Intergovernmental Agreement for Data Use

This Intergovernmental Agreement for Data Use ("Agreement") is entered into as of the date of the last signature below ("Effective Date") by and between: Arapahoe County on behalf of the Arapahoe County Assessor's Office, a political subdivision of the State of Colorado ("the County" or "Assessor's Office"); and the City of Greenwood Village, a Colorado home rule municipality ("the City") (together, the "Parties").

WHEREAS, the City possesses certain data that is valuable to the Assessor's Office for the performance of its statutory duties including, but not limited to, property valuation, assessment, and related governmental functions; and

WHEREAS, pursuant to Article XIV, Section 18(2)(a) of the Colorado Constitution and C.R.S. § 29-1-203, governments may cooperate and contract with one another to provide any function, service, or facility each is authorized to perform; and

WHEREAS, the Parties wish to establish terms governing the use, storage, protection, and disclosure of such data to protect personally identifiable information ("PII") and other sensitive information from unauthorized access, use, or disclosure; and

WHEREAS, the Parties intend for this Agreement to comply with applicable federal, state, and local laws, including the Colorado Open Records Act (C.R.S. § 24-72-200.1 et seq.) ("CORA"), and to follow industry best practices for data security.

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

ARTICLE 1. DEFINITIONS

For purposes of this Agreement, the following terms shall have the meanings set forth below:

"Authorized Personnel" means employees, contractors, and agents of the Assessor's Office, as well as members of the Arapahoe County IT Department have a legitimate business need to access Covered Data.

"Covered Data" means all data, information, records, and materials provided by the City to the Assessor's Office under this Agreement, regardless of format or medium. Covered Data includes, but is not limited to, the categories and examples described in Section 2.4 of this Agreement, as well as any other data collected and used by the Assessor's Office from the City for the purposes described herein.

"Data Breach" means any unauthorized access, acquisition, use, or disclosure of Covered Data that compromises the security, confidentiality, or integrity of such data.

"Personally Identifiable Information" or "PII" means any information that can be used to identify, contact, or locate an individual, either alone or in combination with other

information, including but not limited to: names, addresses, telephone numbers, email addresses, Social Security numbers, driver's license numbers, financial account information, and any other information defined as personally identifiable under applicable law.

"Third-Party Processor" means any entity, including the Arapahoe County Information Technology Department that processes Covered Data on behalf of the Assessor's Office pursuant to a written agreement containing data protection terms substantially equivalent to this Agreement.

"IT Data Team" means the data management personnel within the Arapahoe County Information Technology Department who are specifically authorized to perform data processing, data cleaning, data migration, and automation services on behalf of the Assessor's Office.

ARTICLE 2. PURPOSE AND SCOPE

2.1 Purpose. The purpose of this Agreement is to establish the terms and conditions under which the City will share Covered Data with the Assessor's Office, and to ensure that such data is protected from unauthorized access, use, or disclosure in accordance with applicable laws and industry best practices.

2.2 Scope. This Agreement governs all Covered Data provided by the City to the Assessor's Office, regardless of the format or medium in which such data is transmitted or stored. This Agreement applies to data obtained through direct provision, automated data feeds, API connections, manual uploads, and downloads from third-party maintained sites or systems.

2.3 Permitted Uses. The Assessor's Office shall use Covered Data solely for the following purposes: (a) property valuation and assessment activities; (b) compliance with statutory and regulatory requirements; (c) generation of aggregate statistical analyses and reports that do not identify individuals or specific properties at a granular level; and (d) other governmental functions directly related to the Assessor's Office's statutory duties.

2.4 Categories of Covered Data. Covered Data under this Agreement includes, but is not limited to, the following categories and examples. This list is illustrative and not exhaustive; additional data types not specifically listed are equally protected under this Agreement:

(a) Property and Infrastructure Data:

- Building plans, architectural drawings, blueprints, and construction documents
- Site plans, surveys, plats, and geospatial data
- Infrastructure records including utility connections, easements, and rights-of-way
- Property photographs, renderings, and visual documentation

(b) Permit and Regulatory Data:

- Building permits, certificates of occupancy, and inspection records

- Zoning applications, variances, and land use approvals
- Code enforcement records and violation notices
- Environmental permits and compliance documentation

(c) City Works and Municipal Operations Data:

- Public works project records and capital improvement data
- Maintenance and repair records for public infrastructure
- Service request and work order information
- Asset management and inventory data

(d) Valuation and Assessment Data:

- Property valuations, appraisals, and assessor's estimates
- Sales data, comparable property information, and market analyses
- Cost and income approach calculations
- Property characteristic data including square footage, lot size, and improvements

(e) Personally Identifiable Information (PII):

- Property owner names, mailing addresses, and contact information
- Permit applicant and contractor information
- Business owner and registered agent information
- Any other information that could identify specific individuals

(f) Financial and Transactional Data:

- Fee schedules, payment records, and billing information
- Project cost estimates and actual expenditures
- Contract and vendor information related to covered activities

The Parties acknowledge that data formats may include structured databases, spreadsheets, documents, images, PDFs, GIS files, CAD files, APIs, data feeds, and other electronic or physical formats. All such formats are equally protected under this Agreement regardless of whether specifically enumerated above.

ARTICLE 3. DATA ACCESS AND AUTHORIZATION

3.1 Exclusive Access. Access to Covered Data shall be strictly limited to the Assessor's Office and its Authorized Personnel.

3.2 Minimum Necessary Standard. Authorized Personnel shall access only the minimum amount of Covered Data necessary to perform their assigned duties. Access permissions shall be configured to enforce this principle through technical controls where feasible.

3.3 Third-Party Processors. The Assessor's Office may engage Third-Party Processors to process Covered Data on its behalf, provided that: (a) such Third-Party Processors are bound by written agreements containing data protection terms substantially equivalent to this Agreement; (b) such Third-Party Processors implement security measures consistent with the requirements of Article 5; and (c) the Assessor's Office remains responsible for the acts and omissions of its Third-Party Processors.

3.4 IT Data Team Authorization. The Arapahoe County IT Department's Data Team is expressly authorized to perform the following functions with respect to Covered Data on behalf of the Assessor's Office:

- Data Processing: Transforming, validating, and structuring Covered Data for use by the Assessor's Office
- Data Cleaning: Identifying and correcting errors, inconsistencies, duplicates, and data quality issues within Covered Data
- Data Migration: Transferring Covered Data between approved storage systems, including system upgrades and platform transitions
- Automation: Developing, implementing, and maintaining automated data workflows, ETL (Extract, Transform, Load) processes, API integrations, and scheduled data operations
- Technical Support: Providing database administration, system maintenance, and troubleshooting services related to systems storing Covered Data

3.5 IT Data Team Obligations. IT Data Team members performing functions under Section 3.4 shall: (a) access only the minimum Covered Data necessary to perform their assigned functions; (b) not retain copies of Covered Data beyond what is necessary for their assigned tasks; and (c) comply with all security requirements set forth in Article 5.

3.6 Prohibition on Unauthorized Access. No individual or entity other than Authorized Personnel and approved Third-Party Processors shall have access to Covered Data. The Assessor's Office shall implement technical and administrative controls to prevent unauthorized access.

3.7 Access Reviews. The Assessor's Office shall conduct periodic reviews of access permissions, no less frequently than annually, to ensure that only Authorized Personnel with a current business need retain access to Covered Data. This review shall include verification of IT Data Team access permissions.

ARTICLE 4. DATA STORAGE AND SYSTEMS

4.1 Approved Storage Systems. Covered Data may only be stored in the following approved systems and locations, all of which must meet the security requirements specified in Article 5:

- Assessor's Office proprietary software systems
- Designated network folder systems (IFL folder systems)
- Google Cloud Platform (GCP) BigQuery and Cloud Storage

- Microsoft SQL Server databases
- Third-party assessment and valuation software platforms licensed by the Assessor's Office (e.g., Computer Assisted Mass Appraisal systems and related industry software)
- Other systems expressly approved in writing by the Assessor's Office and the City

4.2 Third-Party Software Vendors. The Assessor's Office utilizes specialized software systems provided by third-party vendors to perform assessment, valuation, and related governmental functions. These systems may include Computer Assisted Mass Appraisal (CAMA) platforms, property records management systems, and other industry-standard assessment tools. The following requirements apply to all third-party software vendors whose systems store or process Covered Data:

(a) Vendor Security Standards. Third-party software vendors must maintain security practices consistent with industry standards, including:

- Implementation of access controls requiring unique user credentials for all system users
- Encryption of data at rest and in transit using industry-standard protocols
- Regular security assessments, vulnerability testing, and timely patching of known vulnerabilities
- Maintenance of audit logs tracking user access and system activities
- Incident response procedures and breach notification capabilities

(b) Access Governance. Access to third-party software systems containing Covered Data shall be governed as follows:

- User accounts shall be assigned only to Authorized Personnel with a legitimate business need
- User permissions shall follow the principle of least privilege, granting only the minimum access necessary to perform assigned duties
- User accounts shall be promptly deactivated upon termination of employment or when access is no longer required
- Shared or generic login credentials are prohibited; each user must have unique credentials
- Strong password requirements and, where supported, multi-factor authentication shall be enforced

(c) Vendor Agreements. The Assessor's Office shall maintain written agreements with third-party software vendors that include:

- Confidentiality provisions protecting Covered Data from unauthorized disclosure
- Security requirements consistent with the standards set forth in this Agreement
- Data breach notification obligations

- Restrictions on the vendor's use of Covered Data for purposes other than providing the contracted services
- Data return or destruction provisions upon termination of the vendor relationship

(d) Vendor Oversight and Security Review. The Assessor's Office, in conjunction with the Arapahoe County Information Technology Department's Security Officer (or equivalent designated security personnel), shall exercise appropriate oversight of third-party software vendors. This oversight shall include:

- Periodic review of vendor security practices, certifications, and compliance with contractual obligations
- Evaluation of vendor security controls prior to initial deployment and upon significant system changes or upgrades
- Assessment of vendor incident response capabilities and review of any security incidents affecting the vendor
- Verification that vendor access controls and authentication mechanisms meet the requirements of this Agreement
- Coordination between the Assessor's Office and IT Security to address any identified security concerns or deficiencies

The Assessor's Office remains responsible for Covered Data processed by third-party software vendors on its behalf and shall work collaboratively with the IT Data Team to ensure ongoing compliance with security requirements.

(e) City Notification. Upon request, the Assessor's Office shall provide the City with a general description of the third-party software systems used to store or process Provider's Covered Data, along with confirmation that such vendors are subject to appropriate security and confidentiality requirements.

4.3 Cloud Storage Security Assurances.. The following assurances are provided regarding the use of cloud platforms such as Google Cloud Platform (GCP):

(a) Enterprise-Grade Security. Cloud platforms used by the Assessor's Office are enterprise-grade services that maintain rigorous security certifications, including:

- SOC 1, SOC 2, and SOC 3 compliance (System and Organization Controls)
- ISO 27001, ISO 27017, and ISO 27018 certifications (Information Security Management)
- FedRAMP authorization (Federal Risk and Authorization Management Program)
- HIPAA compliance capabilities for protected health information standards
- PCI DSS compliance for payment card industry standards

(b) Data Location and Sovereignty. Covered Data stored in cloud systems shall be hosted within data centers located in the United States. The County shall configure cloud services

to prevent data from being transferred to or processed in foreign jurisdictions without the City's prior written consent.

(c) Encryption. All Covered Data stored in cloud systems is encrypted both at rest (when stored) and in transit (when transmitted). Encryption uses industry-standard algorithms such as AES-256, which is the same standard used by financial institutions and government agencies for highly sensitive data.

(d) Access Controls. Cloud systems are configured with strict access controls, including: unique user authentication, role-based permissions limiting access to authorized personnel only, multi-factor authentication requirements, and detailed audit logging of all access attempts.

(e) No Public Access. Covered Data stored in cloud systems is never publicly accessible. All storage locations are configured as private, with no public URLs, anonymous access, or shared links permitted.

(f) Physical Security. Cloud data centers maintain physical security measures including 24/7 security personnel, biometric access controls, video surveillance, and environmental controls. These facilities typically exceed the physical security capabilities of traditional on-premises data centers.

(g) Redundancy and Disaster Recovery. Cloud platforms provide automated data redundancy and backup capabilities, protecting against data loss due to hardware failure, natural disasters, or other unforeseen events. This ensures greater data durability than most traditional storage methods.

(h) City's Right to Request Information. the City may request documentation regarding the security certifications, configurations, and controls applicable to cloud systems storing their Covered Data. The Assessor's Office shall respond to such requests within thirty (30) days.

4.4 Prohibited Storage. Covered Data shall not be stored on: (a) personal devices or computers not owned or managed by the Assessor's Office or Arapahoe County; (b) mobile devices unless expressly approved and encrypted; (c) removable media unless encrypted and approved for specific, documented purposes; or (d) any cloud service, application, or system not approved under Section 4.1.

4.5 Data Identification and Tracking. Covered Data shall be stored in a manner that allows identification of its source to the extent practicable. To the extent possible, the Assessor's Office shall maintain records identifying data as originating from the City using one or more of the following methods, as available and appropriate: (a) a unique identifier associated with the City, which may change over time due to system updates or administrative changes; (b) metadata or tagging systems that link data to the City; (c) segregated storage locations designated for the City's data; or (d) documentation or cataloging that associates data sets with the City. The parties acknowledge that unique identifiers may be unknown at the time of initial data transfer, may change over time, or may not be available for all data types. The Assessor's Office shall use commercially reasonable efforts to maintain data provenance and shall work toward

implementing a consistent identifier system that directly associates data with the City as systems and capabilities permit.

4.6 Data Downloads from Third-Party Sites. When Covered Data is obtained from websites or systems maintained by third parties on behalf of the City, such data shall be: (a) transferred immediately to approved storage systems; (b) not retained on local machines beyond the time necessary for transfer; and (c) processed only through secured programs and automated workflows that comply with Section 5.4.

ARTICLE 5. SECURITY REQUIREMENTS

5.1 Security Standards. The Assessor's Office shall implement and maintain administrative, technical, and physical safeguards that meet or exceed standards equivalent to those required under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (45 C.F.R. Part 160 and Part 164, Subparts A and C), adapted as appropriate for the nature of Covered Data. These safeguards shall include, at minimum, the following:

(a) Encryption at Rest. All Covered Data stored in any approved system shall be encrypted using industry-standard encryption algorithms (AES-256 or equivalent) when at rest.

(b) Encryption in Transit. All transmissions of Covered Data shall be encrypted using TLS 1.2 or higher, or equivalent secure protocols.

(c) Access Controls. Access to systems containing Covered Data shall be controlled through strong authentication mechanisms including unique user identifiers, complex passwords, and, where technically feasible, multi-factor authentication.

(d) Network Security. Systems storing Covered Data shall be protected by firewalls, intrusion detection systems, and network segmentation. IP address restrictions shall be implemented where appropriate.

(e) Audit Logging. The Assessor's Office shall maintain audit logs of access to and modifications of Covered Data. Logs shall be retained for a minimum of two (2) years.

5.2 Additional Security Guidelines. The Assessor's Office shall implement security measures consistent with the following frameworks and guidelines, as applicable:

- NIST Cybersecurity Framework (NIST CSF)
- NIST Special Publication 800-53 (Security and Privacy Controls)
- CIS Critical Security Controls
- Colorado Information Security Policies (8 CCR 1501-5)

5.3 Object Storage Security. Object stores used for PDFs, files, images, and other unstructured data shall be configured with: (a) private access by default; (b) no public URLs or anonymous

access; (c) access limited to Authorized Personnel through role-based permissions; and (d) encryption at rest and in transit.

5.4 Automated Processing Security. Automated data processing performed by the Assessor's Office or the IT Data Team, including API integrations, scheduled downloads, ETL processes, and data pipelines, shall be: (a) executed only through approved, secured programs and projects; (b) subject to permission boundaries limiting data access to the minimum necessary; (c) designed to ensure that Covered Data does not persist on processing hardware beyond the completion of the processing task; (d) documented and subject to periodic security review; and (e) logged for audit purposes.

5.5 Data Migration Security. When the IT Data Team performs data migration activities, the following security measures shall apply: (a) migration plans shall be documented and approved by the Assessor's Office prior to execution; (b) data shall be encrypted during transfer between systems; (c) source data shall not be deleted until successful migration is verified; (d) temporary copies created during migration shall be securely deleted upon completion; and (e) migration activities shall be logged and auditable.

5.6 Data Lake Security. Data lakes storing Covered Data shall implement: (a) access controls limiting access to Authorized Personnel; (b) data classification and tagging; (c) row-level and column-level security where supported; and (d) audit logging of all queries and data access.

ARTICLE 6. PERSONALLY IDENTIFIABLE INFORMATION

6.1 PII Protection. PII contained within Covered Data shall not be released to the public or any unauthorized party under any circumstances except as may be required by law and subject to the procedures set forth in Article 7.

6.2 Data Masking. When limited release of data is permitted, data masking techniques shall be applied to PII, including but not limited to: (a) truncation or partial redaction of identifiers; (b) replacement with pseudonymous identifiers; (c) generalization of specific values to ranges or categories; and (d) suppression of fields containing sensitive information.

6.3 Use of Identifiers. Where possible, internal identifiers shall be used in place of PII for data processing and analysis. Direct identifiers (names, SSNs, addresses) shall be stored separately from analytical data and linked only when necessary for legitimate business purposes.

6.4 Re-identification Prohibition. No individual or entity shall attempt to re-identify individuals from de-identified or aggregated Covered Data. Any inadvertent re-identification shall be reported immediately to the Assessor's Office and the City.

ARTICLE 7. PUBLIC RECORDS AND CORA REQUESTS

7.1 Ownership and Release Constraints: All Covered Data shared pursuant to this Agreement remains the sole and exclusive property of the Party who initially collected it. Each Party shall retain control of its information and data submitted to the County. For purposes of C.R.S. 24-72-201 et seq. or C.R.S. 24-72-301 et. seq., each Party shall remain the custodian of the information they collected. All requests for information shall be referred to the Party that contributed the original information and data being requested.

7.2 Provider Notification. Upon receipt of a CORA request or any other legal demand for disclosure of Covered Data, the Assessor's Office shall refer the requestor to the City for any Covered Data.

ARTICLE 8. ANALYTICS AND AGGREGATION

8.1 Permitted Analytics. The Assessor's Office may use Covered Data for analytical purposes, including statistical analysis, trend identification, and report generation, provided that such analytics: (a) do not identify individuals or specific properties at a granular level; (b) use aggregated data where possible; and (c) comply with the PII protections set forth in Article 6.

8.2 Public Release of Analytics. Any public release of analytical results derived from Covered Data shall: (a) present data only in aggregate form; (b) ensure that no individual or property can be identified from the released data (e.g., through k-anonymity or similar techniques); (c) mask or suppress data where aggregation alone is insufficient to prevent identification; and (d) be reviewed and approved by the Assessor's Office prior to release.

8.3 Internal Reporting. Internal reports generated for Assessor's Office purposes may contain more granular data, provided that access to such reports is limited to Authorized Personnel and the reports are not disclosed to the public.

ARTICLE 9. DATA BREACH NOTIFICATION

9.1 Breach Notification. In the event of a Data Breach involving Covered Data, the Assessor's Office shall: (a) notify the City within seventy-two (72) hours of discovery of the breach; (b) provide a detailed description of the breach, including the nature and extent of data affected; (c) describe the remedial actions taken or planned; and (d) cooperate with the City in investigating and responding to the breach.

9.2 Regulatory Notification. The Assessor's Office shall comply with all applicable breach notification laws, including the Colorado Consumer Protection Act provisions regarding data breach notification (C.R.S. § 6-1-716).

9.3 Mitigation. The Assessor's Office shall take all reasonable steps to mitigate the effects of a Data Breach and prevent future breaches, including implementing additional security measures as may be appropriate.

ARTICLE 10. TERM AND TERMINATION

10.1 Term. This Agreement shall be effective as of the Effective Date and shall remain in effect for a period of three (3) years, unless earlier terminated in accordance with this Article. This Agreement shall automatically renew for successive one (1) year periods unless either party provides written notice of non-renewal at least sixty (60) days prior to the end of the then-current term.

10.2 Termination for Breach. Either party may terminate this Agreement upon written notice if the other party materially breaches any provision of this Agreement and fails to cure such breach within thirty (30) days after receiving written notice of the breach.

10.3 Termination for Convenience. Either party may terminate this Agreement for any reason upon ninety (90) days' prior written notice to the other party.

10.4 Effect of Termination. Upon termination or expiration of this Agreement: (a) the Assessor's Office shall cease using Covered Data for any purpose not previously completed; (b) at the City's request, the Assessor's Office shall return or securely destroy all Covered Data in its possession, unless retention is required by law; and (c) the provisions of Articles 6, 7, 9, and 11 shall survive termination.

ARTICLE 11. GENERAL PROVISIONS

11.1 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Colorado, without regard to its conflict of laws principles.

11.2 Entire Agreement. This Agreement, together with any addenda or exhibits attached hereto, constitutes the entire agreement between the Parties concerning the subject matter hereof and supersedes all prior agreements, understandings, and negotiations, whether written or oral.

11.3 Amendments. This Agreement may be amended only by a written instrument signed by both parties.

11.4 Severability. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

11.5 Waiver. The failure of either party to enforce any provision of this Agreement shall not constitute a waiver of that party's right to enforce such provision in the future.

11.6 Notices. All notices required or permitted under this Agreement shall be in writing and shall be deemed delivered when personally delivered, or three (3) business days after being sent by certified mail, return receipt requested, or one (1) business day after being sent by overnight courier, to the addresses set forth in the signature blocks below.

11.7 Counterparts. This Agreement may be executed in counterparts, each of which shall be deemed an original, and all of which together shall constitute one and the same instrument. Electronic signatures shall be deemed valid and binding.

11.8 Assignment. Neither party may assign its rights or delegate its duties under this Agreement without the prior written consent of the other party, except that the Assessor's Office may assign this Agreement to any successor entity responsible for performing the Assessor's statutory functions.

SIGNATURE PAGE

IN WITNESS WHEREOF, the parties have executed this Data Use Agreement as of the date last signed below.

The Board of County Commissioners of Arapahoe County
on behalf of the Arapahoe County Assessor's Office

Signature: _____ Date: _____

Printed Name: _____ Title: _____

City of Greenwood Village:

_____
Mayor George E. Lantz

Date: _____

ATTEST:

_____
Susan M. Ortiz, MMC, City Clerk

APPROVED AS TO FORM:

_____
Shannon Chambers-Nelson, Interim City Attorney