an IoT Device to the City shall provide the City with general information on the ability of the device to be updated, such as:

5.1. the manner in which the device received security updates;

5.2. the anticipated timeline for ending security support associated with the network-connected device;

5.3. formal notification six (6) months prior to when the security support will cease; and

5.4. any additional information required by the City or recommended by industry best-practices.

6. City Agencies and Departments shall maintain continuous and non-lapsing support and maintenance over the IoT Devices' Lifecycle that provide for Properly Authenticated Updates of Security Vulnerabilities and other defects on all devices that are within their span of control.

7. City Agencies and Departments shall securely and uniformly configure and properly deploy and operate all IoT Devices, including proper use of mechanisms in §1.6, §1.7, and §1.8, on all devices that are within their span of control.

8. In the event that a City Agency or Department reasonably believes the procurement of an IoT Device that is consistent with §1 through §5 would be unfeasible or economically impractical, the Agency or Department may request a waiver to this policy from the Information Governance Committee or its delegate in order to purchase or otherwise use a non-compliant IoT Device with compensating controls to mitigate the cybersecurity, privacy, and infrastructure risks as well as address any other impacts the device may impose. These compensating controls may include:

8.1. network segmentation or micro-segmentation;

8.2. the adoption of system-level security controls, including but not limited to operating system containers and micro-services;

8.3. multifactor authentication or other cryptographic methods;

8.4. intelligent network solutions and edge systems, such as gateways or proxies, that can isolate, disable, or remediate the IoT Device's non-compliance; and

8.5. additional redundancy or continuity of operation mechanisms.

9. Technology Services may stipulate additional requirements for management and use of non-compliant devices regardless of the method of acquisition or any type of grandfather clause to address the long-term risk of any active non-compliant IoT Devices. These requirements may include:

9.1. deadlines for the removal, replacement, or disabling of non-compliant devices (or their network connectivity);

9.2. defining the minimal requirements for compensating controls to ensure the integrity or security of the non-compliant device.

10. If an existing credible and recognized third-party security standard for an IoT Device provides an equivalent or greater level of security to that described in §1 through §5, the City may allow the vendor or contractor to demonstrate compliance with that standard in lieu of the requirements under §1 through §5 of this policy. Vendors or contractors that provide an IoT Device to the City shall provide third-party certification and attestation that the device complies with the security requirements of the industry certification method of the third party.

Definitions

The following terms are used in this policy:

Firmware: a computer program and the data stored in hardware, typically in read-only memory (ROM) or programmable read-only memory (PROM), such that the program and data cannot be dynamically written or modified during execution of the program.

Fixed or Hard-Coded Credential: a value, such as a password, token, cryptographic key, or other data element used as part of an authentication mechanism for granting remote access to an information system or its information, that is:

a) established by a product vendor or service provider; and
b) incapable of being modified or revoked by the City or vendor partner lawfully operating the information system, except via a Firmware update.

Hardware: the physical components of a device

Interface Capability: the capability of a device that enables device interactions (*e.g.*, device-to-device communication, human-to-device interaction). These types of Interface Capabilities include:

a) Application Interface: the ability for other computing devices to communicate with an IoT Device through an IoT Device application. An example of an application interface capability is an application programming interface (API).
b) Human User Interface: the ability for an IoT Device and people to communicate directly with each other. Examples of Human User Interfaces include: touch screens, haptic devices, microphones, keypads, multifunction printers (*e.g.*, touch screen), and cameras.
c) Network Interface: the ability for an IoT Device to interface with a communication network for the purpose of communicating data to or from an IoT Device. A network interface capability includes both Hardware and Software. Examples of Network Interfaces include: 802.3 (ethernet), 802.11 (WiFi), WiMAX, ISO/IEC 18000 (RFID), ECMA-340 & ISO/IEC 18092 (NFC), 802.15 (Bluetooth), Long-Term Evolution (LTE), IMT-2020 (5G), Z-Wave, and 802.14 (ZigBee).

Internet of Things (IoT) Device: The full scope of the Internet of Things is not precisely defined by the industry; it is clearly vast. Each City Agency or Department may have its own type of IoT Devices, such as: traffic and smart road technologies, and underground tank monitoring technologies in Transportation & Infrastructure; smart LED lighting and smart landscape watering in Parks and Recreation; service kiosks in Human Services; building automation devices and electronic door locks in General Services; smart voting and smart petitions in Elections; garage door automation in Denver Fire Department; and video sensors and gunshot detection systems in the Denver Police Department; air quality and environmental monitoring devices in Public Health & Environment; not to mention smart televisions, queue management, and employee time clocks in Technology Services. For the purposes of this policy, the term "IoT Device" means a device that:

a) is a Network-Connected Device, and
b) has one or more of the following capabilities:
   i. Transducer Capability,
   ii. Interface Capability,
   iii. Supporting Capability.

Lifecycle: activities associated with an IoT Device that fully encompass the device's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its decommissioning and disposal.

Network-Connected Device: a device that:

a) is capable of connecting to and is in regular connection with any type of City network or the Internet; and
b) has computer processing capabilities that can collect, send, or receive data

Properly Authenticated Update: an update, remediation, or technical fix to a Hardware, Firmware, or Software component issued by a product vendor or service

	provider used to correct particular problems with the component, and that, in the case of Software or Firmware, contains some method of authenticity protection utilizing Strong Cryptography, such as a digital signature, so that unauthorized updates can be automatically detected and rejected.
Security Vulnerability:	any attribute of Hardware, Firmware, Software, process, or procedure or any combination of these factors that could enable or facilitate the defeat or compromise of the confidentiality, integrity, or availability of an information system or its information or physical devices to which it is connected.
Software:	a computer program and associated data that may be dynamically written or modified.
Strong Cryptography:	the current and promulgated cryptographic standards and mechanisms as defined by the National Institute of Standards and Time (NIST). Any cryptographic standard or mechanism that has been deprecated or otherwise removed from the current promulgated standards and mechanisms shall not be grandfathered or otherwise considered compliant.
Supporting Capability:	the capability of a device to provide functionality that supports the other IoT capabilities. Examples of Supporting Capabilities include, but are not limited to: device management, cybersecurity, and identity (*e.g.*, PKI certificates or other identification tokens) capabilities.
Transducer Capability:	the capability of a device to interact with the physical world and serve as the edge between digital and physical environments. Transducer capabilities provide for the ability for a Network-Attached Device to interact directly with physical entities of interest. The two types of Transducer Capabilities are: a) Sensing: is the ability for a device to provide an observation of an aspect in the physical world in the form of measurement data. Examples include: temperature measurement, radiographic imaging, optical sensing, audio sensing, multifunction printer (*e.g.*, scanner), or door position. b) Actuating: is the ability to change something in the physical world. Examples include: heating coils, cardiac electric shock delivery, electronic door locks, servo motors, unmanned aerial vehicle operation, robotic arms, multifunction printer, electronic valves and switches.

EXHIBIT A - 2

MAINTENANCE SERVICES

Software Maintenance

- 7X24 technical software support hotline during declared election cycles
- Installation of all software updates
- Testing and validation of all software updates
- License and Support Fee

Hardware Maintenance

- 7X24 technical support hotline during declared election cycles
- License and Support Fee
- Client also agrees to allow Runbeck employees access to the equipment, when requested, during normal working hours

Repair Services

During the term of the Agreement, as set forth in Section 27 thereof, should any component of the Equipment, to include hardware and software items listed above, become damaged and require repair as a result of Client's actions, Client agrees to pay Runbeck a Repair Fee of $150.00 per hour.

Election Data

At the conclusion of the election, Runbeck will provide phone assistance with the export of all election data from the Equipment. This data will be retained by the Client. Media (DVDs, jump drives, etc.) for this data will be provided by the Client. Client is responsible for the retention of this media and data.

Training

Additional training requires an on-site support fee, indicated below.

Materials management

- Client is responsible for any pre-election inventory of Equipment consumables
- Client is responsible for purchasing consumables, the shipping and taxes associated with such consumables
- Client is responsible for providing storage area that provides adequate space and maintains proper environmental conditions for stocking of supplies. Client must provide Runbeck notice of election at least 75 days in advance of 1st day that services will be required. Client is responsible for installation of consumables while operating the Equipment during an election cycle

On-Site Support Fees

Optional dedicated on-site support and/or training (does not include election set-up or routine maintenance) will be billed at a rate of $1,750.00 for the first day (an eight-hour workday) and $1,500 for each additional eight-hour workday. The amount billed shall be due and payable within thirty (30) days of the invoice date. This service is subject to availability.

Other

Shipping Fees

Shipping fees will apply as goods may be purchased and need to be shipped to the jurisdiction. Shipping fees are the sole responsibility of the Client.

End of Contract Options – Subject to Section 27 of the Agreement, Client May:

- Renew with existing system, for which new Usage, License, Maintenance and Service agreements shall apply
- Renew with upgrade to existing system, for which new Usage, License, Maintenance and Service agreements shall apply

Software

- Agilis Verus Pro
    - ASR/ASV (automatic signature recognition / verification)
    - $50,000 Parascript ASR/ASV license cost per year as per signed agreement
    - Alternate ASR/ASV: $15,000 RAFF license cost per year

EXHIBIT B -2

SOFTWARE LICENSE

Grant and Scope of License

A. Grant of License. Subject to Client's discharge of its material duties under this Agreement, to include the timely payment of any fees due hereunder, Runbeck hereby grants to Client an irrevocable, non-exclusive right and license to install, display and use the Software pursuant to the terms of the Agreement. For the avoidance of doubt, the license granted under this clause shall become revocable in the event that Client materially breaches this Agreement and Client fails to cure within the proscribed cure period.

B. Title. Runbeck shall at all times retain title to the Software provided by it hereunder and Runbeck does not convey any proprietary interest therein to Client.

C. Updates. For payment of the required fees by the Client as set forth herein and, in the Agreement, Runbeck shall provide to Client updates of any Software licensed hereunder at no additional charge and continue to maintain the Software in accordance with the requirements of the attached Agreement as long as Client continues to pay annual license and support services fees with respect to such Software.

D. Breach. In the event Client commits a material breach of its obligations under this Agreement, to expressly include failure to timely pay any fees due hereunder, and Client fails to cure the breach within sixty (60) days after receiving notice thereof, Runbeck may terminate this Agreement, and the license hereunder, immediately upon delivery of written notice to Client.

Annual License and Support Fee

A. Fees. Runbeck will invoice Client for the annual License and Support Fee ("Fee"), set forth in Exhibit "D" to the Agreement. The annual License and Support Fee for the first year of this Agreement is included in the purchase and installation price of the Equipment. All payments of this Fee shall be made annually on each successive anniversary term of the Agreement, for as long as Client continues to use referenced Software. The license for the Software entitles Client to the warranties set forth in the "Warranties" section below but does not otherwise entitle Client to receive maintenance and support or updates to the Software. The annual License and Support Fee is subject to an annual adjustment not to exceed five percent (5%).

B. Invoices. Runbeck's invoices will conform to the format requirements of the Client. Client will pay Runbeck's valid invoices within thirty (30) days after receipt.

Delivery, Installation and Acceptance

A. Estimated Shipping. Runbeck agrees to ship the Software to the location, and on or about the Estimated Shipping date, set forth in Exhibit "D".

    i. Cost – TBD, not to exceed $5,000.00

B. Installation. Runbeck agrees to install the Software ready for use and in good working order and render said Software Functional as a part of the fully Functional System at the applicable location as soon as practicable after delivery, but in no event more than ten (10) days after delivery.

    i. Cost - $2,500.00

C. Acceptance. Acceptance Testing and Acceptance of the Software as a part of the System shall be in accordance with the provisions of the attached Agreement.

Training

If Client's personnel require training in order to properly use the Software and System, Runbeck will provide such training for all users designated by Client, at a time agreed to by the Parties. All initial training by Runbeck in the proper use of the Software and System shall be at no additional charge unless a fee for such training is otherwise agreed upon and funds appropriated and certified as available for such purposes by the Client in accordance with the Agreement.

i. Cost - $2,500.00 (on-site training per day)

Maintenance of Software; Term and Termination

A. Maintenance Services. During the term of this Agreement and subject to payment of any required fees by the Client, Runbeck agrees to provide maintenance and support services for the Software ("Maintenance Services").

B. Software Updates. Runbeck shall provide updates to the Software as they become available. Installation of Software updates will include testing and validation of the updated Software. Runbeck will provide the Client with a toll- free support hotline number that may be used to obtain assistance with the Software during the term of this Agreement, subject to payment of any required fees.

Warranties

A. In addition to any warranties which may be contained in the Agreement, Runbeck provides the following warranties:

i. Non-Infringement. Runbeck warrants that Runbeck owns the Software, including all associated rights, and has the right to grant Client the licenses provided pursuant to this Agreement, free from all liens, claims, encumbrances, security interests and other restrictions. Runbeck warrants that the Software does not, and use of the Software will not; infringe any valid patents, copyrights, trademarks, trade secrets, or other proprietary rights of any third parties.

ii. Correction of Defects. In the event of discovery of any material defect in the Software, Client agrees to provide Runbeck with sufficient detail to allow Runbeck to verify and reproduce the error, and Runbeck shall use reasonable diligence to correct such defect. Runbeck shall use its reasonable efforts to promptly respond and thereafter to diagnose and correct the material defect. Runbeck is not responsible for any error in the Software that has been modified by Client without Runbeck's prior written consent..

iii. Performance of Services. Runbeck represents and warrants that all services provided by Runbeck to Client will be performed in a timely, competent, and skillful manner. Runbeck further represents and warrants that it has a sufficient number of competent, qualified employees to provide the Services to support the Software.

EXHIBIT D - 2

EQUIPMENT LIST AND PRICES

Agilis Sorting System includes: $275,000.00

- Agilis Sorting System
- 2 Stackers, 8 pockets
- Label printer
- Auto Thickness Detect
- Agilis Sorting Software

Optional Stacker, 4 Pockets: $25,000.00 / EA
Optional Automatic Opener: $25,000.00

Auto Signature Recognition / Auto Signature Verification (ASR / ASV) Options:
(Option 1) Parascript $50,000.00*
(Option 2) RAFF $15,000.00*
(*first year price)

INVOICE SCHEDULE

Invoice To:
Denver Elections Division
Attn: Administration Dept.
200 W. 14th Ave., Ste. 100
Denver, CO 80204

Contract Period: August 1, 2022 – December 31, 2027
Estimated Ship Date: Unit #2: TBD

A. Option 1 fee schedule for Parascript ASV Years 1-4; RAFF ASV Year 5:

License Fees, Maintenance and Support Type of Service	Year 1 (Aug 2022-2023)	Year 2 (2023-2024)	Year 3 (2024-2025)	Year 4 (2025-2026)	Year 5 (2026-2027)
	Agilis Unit #1	**Agilis Unit #2**			
Agilis Sorting System	$275,000	$275,000			
In-line Envelope Opener	$25,000	$25,000			
Additional 4 pocket Stacker 2 x $25,000/each	$50,000	n/a			
Training (on-site 6-8 hours)	$1,500	$2,500			
Installation	$1,500	$2,500			
Set up and Integration	Included	Included			
Shipping	$3,780	$5,000 (est.)			
License and Support Fee Unit 1	Included	$35,000	$36,050	$37,131	$38,244
License and Support Fee Unit 2		Included	$35,000	$36,050	$37,131
ASV Annual License Fee "Parascript" Years 1-4	$50,000	$50,000	$60,000	$63,000	
ASV Annual License Fee "Raff" Year 5					$15,000
Total Year 1 2022	$406,780				
Total Year 2 2023		$395,000			
Total Year 3 2024			$131,050		
Total Year 4 2025				$136,181	
Total Year 5 2026					$90,375

B. Option 2 fee schedule for Parascript ASV Years 1-5:

License Fees, Maintenance and Support **Type of Service**	**Year 1** **(Aug 2022-2023)**	**Year 2** **(2023-2024)**	**Year 3** **(2024-2025)**	**Year 4** **(2025-2026)**	**Year 5** **(2026-2027)**
	Agilis Unit #1	**Agilis Unit #2**			
Agilis Sorting System	$275,000	$275,000			
In-line Envelope Opener	$25,000	$25,000			
Additional 4 pocket Stacker 2 x $25,000/each	$50,000	n/a			
Training (on-site 6-8 hours)	$1,500	$2,500			
Installation	$1,500	$2,500			
Set up and Integration	Included	Included			
Shipping	$3,780	$5,000 (est.)			
License and Support Fee Unit 1	Included	$35,000	$36,050	$37,131	$38,244
License and Support Fee Unit 2		Included	$35,000	$36,050	$37,131
ASV Annual License Fee "Parascript"	$50,000	$50,000	$60,000	$63,000	$66,150
Total Year 1 2022	$406,780				
Total Year 2 2023		$395,000			
Total Year 3 2024			$131,050		
Total Year 4 2025				$136,181	
Total Year 5 2026					$141,525