

AMENDATORY AGREEMENT

THIS 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 **BAKER TILLY US, LLP**, an Illinois limited liability partnership, authorized to do business in Colorado with a mailing address of P.O. Box 7398 Madison, Wisconsin, 53707-7398 (the "Contractor") which has merged with **MOSS ADAMS LLP**, a Washington limited liability partnership, whose address is 999 Third Avenue Suite 2800 Seattle, Washington 98104 (the "Original Contractor").

WITNESSETH:

WHEREAS, the City and the Original Contractor previously entered into an Agreement dated December 20, 2021 (the "Agreement") relating to audit services described in the Statement of Work; and

WHEREAS, Original Contractor entered into an Equity Purchase Agreement under which Original Contractor combined with Contractor ("**Transaction**") and as of the closing of the Transaction on June 3, 2025 ("**Effective Date**"), Contractor desires to provide services described in the Agreement (the "**Services**"), and City desires to permit Contractor to do so; and

WHEREAS, the Contractor requires revisions to the Scope of Work to conform to its business practices; and

WHEREAS, the certain updates to the Agreement are necessary to conform to current law and regulations;

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

1. The additional Scope of Work is attached hereto and incorporated herein as **Exhibit A-1** and all references to "Exhibit A" are hereby amended to read "**Exhibits A and A-1** as applicable". Exhibit A-1 will be applicable to all work undertaken after the execution of this Amendatory Agreement

2. The replacement proof of insurance is attached hereto and incorporated herein as **Exhibit C-1** and all references to "Exhibit C" are hereby amended to read "**Exhibits C and C-1** as applicable".

3. Paragraph 20 of the Agreement, entitled "NO EMPLOYMENT OF A WORKER

WITHOUT AUTHORIZATION TO PERFORM WORK UNDER THE AGREEMENT,” is amended to read as follows:

20. RESERVED.

4. Paragraph 30 of the Agreement, entitled “CONFIDENTIAL INFORMATION,” is amended to read as follows:

30. CONFIDENTIAL INFORMATION:

a. City Information: Contractor acknowledges and accepts that, in performance of all work under the terms of this Agreement, Contractor may have access to Proprietary Data or confidential information that may be owned or controlled by the City, and that the disclosure of such Proprietary Data or information may be damaging to the City or third parties. Contractor agrees that all Proprietary Data or confidential information provided or otherwise disclosed by the City to Contractor shall be held in confidence and used only in the performance of its obligations under this Agreement. Contractor shall exercise the same standard of care to protect such Proprietary Data and information as a reasonably prudent Contractor would to protect its own proprietary or confidential data. “Proprietary Data” shall mean any materials or information which may be designated or marked “Proprietary” or “Confidential”, and shall include protected and sensitive data as set forth in §§ 24-73-101 and 6-1-716(1)(g)(I)(A), C.R.S., as amended that are not otherwise in the public domain (except as a result of a breach of confidentiality), or which would not be documents subject to disclosure pursuant to the Colorado Open Records Act or City ordinance, and provided or made available to Contractor by the City. Such Proprietary Data may be in hardcopy, printed, digital or electronic format. The Contractor shall store all City Data inside of the United States. The Contractor shall require all co-processing of data with Baker Tilly entities, including its international affiliates, to be bound by Contractor’s Information Technology Security Policies and Procedures. The City may approve or deny such request within the City’s sole discretion.

For the purposes of this Agreement the following definitions shall apply:

(1) “City Data” means all information, data, and records, regardless of form, created by or in any way originating with the City and all information that is the output of any computer processing or other electronic manipulation including all records relating to the City’s use of the Work. City Data also includes Confidential Information and Protected Information, as defined in this Agreement.

(2) “Confidential Information” is described in subparagraph c below and additionally means all information or data, regardless of form, not subject to disclosure under the Colorado Open Records Act, § 24-72-201, et seq., C.R.S. (“CORA”), and is marked or identified at the time of disclosure as being confidential, proprietary, or its equivalent.

(3) “D(d)ata” means information, regardless of form, that can be read, transmitted, or processed.

(4) “Protected Information” means data, regardless of form, that has been designated as sensitive, private, proprietary, protected, or confidential by law, policy, or the City. Protected Information includes, but is not limited to, employment records, protected health information, student and education records, criminal justice information, personal financial records, research data, trade secrets, classified government information, other regulated data, and personally identifiable information as defined by §§ 24-73-101(4)(b) and 6-1-716(1)(g)(I)(A), C.R.S., as amended. Protected Information shall not include public records that by law must be made available to the public under CORA. To the extent there is any uncertainty as to whether data constitutes Protected Information, the data in question shall be treated as Protected Information until a determination is made by the City or an appropriate legal authority.

b. Use of Proprietary Data or Confidential Information:

(i) Except as expressly provided by the terms of this Agreement, Contractor agrees that it shall not disseminate, transmit, license, sublicense, assign, lease, release, publish, post on the internet, transfer, sell, permit access to, distribute, allow interactive rights to, or otherwise make available the Proprietary Data or Confidential Information or any part thereof to any other person, party or entity in any form of media for any purpose other than performing its obligations under this Agreement or as otherwise permitted under this Agreement. Contractor further acknowledges that by providing this Proprietary Data or Confidential Information, the City is not granting to Contractor any right or license to use such data except as provided in this Agreement. Contractor further agrees not to disclose or distribute to any other party, in whole or in part, the Proprietary Data or confidential information without written authorization from the Manager.

(ii) Contractor agrees, with respect to the Proprietary Data and Confidential Information, that: (1) Contractor shall not copy, recreate, reverse engineer or decompile such data, in whole or in part, unless authorized in writing by the Manager; (2) Contractor shall retain no copies, recreations, compilations, or decompilations, in whole or in part, of such data; and (3) Contractor shall, upon the expiration or earlier termination of the Agreement, destroy (and, in writing, certify destruction) or return all such data or work products incorporating such data or information to the City. Notwithstanding the foregoing or anything else in this Agreement, Contractor shall be permitted to retain its Workpapers, excluding any Proprietary Data or confidential information that is referenced or incorporated therein.

(iii) At its reasonable discretion, the City may prohibit the Contractor from the use of certain software programs, databases, and computing systems with known vulnerabilities to collect, use, process, store, or generate data and information received

under this Agreement. The Contractor shall fully comply with all requirements and conditions, if any, associated with the use of software programs, databases, and computing systems as reasonably directed by the City. The Contractor shall not use funds paid by the City for the acquisition, operation, or maintenance of software in violation of any copyright laws or licensing restrictions. The Contractor shall maintain commercially reasonable network security that, at a minimum, includes network firewalls, intrusion detection/prevention, and enhancements or updates consistent with evolving industry standards. The Contractor shall use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to, anti-virus and anti-malware protections. The Contractor shall ensure that any underlying or integrated software employed under this Agreement is updated on a regular basis and does not pose a security threat. Contractor shall procure annual security audits of the systems used to provide the Services (“Systems”), including organizational process controls, information technology controls, and data center or hosting center controls, by an independent third party. At City’s request and execution of Contractor’s confidentiality agreement, Contractor will at no charge provide City with copies of the most recently completed Service Organization Control (“SOC”) report which is related to the Systems and will complete the City’s Vendor Risk Assessment.

c. Safeguarding City Confidential Information: “Confidential Information” includes, but is not limited to, employment records, protected health information, student and education records, criminal justice information, personal financial records, research data, trade secrets, classified government information, other regulated data, and personally identifiable information. Confidential Information also includes, without limitation, any information maintained by the City about an individual that can be used to distinguish or trace an individual’s identity, including, but not limited to, first and last name, residence or other physical address, banking information, electronic mail address, telephone number, credit card information, an official government-issued driver’s license or identification card number, social security number or tax identification number, date and place of birth, mother’s maiden name, or biometric records. Confidential Information includes, but is not limited to, all information defined as personally identifiable information in §§ 24-73-101, C.R.S. Confidential Information shall also include “personal information” as defined in § 24-73-103(1)(g), C.R.S. To the extent there is any uncertainty as to whether data constitutes Confidential Information, the data in question shall be treated as Confidential Information until a determination is made by the City or an appropriate legal authority. The Contractor shall only store Confidential Information in facilities located within the United States or located outside of the United States when approval has been provided by the City’s Technology Services agency upon completion of required security reviews. Disclosure of Confidential Information does not include disclosure to a third party under circumstances where the City retains primary responsibility for implementing and maintaining reasonable security procedures and practices appropriate to the nature of the

Confidential Information, and the City implements and maintains technical controls reasonably designed to safeguard Confidential Information from unauthorized access, modification, disclosure, or destruction or effectively eliminate the third party's ability to access Confidential Information, notwithstanding the third party's physical possession of Confidential Information. If the Contractor has been contracted to maintain, store, or process personal information on the City's behalf, the Contractor is a "Third-Party Service Provider" as defined by § 24-73-103(1)(i), C.R.S. and shall maintain security procedures and practices consistent with §§ 24-73-101, et seq., C.R.S. In addition, as set forth in § 28-251, D.R.M.C., the Contractor, including, but not limited to, the Contractor's employees, agents, and Subcontractors, shall not collect or disseminate individually identifiable information about the national origin, immigration, or citizenship status of any person, over and above the extent to which the City is required to collect or disseminate such information in accordance with any federal, state, or local law. The Contractor shall comply with all legislative and regulatory requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); the Health Information Technology for Economic and Clinical Health Act ("HITECH"); 42 CFR Part 2, Confidentiality of Substance use Disorder Patient Records; the privacy standards adopted by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, Subparts A and E; and the security standards adopted by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160, 162, 164, and Subpart C (collectively, "HIPAA Rules") to the extent applicable to the Services. The Contractor shall implement all necessary protective measures designed to comply with HIPAA Rules, and the Contractor hereby agrees to be bound by the terms of the Business Associate Agreement attached hereto and incorporated herein as **Appendix 1** to **Exhibit A-1**. The Contractor shall not use protected health information or substance use treatment records except as legally necessary to fulfill the purpose of this Agreement and shall hold the City harmless, to the extent permitted by law, for any breach of these regulations. This Section shall survive the expiration or earlier termination of this Agreement, and the Contractor shall ensure that the requirements of this Section are included in any relevant subcontracts or subgrants.

d. Data Retention, Transfer, Litigation Holds, and Destruction: Using appropriate and reliable storage media, the Contractor shall regularly backup data used in connection with this Agreement and retain such backup copies for a period of seven (7) years or longer if required under applicable City Retention Schedule and regulatory requirements or longer to be consistent with the Contractor's data and record retention policies. All City Data shall be encrypted in transmission, including by web interface, and in storage by an agreed upon National Institute of Standards and Technology ("NIST") approved strong encryption method and standard. The Contractor shall not transfer, maintain or store data under this Agreement outside of the United States without the City's express written permission unless otherwise permitted under this Agreement. Upon termination of this Agreement, the

Contractor shall securely delete or securely transfer all data, including Protected Information, to the City in an industry standard format as directed by the City; however, this requirement shall not apply to the extent the Contractor is required by law to retain data, including Protected Information. Upon the City's request, the Contractor shall confirm, by providing a certificate, the data disposed of, the date disposed of, and the method of disposal. The City will promptly coordinate with the Contractor regarding the preservation and disposition of any data and records relevant to any current or anticipated litigation, and the Contractor shall continue to preserve the records until further notice by the City. Unless otherwise required by law or regulation, when paper or electronic documents are no longer needed, the Contractor shall destroy or arrange for the destruction of such documents within its custody or control that contain Protected Information by shredding, erasing, or otherwise modifying the Protected Information in the paper or electronic documents to make it unreadable or indecipherable. The Contractor and its third-party services providers must develop and maintain a written policy for the destruction of such records.

e. Employees and Sub-contractors: Contractor will inform its employees and officers of the obligations under this Agreement, and all requirements and obligations of Contractor under this Agreement shall survive the expiration or earlier termination of this Agreement. Contractor shall not disclose Proprietary Data or confidential information to subcontractors unless such subcontractors are bound by non-disclosure and confidentiality provisions at least as strict as those contained in this Agreement. If the Contractor engages a subcontractor under this Agreement, the Contractor shall impose data protection terms that provide at least the same level of data protection as in this Agreement and to the extent appropriate to the nature of the Work provided. The Contractor shall monitor the compliance with such obligations and remain responsible for its subcontractor's compliance with the obligations of this Agreement and for any of its subcontractors acts or omissions that cause the Contractor to breach any of its obligations under this Agreement. Unless the Contractor provides its own security protection for the information it discloses to a third party, the Contractor shall require the third party to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the Protected Information disclosed and that are reasonably designed to protect it from unauthorized access, use, modification, disclosure, or destruction. Any term or condition within this Agreement relating to the protection and confidentiality of any disclosed data shall apply equally to both the Contractor and any of its subcontractors, agents, assigns, employees, or volunteers. The Contractor shall complete a Vendor Risk Assessment with the City. The Contractor shall ensure all subcontractors sign, or have signed, agreements containing nondisclosure provisions at least as protective as those in this Agreement, and that the nondisclosure provisions are in force so long as the subcontractor has access to any data disclosed under this Agreement. Upon request, the Contractor shall verify it has received all required signed nondisclosure agreements to the City.

f. Disclaimer: The City is responsible for the information provided, however, it assumes no financial liability to Contractor for any errors or omissions herein. Specifically, the City is not responsible for any costs including, but not limited to, those incurred as a result of lost revenues, loss of use of data, the costs of recovering such programs or data, the cost of any substitute program, claims by third parties, or for similar costs. If discrepancies are found, Contractor agrees to contact the City immediately.

g. Contractor's Information: The parties understand that all the material provided or produced under this Agreement may be subject to the Colorado Open Records Act., § 24-72-201, et seq., C.R.S. (2003). In the event of a request to the City for disclosure of such information, the City shall advise Contractor of such request in order to give Contractor the opportunity to object to the disclosure of any of its documents which it marked as proprietary or confidential material. In the event of the filing of a lawsuit to compel such disclosure, the City will tender all such material to the court for judicial determination of the issue of disclosure and Contractor agrees to intervene in such lawsuit to protect and assert its claims of privilege against disclosure of such material or waive the same. Contractor further agrees to defend, indemnify and save and hold harmless the City, its officers, agents and employees, from any claim, damages, expense, loss or costs arising out of Contractor's intervention to protect and assert its claim of privilege against disclosure under this Article including but not limited to, prompt reimbursement to the City of all reasonable attorney fees, costs and damages that the City may incur directly or may be ordered to pay by such court.

h. Security Breach: If the Contractor becomes aware of an unauthorized acquisition or disclosure of unencrypted data, in any form, that compromises the security, access, confidentiality, or integrity of City Data, Protected Information, or other data maintained or provided by the City ("Security Breach"), the Contractor shall notify the City in the most expedient time and without unreasonable delay but no less than seventy-two (72) hours. A Security Breach shall also include, without limitation, (i) successful attempts to gain unauthorized access to a City system or City Data regardless of where such information is located; (ii) the unauthorized use of a City system for the processing or storage of data; or (iii) changes to the City's system hardware, firmware, or software characteristics without the City's knowledge, instruction, or consent. Any oral notice of a Security Breach provided by the Contractor shall be immediately followed by a written notice to the City. The Contractor shall maintain documented policies and procedures for Security Breaches including reporting, notification, and mitigation.

i. Cooperation: The Contractor shall assist the City with its efforts regarding recovery, lawful notices, investigations, remediation, and the necessity to involve law enforcement, as determined by the City and as required by law. The Contractor shall preserve and provide all information relevant to the Security Breach to the City; provided, however, the Contractor shall not be obligated to disclose confidential business information

or trade secrets. The Contractor will provide City with cooperation and assistance as City may commercially reasonably request to comply with its data breach reporting obligations under Data Protection Laws and the Contractor shall further take commercially reasonable steps to remedy or mitigate the effects of the Security Breach. The Contractor will comply with this Section at Contractor's expense unless the Security Breach arose solely from City's negligent or willful acts or Contractor's compliance with City's express written instructions. Unless the Contractor can establish that neither it nor any of its agents, employees, assigns, or subcontractors are the cause or source of the Security Breach, the Contractor shall indemnify, defend, and hold harmless the City for all claims, including reasonable attorneys' fees, costs, and expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from the City in connection with a Security Breach and any required lawful notices.

j. Reporting: The Contractor shall provide a written report to the City that identifies, to the extent known: (i) the nature of the unauthorized use or disclosure; (ii) the data used or disclosed; (iii) the parties responsible for the Security Breach (if known); (iv) what the Contractor has done or shall do to mitigate the effect of the Security Breach; and (v) what corrective action the Contractor has taken or shall take to prevent future Security Breaches. Except as expressly required by law, the Contractor will not disclose or otherwise provide notice of the incident directly to any person, regulatory agencies, or other entities, without prior written permission from the City.

k. Costs: Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to the City under law or equity, the Contractor will be responsible for the following costs to the extent legally required resulting from any Security Breach: (i) providing notification to third parties whose data was compromised and to regulatory bodies, law-enforcement agencies, or other entities as required by law or contract; (ii) establishing and monitoring call center(s), and credit monitoring and/or identity restoration services to assist each person impacted by a Security Breach for a specific period as required by applicable law; and (iii) the payment of fines and penalties, and other fees imposed by regulatory agencies, courts of law, or contracting partners as a result of the Security Breach.

l. Remediation: After a Security Breach, the Contractor shall take steps to reduce the risk of incurring a similar type of Security Breach in the future as directed by the City, which may include, but is not limited to, developing and implementing a remediation plan that is approved by the City at no additional cost to the City. The City may adjust or direct modifications to this plan, and the Contractor shall make all reasonable modifications as directed by the City. The City may, in its sole discretion and at the Contractor's sole expense, require the Contractor to engage the services of an independent, qualified, City-approved third party to conduct a security audit. The Contractor shall provide the City with the high-level results of such audit and evidence of the Contractor's planned remediation

in response to any negative findings. Implementation of corrective actions to remedy the Security Breach and restore the City's access to the Work shall occur within thirty (30) calendar days of the date the Contractor becomes aware of any Security Breach.

5. A new paragraph 35 entitled "COMPLIANCE WITH DENVER WAGE LAWS" is added to read:

35. COMPLIANCE WITH DENVER WAGE LAWS: To the extent applicable to the Contractor's provision of Services hereunder, the Contractor shall comply with, and agrees to be bound by, all rules, regulations, requirements, conditions, and City determinations regarding the City's Minimum Wage and Civil Wage Theft Ordinances, Sections 58-1 through 58-26 D.R.M.C., including, but not limited to, the requirement that every covered worker shall be paid all earned wages under applicable state, federal, and city law in accordance with the foregoing D.R.M.C. Sections. By executing this Agreement, the Contractor expressly acknowledges that the Contractor is aware of the requirements of the City's Minimum Wage and Civil Wage Theft Ordinances and that any failure by the Contractor, or any other individual or entity acting subject to this Agreement, to strictly comply with the foregoing D.R.M.C. Sections shall result in the penalties and other remedies authorized therein

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

Remainder of page left intentionally blank.

Contract Control Number: AUDIT-202580685-01 / AUDIT 202158955-01
Contractor Name: BAKER TILLY US LLP

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:

REGISTERED AND COUNTERSIGNED:

Attorney for the City and County of Denver


By:

By:

By:

Contract Control Number:
Contractor Name:

AUDIT-202580685-01 / AUDIT-202158955-01
BAKER TILLY US LLP

By:  Signed by:
Olga A Darlington
0443CEA83EE542E...

Name: Olga A Darlington
(please print)

Title: Principal
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)

EXHIBIT A-1

(exhibit follows)



Baker Tilly US, LLP
675 15th Street
Suite 1900
Denver, CO 80202
United States of America

T: +1 (303) 298 9600
F: +1 (303) 298 8118

bakertilly.com

October 7, 2025

Timothy M. O'Brien, CPA, Denver Auditor's Office
Audit Committee
City and County of Denver
201 West Colfax, 705
Denver, CO 80202

Re: 2025 Financial Audit Services

Dear Mr. O'Brien:

Thank you for the opportunity to provide services to the City and County of Denver. This engagement letter ("Engagement Letter") is issued under, and governed by the terms of, the Agreement between the City and County of Denver and Moss Adams LLP dated December 20, 2021, as amended, (the "Agreement"), which is incorporated by this reference. Moss Adams LLP merged with Baker Tilly US, LLP on June 3, 2025, accordingly the governing terms of the Agreement between the City and County of Denver and Moss Adams will be assigned to Baker Tilly US, LLP. This Engagement Letter confirms our acceptance and understanding of the terms and objectives of our engagement, and limitations of the services that Baker Tilly US, LLP ("Firm," "we," "us," and "our") will provide to the City and County of Denver ("you," "your," and "Company").

Scope of Services – Audit

You have requested that we audit the City's Denver Airport Enterprise Fund (the "Airport Fund") financial statements, which comprise the statement of net position as of December 31, 2025, and the related statements of changes in net position and cash flows for the year then ending, and the related notes to the financial statements. We have not been engaged to report on whether the supplementary information is fairly stated, in all material respects, in relation to the financial statements as a whole.

We will also perform the audit of the Airport Fund's Passenger Facility Charge Program for the year ending December 31, 2025. We have not been engaged to report on whether the supplementary information, is fairly stated, in all material respects, in relation to the financial statements as a whole.

Accounting standards generally accepted in the United States of America provide for certain required supplementary information ("RSI"), such as management's discussion and analysis, to supplement the basic financial statements. Such information, although not a part of the basic financial statements, is required by the Governmental Accounting Standards Board who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. As part of our engagement, we will apply certain limited procedures to the Airport Fund's RSI in accordance with auditing standards generally accepted in the United States of America. We will not express an opinion or provide assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide assurance. The following RSI will be subjected to certain limited procedures, but will not be audited:

- 1) Management's discussion and analysis



Timothy O'Brien, CPA, Denver Auditor's Office
Audit Committee
City and County of Denver
October 7, 2025
Page 2 of 10

- 2) Schedule of Airport proportionate share – net pension liability
- 3) Schedule of Airport contributions – net pension liability
- 4) Schedule of Airport proportionate share – net OPEB liability
- 5) Schedule of Airport employer contributions – net OPEB liability
- 6) Schedule of Airport proportionate share – implicit rate subsidy

Objectives of the Audit

The objectives of our audit are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with auditing standards generally accepted in the United States of America (U.S. GAAS) will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the financial statements.

The objectives also include reporting on the following:

- Internal control related to the financial statements and compliance with the provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a material effect on the financial statements as required by *Government Auditing Standards*.

The report on internal control and compliance will include a statement that the purpose of the report is solely to describe the scope of testing of internal control over financial reporting and compliance and the result of that testing, and not to provide an opinion on the effectiveness of the Airport Fund's internal control over financial reporting or on compliance, that the report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the City's internal control over financial reporting and compliance, and, accordingly, it is not suitable for any other purpose.

Procedures and Limitations

Our procedures may include tests of documentary evidence supporting the transactions recorded in the accounts, tests of the physical existence of inventories, and direct confirmation of certain receivables and certain other assets, liabilities, and transaction details by correspondence with selected customers, creditors, and financial institutions. We may also request written representations from your attorneys as part of the engagement, and they may bill you for responding to this inquiry. At the conclusion of our audit, we will require certain written representations from management about the financial statements and related matters. Management's failure to provide representations to our satisfaction will preclude us from issuing our report.

An audit includes examining evidence, on a test basis, supporting the amounts and disclosures in the financial statements. Therefore, our audit will involve judgment about the number of transactions to be examined and the areas to be tested. Material misstatements may include errors, fraudulent financial reporting, misappropriation of assets, or noncompliance with the provisions of laws, regulations, contracts, and grant agreements that are attributable to the entity or to acts by management or employees acting on behalf of the City that may have a direct



Timothy O'Brien, CPA, Denver Auditor's Office
Audit Committee
City and County of Denver
October 7, 2025
Page 3 of 10

financial statement impact. Pursuant to *Government Auditing Standards*, we will not provide reasonable assurance of detecting abuse.

Because of the inherent limitations of an audit, together with the inherent limitations of internal control, an unavoidable risk exists that some material misstatements and noncompliance may not be detected, even though the audit is properly planned and performed in accordance with U.S. GAAS and *Government Auditing Standards*. An audit is not designed to detect immaterial misstatements or noncompliance with the provisions of laws, regulations, contracts, and grant agreements that do not have a direct and material effect on the financial statements. However, we will inform you of any material errors, fraudulent financial reporting, misappropriation of assets, and noncompliance with the provisions of laws, regulations, contracts and grant agreements that come to our attention, unless clearly inconsequential. We will also inform you of any other conditions or other matters involving internal control, if any, as required by *Government Auditing Standards*. Our responsibility as auditors is limited to the period covered by our audit and does not extend to any time period for which we are not engaged as auditors.

We may assist management in the preparation of the Airport Fund's financial statements, this would be limited to providing examples of footnote disclosures. Regardless of any assistance we may render, all information included in the financial statements the representation of management. We may issue a preliminary draft of the financial statements to you for your review. Any preliminary draft financial statements should not be relied upon, reproduced or otherwise distributed without the written permission of the Firm.

Management's Responsibility

As a condition of our engagement, management acknowledges and understands that management is responsible for the preparation and fair presentation of the financial statements in accordance with accounting principles generally accepted in the United States of America. We may advise management about appropriate accounting principles and their application and may assist in the preparation of your financial statements, but management remains responsible for the financial statements. Management also acknowledges and understands that management is responsible for the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to error or fraud. This responsibility includes the maintenance of adequate records, the selection and application of accounting principles, and the safeguarding of assets. You are responsible for informing us about all known or suspected fraud affecting the Airport Fund involving: (a) management, (b) employees who have significant roles in internal control, and (c) others where the fraud could have a material effect on the financial statements. You are responsible for informing us of your knowledge of any allegations of fraud or suspected fraud affecting the Airport Fund received in communications from employees, former employees, regulators or others.

Management is responsible for adjusting the financial statements to correct material misstatements and for confirming to us in the management representation letter that the effects of any uncorrected misstatements aggregated by us during the current engagement and pertaining to the latest period presented are immaterial, both individually and in the aggregate, to the financial statements as a whole.



Timothy O'Brien, CPA, Denver Auditor's Office
Audit Committee
City and County of Denver
October 7, 2025
Page 4 of 10

Management is responsible for establishing and maintaining internal control over compliance with the provisions of laws, regulations, contracts, and grant agreements, and for identifying and ensuring that you comply with such provisions. Management is also responsible for addressing the audit findings and recommendations, establishing and maintaining a process to track the status of such findings and recommendations, and taking timely and appropriate steps to remedy any fraud and noncompliance with the provisions of laws, regulations, contracts, and grant agreements or abuse that we may report.

Management is responsible for making all financial records and related information available to us and for the accuracy and completeness of that information. Management agrees that as a condition of our engagement, management will provide us with:

- access to all information of which management is aware that is relevant to the preparation and fair presentation of the financial statements, whether obtained from within or outside of the general and subsidiary ledgers (including all information relevant to the preparation and fair presentation of disclosures), such as records, documentation, and other matters;
- additional information that we may request from management for the purpose of the audit; and
- unrestricted access to persons within the Airport Fund from whom we determine it necessary to obtain audit evidence.

Management's Responsibility to Notify Us of Affiliates

Our professional standards require that we remain independent of the Airport Fund as well as any "affiliate" of the Airport Fund. Professional standards define an affiliate as follows:

- a fund, component unit, fiduciary activity or entity that the Airport Fund is required to include or disclose, and is included or disclosed in its basic financial statements, in accordance with generally accepted accounting principles (U.S. GAAP);
- a fund, component unit, fiduciary activity or entity that the Airport Fund is required to include or disclosed in its basic financial statements in accordance with U.S. GAAP, which is material to the Airport Fund but which the Airport Fund has elected to exclude, and for which the Airport Fund has more than minimal influence over the entity's accounting or financial reporting process;
- an investment in an investee held by the Airport Fund or an affiliate of the Airport Fund, where the Airport Fund or affiliate controls the investee, excluding equity interests in entities whose sole purpose is to directly enhance the Airport Fund's ability to provide government services;
- an investment in an investee held by the Airport Fund or an affiliate of the Airport Fund, where the Airport Fund or affiliate has significant influence over the investee and for which the investment is material to the Airport Fund's financial statements, excluding equity interests in entities whose sole purpose is to directly enhance the Airport Fund's ability to provide government services.



Timothy O'Brien, CPA, Denver Auditor's Office
Audit Committee
City and County of Denver
October 7, 2025
Page 5 of 10

In order to fulfill our mutual responsibility to maintain auditor independence, you agree to notify the Firm of any known affiliate relationships, to the best of your knowledge and belief. Additionally, you agree to inform the Firm of any known services provided or relationships between affiliates of the Airport Fund and the Firm or any of its employees or personnel.

Management's Responsibility for Supplementary Information

Management is responsible for the preparation of the supplementary information in accordance with the applicable criteria. Management agrees to include the auditor's report on the supplementary information in any document that contains the supplementary information and that indicates that we have reported on such supplementary information. Management is responsible to present the supplementary information with the audited financial statements or, if the supplementary information will not be presented with the audited financial statements, to make the audited financial statements readily available to the intended users of the supplementary information no later than the date of issuance by the entity of the supplementary information and the auditor's report thereon. For purposes of this Agreement, audited financial statements are deemed to be readily available if a third-party user can obtain the audited financial statements without any further action by management. For example, financial statements on your Web site may be considered readily available, but being available upon request is not considered readily available.

Other Information Included in an Annual Report

When financial or nonfinancial information, other than financial statements and the auditor's report thereon, is included in an entity's annual report, management is responsible for that other information. Management is also responsible for providing the document(s) that comprise the annual report to us as soon as it is available.

Our opinion on the financial statements does not cover the other information, and we do not express an opinion or any form of assurance thereon. Our responsibility is to read the other information and consider whether a material inconsistency exists between the other information and the audited financial statements. If we identify that a material inconsistency or misstatement of the other information exists, we will discuss it with you; if it is not resolved U.S. GAAS requires us to take appropriate action.

Key Audit Matters

U.S. GAAS does not require the communication of key audit matters in the audit report unless engaged to do so. You have not engaged us to report on key audit matters, and the Engagement Letter does not contemplate the Firm providing any such services. You agree we are under no obligation to communicate key audit matters in the auditor's report.

If you request to engage the Firm to communicate key audit matters in the auditor's report, before accepting the engagement we would discuss with you the additional fees to provide any such services, and the impact to the timeline for completing the audit.



Timothy O'Brien, CPA, Denver Auditor's Office
Audit Committee
City and County of Denver
October 7, 2025
Page 6 of 10

Use of Internal Auditor(s)

You agree that we may use your internal auditor(s) to perform audit procedures under our direction, supervision, and review. You also agree that the internal auditor(s) providing us with such direct assistance will be allowed to follow our instructions, and that you will not intervene in the work the internal auditor performs for us. We have not used their assistance in the past and do not plan to use it in 2025.

Dissemination of Financial Statements

Our report on the financial statements must be associated only with the financial statements that were the subject of our engagement. You may make copies of our report, but only if the entire financial statements (including related footnotes and supplementary information, as appropriate) are reproduced and distributed with our report. You agree not to reproduce or associate our report with any other financial statements, or portions thereof, that are not the subject of this engagement.

The Firm acknowledges that the City may post audited financial statements, including our report, on their website to satisfy legal requirements, including to satisfy Freedom of Information Act or other public records requests, and we acknowledge that neither this Engagement Letter nor the Agreement prohibits the City from doing so. Any posting on the City's website is not intended to expand any intended users of the report, to extend any duty or obligation from the Firm to any third party, to create privity between the Firm and any third party, nor to create any third-party beneficiaries of this Engagement Letter or the Agreement. The Firm shall place any disclaimer related to non-reliance that it deems necessary. The Firm has no obligation to review any such website posting, nor to monitor or correct any errors therein, nor to consider the consistency with the Report of any other information on such site.

Offering of Securities

This Engagement Letter does not contemplate the Firm providing any services in connection with the offering of securities, whether registered or exempt from registration, and the Firm will charge additional fees to provide any such services. You further agree we are under no obligation to reissue our report or provide written permission for any other use of our report at a later date in connection with an offering of securities, the issuance of debt instruments, or for any other circumstance. We will determine, at our sole discretion, whether we will reissue our report or provide written permission for the use of our report only after we have conducted any procedures we deem necessary in the circumstances. You agree to provide us with adequate time to review documents where (a) our report is requested to be reissued, or (b) if you request written permission for other uses of the report. If we decide to reissue our report or provide written permission to the use of our report, you agree that the Firm will be included on each distribution of draft offering materials and we will receive a complete set of final documents. If we decide not to reissue our report or withhold our written permission to use our report, you may be required to engage another firm to audit periods covered by our audit reports, and that firm will likely bill you for its services.



Timothy O'Brien, CPA, Denver Auditor's Office
Audit Committee
City and County of Denver
October 7, 2025
Page 7 of 10

Changes in Professional or Accounting Standards

To the extent that future federal, state, or professional rule-making activities require modification of our audit approach, procedures, scope of work, etc., we will advise you of such changes and the impact on our fee estimate. If we are unable to agree on the additional fees, if any, that may be required to implement any new accounting and auditing standards that are required to be adopted and applied as part of our engagement, we may terminate this Engagement Letter as provided herein, regardless of the stage of completion.

Representations of Management

During the course of our engagement, we may request information and explanations from management regarding, among other matters, the Airport Fund's operations, internal control, future plans, specific transactions, and accounting systems and procedures. At the conclusion of our engagement, we will require, as a precondition to the issuance of our report, that management provide us with a written representation letter confirming some or all of the representations made during the engagement. The procedures that we will perform in our engagement will be heavily influenced by the representations that we receive from management. Accordingly, false representations could cause us to expend unnecessary efforts or could cause a material error or fraud to go undetected by our procedures. In view of the foregoing, you agree that we will not be responsible for any misstatements in the Airport Fund's financial statements that we fail to detect as a result of false or misleading representations, whether oral or written, that are made to us by the Airport Fund's management. While we may assist management in the preparation of the representation letter, it is management's responsibility to carefully review and understand the representations made therein.

In addition, because our failure to detect material misstatements could cause others relying upon our audit report to incur damages, the Airport Fund further agrees that the Firm may not be held liable by the City for any claims based upon our failure to detect material misstatements in the Airport Fund's financial statements resulting in whole or in part from knowingly false or misleading representations made to us by any member of the Airport Fund's management.

Use of the Firm's Name

Except as otherwise addressed in this Engagement Letter, the City may not use any of the Firm's name, trademarks, service marks or logo in connection with the services contemplated by this Agreement or otherwise without the prior written permission of the Firm, which permission may be withheld for any or no reason and may be subject to certain conditions.

Use of Nonlicensed Personnel

Certain engagement personnel who are not licensed as certified public accountants may provide services during this engagement.

Hiring of Employees

Any offer of employment to members of the audit team prior to issuance of our report may impair our independence, and as a result, may result in our inability to complete the engagement and issue a report.



Timothy O'Brien, CPA, Denver Auditor's Office
Audit Committee
City and County of Denver
October 7, 2025
Page 8 of 10

Data Privacy and Security

Subject to the terms of the Agreement, to the extent the Services require the Firm to receive personal data or personal information from Company, the Firm may process, and engage subcontractors to assist with processing, any personal data or personal information, as those terms are defined in applicable privacy laws, and such processing shall be in accordance with the requirements of the applicable privacy laws relevant to the processing in providing Services hereunder, including Services performed to meet the business purposes of the Company, such as the Firm's tax, advisory, and other consulting services. Applicable privacy laws may include any local, state, federal or international laws, standards, guidelines, policies or regulations governing the collection, use, disclosure, sharing or other processing of personal data or personal information with which the Firm or its clients must comply. Such privacy laws may include (i) the EU General Data Protection Regulation 2016/679 (GDPR); (ii) the California Consumer Privacy Act of 2018 (CCPA); and/or (iii) other laws regulating marketing communications, requiring security breach notification, imposing minimum security requirements, requiring the secure disposal of records, and other similar requirements applicable to the processing of personal data or personal information. The Firm is acting as a Service Provider/Data Processor, as those terms are defined respectively under the CCPA/GDPR, in relation to Company personal data and personal information. As a Service Provider/Data Processor processing personal data or personal information on behalf of Company, the Firm shall, unless otherwise permitted by applicable privacy law, (a) follow Company instructions; (b) not sell personal data or personal information collected from the Company or share the personal data or personal information for purposes of targeted advertising; (c) process personal data or personal information solely for purposes related to the Company's engagement and not for the Firm's own commercial purposes; and (d) cooperate with and provide reasonable assistance to Company to ensure compliance with applicable privacy laws. Company is responsible for notifying the Firm of any applicable privacy laws the personal data or personal information provided to the Firm is subject to, and Company represents and warrants it has all necessary authority (including any legally required consent from individuals) to transfer such information and authorize the Firm to process such information in connection with the Services described herein. Company further understands the Firm, Baker Tilly Advisory Group, LP and Moss Adams Advisory Group, LP and their affiliated entities (collectively, the "Firm Entities") may coprocess Company data as necessary to perform the Services, pursuant to the alternative practice structure in place among the entities, and by executing this Agreement, you hereby consent to the sharing of Company data, Company files, workpapers and work product with such Firm Entities. Baker Tilly Advisory Group, LP maintains custody of client files for the Firm. The Firm Entities are bound by the same confidentiality obligations as the Firm. The Firm is responsible for notifying Company if the Firm becomes aware that it can no longer comply with any applicable privacy law and, upon such notice, shall permit Company to take reasonable and appropriate steps to remediate personal data or personal information processing. Company agrees that the Firm Entities have the right to utilize Company data to improve internal processes and procedures and to generate aggregated/deidentified data from the data provided by Company to be used for the Firm Entities' business purposes and with the outputs owned by the Firm Entities. For clarity, the Firm Entities will only disclose aggregated/deidentified data in a form that does not identify Company, Company employees, or any other individual or business entity and that is stripped of all persistent identifiers. Company is not responsible for the Firm Entities' use of aggregated/deidentified data.

The Firm has established information security related operational requirements that support the achievement of our information security commitments, relevant information security related laws and regulations and other information security related system requirements. Such requirements are documented in the Firm's policies and procedures. Information security policies have been implemented that define our approach to how systems and data are protected. Company is responsible for providing timely written notification to the Firm of any additions, changes or removals of access for Company personnel to the Firm provided systems or applications. If Company becomes aware of any known or suspected information



Timothy O'Brien, CPA, Denver Auditor's Office
Audit Committee
City and County of Denver
October 7, 2025
Page 9 of 10

security or privacy related incidents or breaches related to this Agreement, Company should timely notify the Firm via email at dataprotectionofficer@bakertilly.com.

Alternative Practice Structure: Baker Tilly International

Baker Tilly US, LLP and Baker Tilly Advisory Group, LP and its subsidiary entities provide professional services through an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable laws, regulations and professional standards. Baker Tilly US, LLP is a licensed independent CPA firm that provides attest services to clients. Baker Tilly Advisory Group, LP and its subsidiary entities provide tax and business advisory services to their clients. Baker Tilly Advisory Group, LP and its subsidiary entities are not licensed CPA firms.

Baker Tilly Advisory Group, LP and its subsidiaries and Baker Tilly US, LLP, trading as Baker Tilly, are independent members of Baker Tilly International. Baker Tilly International Limited is an English company. Baker Tilly International provides no professional services to clients. Each member firm is a separate and independent legal entity and each describes itself as such. Baker Tilly Advisory Group, LP and Baker Tilly US, LLP are not Baker Tilly International's agents and do not have the authority to bind Baker Tilly International or act on Baker Tilly International's behalf. None of Baker Tilly International, Baker Tilly Advisory Group, LP, Baker Tilly US, LLP, nor any of the other member firms of Baker Tilly International has any liability for each other's acts or omissions. The name Baker Tilly and its associated logo is used under license from Baker Tilly International Limited.

Timing

Olga A. Darlington, Principal, is responsible for supervising the engagement and authorizing the signing of the report. Any substantive change in staffing will be discussed and approved with the City as part of the engagement. We expect to begin our interim audit fieldwork on November 10, 2025, start final fieldwork on April 13, 2026, and issue our report no later than May 31, 2026. Our scheduling depends on your completion of the year-end closing and adjusting process prior to our arrival to begin the fieldwork. We may experience delays in completing our services due to your staff's unavailability or delays in your closing and adjusting process. You understand our fees are subject to adjustment if we experience these delays in completing our services.

Fees

Our fees for the audit services for the year ending December 31, 2025, will be \$199,000. Our ability to provide services in accordance with our estimated fees depends on the quality, timeliness, and accuracy of the Airport Fund's records, and, for example, the number of general ledger adjustments required as a result of our work. To assist you in this process, we will provide you with a Client Audit Preparation Schedule that identifies the key work you will need to perform in preparation for the audit. We will also need your accounting staff to be readily available during the engagement to respond in a timely manner to our requests.

Reporting

We will issue a written report upon completion of our audit of the Airport Fund's financial statements. Our report will be addressed to the Audit Committee and the City and County of Denver. We cannot provide assurance that an unmodified opinion will be expressed. Circumstances may arise in which it is necessary for us to modify our opinion, add an emphasis-of-matter or other-matter paragraph(s), or withdraw from the engagement. Our services will be concluded upon delivery to you of our report on your financial statements for the year ending December 31, 2025.



Timothy O'Brien, CPA, Denver Auditor's Office
Audit Committee
City and County of Denver
October 7, 2025
Page 10 of 10

We also will issue a written report on the Passenger Facility Charge Program for the year ending December 31, 2025, upon completion of our audit.

Other Information in an Annual Report with Audited Financial Statements

It is our understanding that the Airport Fund's Annual Comprehensive Financial Report will contain or incorporate by reference the financial statements and our auditor's report thereon. We further understand that the Airport Fund plans to issue such documents on its website on or before May 31, 2026. You agree to provide the final version of the document(s) comprising the annual report as soon as it is available. If some or all of the documents will not be available until after the date of the auditor's report on the financial statements, we will request a written representation from management at the conclusion of the audit that asserts the final version of the Annual Comprehensive Financial Report will be provided to us when available, and prior to issuance by the Airport Fund.

We appreciate the opportunity to be of service to you. If you agree with the terms of our engagement as set forth in the Agreement, please sign the enclosed copy of this letter and return it to us with the Professional Services Agreement.

Very truly yours,

Baker Tilly US, LLP

Enclosures

Accepted and Agreed:

This Engagement Letter and the attached Professional Services Agreement set forth the entire understanding of the City and County of Denver with respect to this engagement and the services to be provided by the Firm:

Signature: _____

Print Name: Timothy O'Brien

Title: City Auditor

Date: _____

APPENDIX I,
BUSINESS ASSOCIATE AGREEMENT
HIPAA/HITECH

1. GENERAL PROVISIONS AND RECITALS.

- 1.01 The parties agree that the terms used, but not otherwise defined below, shall have the same meaning given to such terms under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and their implementing regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations") as they exist or may hereafter be amended.
- 1.02 The parties agree that a business associate relationship (as described in 45 CFR §160.103) under HIPAA, the HITECH Act, and the HIPAA regulations arises between the CONTRACTOR and the CITY to the extent that CONTRACTOR performs, or delegates to subcontractors to perform, functions or activities on behalf of CITY.
- 1.03 CITY wishes to disclose to CONTRACTOR certain information, some of which may constitute Protected Health Information ("PHI") as defined below, to be used or disclosed in the course of providing services and activities.
- 1.04 The parties intend to protect the privacy and provide for the security of PHI that may be created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement in compliance with the applicable standards, implementation specifications, and requirements of HIPAA, the HITECH Act, and the HIPAA regulations as they exist or may hereafter be amended.
- 1.05 The parties understand and acknowledge that HIPAA, the HITECH Act, and the HIPAA regulations do not pre-empt any state statutes, rules, or regulations that impose more stringent requirements with respect to privacy of PHI.
- 1.06 The parties understand that the HIPAA Privacy and Security rules apply to the CONTRACTOR in the same manner as they apply to a covered entity. CONTRACTOR agrees to comply at all times with the terms of this Agreement and the applicable standards, implementation specifications, and requirements of the Privacy and the Security rules, as they exist or may hereafter be amended, with respect to PHI.

2. DEFINITIONS.

- 2.01 "Administrative Safeguards" are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of CONTRACTOR's workforce in relation to the protection of that information.
- 2.02 "Agreement" means the attached Agreement and its exhibits to which these additional terms are incorporated by reference.
- 2.03 "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

2.03.1 Breach excludes:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of CONTRACTOR or CITY, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI, or organized health care arrangement in which CITY participates, and the information received as a result of such disclosure is not further used or disclosed in a manner disallowed under the HIPAA Privacy Rule.
3. A disclosure of PHI where CONTRACTOR or CITY has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.03.2 Except as provided in paragraph (a) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless CONTRACTOR demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

2.04 "CONTRACTOR" shall have the same meaning as in the attached Agreement, to which these Business Associate terms are incorporated by reference.

2.05 "CITY" shall have the same meaning as in the attached Agreement, to which these Business Associate terms are incorporated by reference.

2.06 "Data Aggregation" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.07 "Designated Record Set" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.08 "Disclosure" shall have the meaning given to such term under the HIPAA regulations in 45 CFR §160.103.

2.09 "Health Care Operations" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

- 2.10 "Immediately" where used here shall mean within 72 hours of discovery.
- 2.11 "Individual" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).
- 2.12 "Parties" shall mean "CONTRACTOR" and "CITY", collectively.
- 2.13 "Physical Safeguards" are physical measures, policies, and procedures to protect CONTRACTOR's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
- 2.14 "The HIPAA Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
- 2.15 "Protected Health Information" or "PHI" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103, limited to the information created or received by CONTRACTOR from or on behalf of CITY.
- 2.16 "Required by Law" shall have the meaning given to such term under the HIPAA Privacy Rule at 45 CFR §164.103.
- 2.17 "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.
- 2.18 "Security Incident" means attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. "Security incident" does not include trivial incidents that occur on a daily basis, such as scans, "pings", or unsuccessful attempts to penetrate computer networks or servers maintained by CONTRACTOR.
- 2.19 "The HIPAA Security Rule" shall mean the Security Standards for the Protection of electronic PHI at 45 CFR Part 160, Part 162, and Part 164, Subparts A and C.
- 2.20 "Subcontractor" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.
- 2.21 "Technical safeguards" means the technology and the policy and procedures for its use that protect electronic PHI and control access to it.
- 2.22 "Unsecured PHI" or "PHI that is unsecured" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services ("HHS") in the guidance issued on the HHS Web site.
- 2.23 "Use" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.

3. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE.

- 3.01 CONTRACTOR agrees not to use or further disclose PHI that CITY discloses to CONTRACTOR except as permitted or required by this Agreement or by law.
- 3.02 CONTRACTOR agrees to use appropriate safeguards, as provided for in this Agreement, to prevent use or disclosure of PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits, on behalf of CITY, except as provided for by this Contract.
- 3.03 CONTRACTOR agrees to comply with the HIPAA Security Rule, at Subpart C of 45 CFR Part 164, with respect to electronic PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits, on behalf of CITY.
- 3.04 CONTRACTOR agrees to mitigate, to the extent practicable, any harmful effect of a Use or Disclosure of PHI by CONTRACTOR in violation of the requirements of this Agreement that becomes known to CONTRACTOR.
- 3.05 CONTRACTOR agrees to immediately report to CITY any unauthorized Use or Disclosure of unsecured PHI not provided for by this Agreement that CONTRACTOR becomes aware of. CONTRACTOR must report Breaches of Unsecured PHI in accordance with 45 CFR §164.410.
- 3.06 CONTRACTOR agrees to require that any of its subcontractors that create, receive, maintain, or transmit, PHI on behalf of CONTRACTOR agree to comply with the applicable requirements of Section 164 Part C by entering into a contract or other arrangement.
- 3.07 To comply with the requirements of 45 CFR §164.524, CONTRACTOR agrees to provide access to CITY, or to an individual as directed by CITY, to PHI in a Designated Record Set within fifteen (15) calendar days of receipt of a written request by CITY.
- 3.08 CONTRACTOR agrees to make amendment(s) to PHI in a Designated Record Set that CITY directs or agrees to, pursuant to 45 CFR §164.526, at the request of CITY or an Individual, within thirty (30) calendar days of receipt of the request by CITY. CONTRACTOR agrees to notify CITY in writing no later than ten (10) business days after the amendment is completed.
- 3.09 CONTRACTOR agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by CONTRACTOR on behalf of CITY, available to the Secretary in a time and as designated by the Secretary, for purposes of the Secretary determining CITY'S compliance with the HIPAA Privacy Rule.
- 3.10 CONTRACTOR agrees to document any Disclosures of PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits on behalf of CITY, and to make information related to such Disclosures available as would be required for CITY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR §164.528.
- 3.11 CONTRACTOR agrees to provide CITY information in a time and manner to be determined by CITY in order to permit CITY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR §164.528.

- 3.12 CONTRACTOR agrees that, to the extent CONTRACTOR carries out CITY's obligation(s) under the HIPAA Privacy and/or Security rules, CONTRACTOR will comply with the requirements of 45 CFR Part 164 that apply to CITY in the performance of such obligation(s).
- 3.13 CONTRACTOR shall work with CITY upon notification by CONTRACTOR to CITY of a Breach to properly determine if any Breach exclusions exist as defined below.

4. SECURITY RULE.

- 4.01 CONTRACTOR shall comply with the requirements of 45 CFR § 164.306 and establish and maintain appropriate Administrative, Physical and Technical Safeguards in accordance with 45 CFR §164.308, §164.310, §164.312, §164.314 and §164.316 with respect to electronic PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits on behalf of CITY. CONTRACTOR shall follow generally accepted system security principles and the requirements of the HIPAA Security Rule pertaining to the security of electronic PHI.
- 4.02 CONTRACTOR shall require that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of CONTRACTOR agree through a contract with CONTRACTOR to substantially the same restrictions and requirements contained here.
- 4.03 CONTRACTOR shall promptly, but in no event later than five (5) business days, report to CITY any Security Incident of which it becomes aware. CONTRACTOR shall report Breaches of Unsecured PHI as described in 5. BREACH DISCOVERY AND NOTIFICATION below and as required by 45 CFR §164.410.

5. BREACH DISCOVERY AND NOTIFICATION.

- 5.01 Following the discovery of a Breach of Unsecured PHI, CONTRACTOR shall notify CITY of such Breach, however, both parties may agree to a delay in the notification if so advised by a law enforcement official pursuant to 45 CFR §164.412.
 - 5.01.1 A Breach shall be treated as discovered by CONTRACTOR as of the first day on which such Breach is known to CONTRACTOR or, by exercising reasonable diligence, would have been known to CONTRACTOR.
 - 5.01.2 CONTRACTOR shall be deemed to have knowledge of a Breach, if the Breach is known, or by exercising reasonable diligence would have been known, to any person who is an employee, officer, or other agent of CONTRACTOR, as determined by the federal common law of agency.
- 5.02 CONTRACTOR shall provide the notification of the Breach promptly, but in no event later than five (5) business days, to the CITY DEH Executive Director or other designee.
 - 5.02.1 CONTRACTOR'S initial notification may be oral, but shall be followed by written notification no later than five (5) business days of the oral notification.
- 5.03 CONTRACTOR'S notification shall include, to the extent possible:

- 5.03.1 The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by CONTRACTOR to have been, accessed, acquired, used, or disclosed during the Breach;
- 5.03.2 Any other information that CITY is required to include in the notification to each Individual under 45 CFR §164.404 (c) at the time CONTRACTOR is required to notify CITY, or promptly thereafter as this information becomes available, even after the regulatory sixty (60) day period set forth in 45 CFR §164.410 (b) has elapsed, including:
 1. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
 2. A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
 3. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;
 4. A brief description of what CONTRACTOR is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any future Breaches; and
 5. Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.
- 5.04 CITY may require CONTRACTOR to provide notice to the Individual as required in 45 CFR §164.404, if at the sole discretion of the CITY, it is reasonable to do so under the circumstances.
- 5.05 In the event that CONTRACTOR is responsible for a Breach of Unsecured PHI in violation of the HIPAA Privacy Rule, CONTRACTOR shall have the burden of demonstrating that CONTRACTOR made all required notifications to CITY, and as required by the Breach notification regulations, or, in the alternative, that the acquisition, access, use, or disclosure of PHI did not constitute a Breach.
- 5.06 CONTRACTOR shall maintain documentation of all required notifications of a Breach or its risk assessment under 45 CFR §164.402 to demonstrate that a Breach did not occur.
- 5.07 CONTRACTOR shall provide to CITY all specific and pertinent information about the Breach, including the information listed above, if not yet provided, to permit CITY to meet its notification obligations under Subpart D of 45 CFR Part 164 as soon as practicable, but in no event later than fifteen (15) calendar days after CONTRACTOR's initial report of the Breach to CITY.
- 5.08 CONTRACTOR shall continue to provide all additional pertinent information about the Breach to CITY as it becomes available, in reporting increments of five (5) business days after the prior report to CITY. CONTRACTOR shall also respond in good faith to all reasonable requests for further information, or follow-up information, after report to CITY, when such request is made by CITY.

- 5.09 In addition to the provisions in the body of the Agreement, CONTRACTOR shall be responsible for the following remediate actions to the extent required by law: (i) preparation and distribution of legally required notice of a breach to individuals affected by the unauthorized access, disclosure, compromise, alteration or loss of the data that includes that individual's personal data; (ii) preparation and distribution of legally required notice of a breach to government agencies and/or other required entities; (iii) the costs of set-up and maintenance of a customer service support center related to the breach (including but not limited to the costs of human resources); and (iv) credit monitoring services designed to protect against potential fraud associated with identity theft crimes for a specific period not to exceed twelve (12) months or such longer period as required by applicable law.

6. PERMITTED USES AND DISCLOSURES BY CONTRACTOR.

- 6.01 CONTRACTOR may use or further disclose PHI that CITY discloses to CONTRACTOR as necessary to perform functions, activities, or services for, or on behalf of, CITY as specified in the Agreement, provided that such use or Disclosure would not violate the HIPAA Privacy Rule if done by CITY.
- 6.02 CONTRACTOR may use PHI that CITY discloses to CONTRACTOR, if necessary, for the proper management and administration of the Agreement.
- 6.03 CONTRACTOR may disclose PHI that CITY discloses to CONTRACTOR to carry out the legal responsibilities of CONTRACTOR, if:
 - 6.03.1 The Disclosure is required by law; or
 - 6.03.2 CONTRACTOR obtains reasonable assurances from the person or entity to whom/which the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person or entity and the person or entity immediately notifies CONTRACTOR of any instance of which it is aware in which the confidentiality of the information has been breached.
- 6.04 CONTRACTOR may use or further disclose PHI that CITY discloses to CONTRACTOR to provide Data Aggregation services relating to the Health Care Operations of CONTRACTOR.
- 6.05 CONTRACTOR may use and disclose PHI that CITY discloses to CONTRACTOR consistent with HIPAA's minimum necessary standards.

7. OBLIGATIONS OF CITY.

- 7.01 CITY shall notify CONTRACTOR of any limitation(s) in CITY'S notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect CONTRACTOR'S Use or Disclosure of PHI.
- 7.02 CITY shall notify CONTRACTOR of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect CONTRACTOR'S Use or Disclosure of PHI.
- 7.03 CITY shall notify CONTRACTOR of any restriction to the Use or Disclosure of PHI that CITY has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect

CONTRACTOR'S use or disclosure of PHI. In the event CONTRACTOR deems in its sole discretion it cannot comply with any such limitations, changes, revocation, or additional restrictions, described in Sections 7.01, 7.02, or 7.03, CONTRACTOR will notify the CITY and terminate this Agreement.

7.04 CITY shall not request CONTRACTOR to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by CITY.

8. BUSINESS ASSOCIATE TERMINATION.

8.01 Upon CITY'S knowledge of a material breach or violation by CONTRACTOR of the requirements of this Contract, CITY shall:

8.01.1 Provide an opportunity for CONTRACTOR to cure the material breach or end the violation within thirty (30) business days; or

8.01.2 Immediately terminate the Agreement, if CONTRACTOR is unwilling or unable to cure the material breach or end the violation within (30) days, provided termination of the Agreement is feasible.

8.02 Upon termination of the Agreement, CONTRACTOR shall either destroy or return to CITY all PHI CONTRACTOR received from CITY and any and all PHI that CONTRACTOR created, maintained, or received on behalf of CITY in conformity with the HIPAA Privacy Rule.

8.02.1 This provision shall apply to all PHI that is in the possession of subcontractors or agents of CONTRACTOR.

8.02.2 CONTRACTOR shall retain no copies of the PHI, except one copy which CONTRACTOR may require to conform with its internal records retention policies.

8.02.3 In the event that CONTRACTOR determines that returning or destroying the PHI is not feasible, CONTRACTOR shall provide to CITY notification of the conditions that make return or destruction infeasible. Upon determination by CITY that return or destruction of PHI is infeasible, CONTRACTOR shall extend the protections of this Agreement to the PHI and limit further Uses and Disclosures of the PHI to those purposes that make the return or destruction infeasible, for as long as CONTRACTOR maintains the PHI. Notwithstanding the foregoing, or anything in this Appendix to the contrary, the parties agree that it is infeasible for CONTRACTOR to return or destroy Protected Health Information to the extent incorporated into its working papers consistent with recordkeeping policy and commercially reasonable and applicable industry standard supporting its professional services for CITY, and no further notice shall be required as to such working papers.

8.03 The obligations of this Agreement shall survive the termination of the Agreement.

EXHIBIT C-1

(exhibit follows)



CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
01/12/2026

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Aon Risk Services Northeast, Inc. New York NY Office One Liberty Plaza 165 Broadway, Suite 3201 New York NY 10006 USA	CONTACT NAME: PHONE (A/C. No. Ext): (312) 381-1000 FAX (A/C. No.): (312) 381-7007 E-MAIL ADDRESS:														
INSURED Baker Tilly US, LLP & Baker Tilly Advisory Group, LP P.O. Box 7398 4807 Innovate Lane Madison WI 53707-7398 USA	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 80%;">INSURER(S) AFFORDING COVERAGE</th> <th style="width: 20%;">NAIC #</th> </tr> </thead> <tbody> <tr> <td>INSURER A: National Fire Ins. Co. of Hartford</td> <td>20478</td> </tr> <tr> <td>INSURER B: The Continental Insurance Company</td> <td>35289</td> </tr> <tr> <td>INSURER C: Valley Forge Insurance Co</td> <td>20508</td> </tr> <tr> <td>INSURER D:</td> <td></td> </tr> <tr> <td>INSURER E:</td> <td></td> </tr> <tr> <td>INSURER F:</td> <td></td> </tr> </tbody> </table>	INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A: National Fire Ins. Co. of Hartford	20478	INSURER B: The Continental Insurance Company	35289	INSURER C: Valley Forge Insurance Co	20508	INSURER D:		INSURER E:		INSURER F:	
INSURER(S) AFFORDING COVERAGE	NAIC #														
INSURER A: National Fire Ins. Co. of Hartford	20478														
INSURER B: The Continental Insurance Company	35289														
INSURER C: Valley Forge Insurance Co	20508														
INSURER D:															
INSURER E:															
INSURER F:															

Holder Identifier :

COVERAGES CERTIFICATE NUMBER: 570117608491 REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS. Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS												
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input checked="" type="checkbox"/> LOC OTHER:			C6016751638 General Liability	01/01/2026	01/01/2027	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>EACH OCCURRENCE</td><td style="text-align: right;">\$1,000,000</td></tr> <tr><td>DAMAGE TO RENTED PREMISES (Ea occurrence)</td><td style="text-align: right;">\$1,000,000</td></tr> <tr><td>MED EXP (Any one person)</td><td style="text-align: right;">\$5,000</td></tr> <tr><td>PERSONAL & ADV INJURY</td><td style="text-align: right;">\$1,000,000</td></tr> <tr><td>GENERAL AGGREGATE</td><td style="text-align: right;">\$2,000,000</td></tr> <tr><td>PRODUCTS - COMP/OP AGG</td><td style="text-align: right;">\$2,000,000</td></tr> </table>	EACH OCCURRENCE	\$1,000,000	DAMAGE TO RENTED PREMISES (Ea occurrence)	\$1,000,000	MED EXP (Any one person)	\$5,000	PERSONAL & ADV INJURY	\$1,000,000	GENERAL AGGREGATE	\$2,000,000	PRODUCTS - COMP/OP AGG	\$2,000,000
EACH OCCURRENCE	\$1,000,000																		
DAMAGE TO RENTED PREMISES (Ea occurrence)	\$1,000,000																		
MED EXP (Any one person)	\$5,000																		
PERSONAL & ADV INJURY	\$1,000,000																		
GENERAL AGGREGATE	\$2,000,000																		
PRODUCTS - COMP/OP AGG	\$2,000,000																		
A	<input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input checked="" type="checkbox"/> NON-OWNED AUTOS ONLY			BUA 6016751641 Auto	01/01/2026	01/01/2027	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>COMBINED SINGLE LIMIT (Ea accident)</td><td style="text-align: right;">\$1,000,000</td></tr> <tr><td>BODILY INJURY (Per person)</td><td></td></tr> <tr><td>BODILY INJURY (Per accident)</td><td></td></tr> <tr><td>PROPERTY DAMAGE (Per accident)</td><td></td></tr> </table>	COMBINED SINGLE LIMIT (Ea accident)	\$1,000,000	BODILY INJURY (Per person)		BODILY INJURY (Per accident)		PROPERTY DAMAGE (Per accident)					
COMBINED SINGLE LIMIT (Ea accident)	\$1,000,000																		
BODILY INJURY (Per person)																			
BODILY INJURY (Per accident)																			
PROPERTY DAMAGE (Per accident)																			
B	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input type="checkbox"/> RETENTION			CUE6016723001 Umbrella	01/01/2026	01/01/2027	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>EACH OCCURRENCE</td><td style="text-align: right;">\$5,000,000</td></tr> <tr><td>AGGREGATE</td><td style="text-align: right;">\$5,000,000</td></tr> </table>	EACH OCCURRENCE	\$5,000,000	AGGREGATE	\$5,000,000								
EACH OCCURRENCE	\$5,000,000																		
AGGREGATE	\$5,000,000																		
B B C	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N N	N/A	WC6016751624 WC6023746823 WC6043413436 Workers Compensation	01/01/2026 01/01/2026 01/01/2026	01/01/2027 01/01/2027 01/01/2027	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td><input checked="" type="checkbox"/> PER STATUTE</td><td style="text-align: center;">O-T-H-E-R</td><td></td></tr> <tr><td>E.L. EACH ACCIDENT</td><td></td><td style="text-align: right;">\$1,000,000</td></tr> <tr><td>E.L. DISEASE-EA EMPLOYEE</td><td></td><td style="text-align: right;">\$1,000,000</td></tr> <tr><td>E.L. DISEASE-POLICY LIMIT</td><td></td><td style="text-align: right;">\$1,000,000</td></tr> </table>	<input checked="" type="checkbox"/> PER STATUTE	O-T-H-E-R		E.L. EACH ACCIDENT		\$1,000,000	E.L. DISEASE-EA EMPLOYEE		\$1,000,000	E.L. DISEASE-POLICY LIMIT		\$1,000,000
<input checked="" type="checkbox"/> PER STATUTE	O-T-H-E-R																		
E.L. EACH ACCIDENT		\$1,000,000																	
E.L. DISEASE-EA EMPLOYEE		\$1,000,000																	
E.L. DISEASE-POLICY LIMIT		\$1,000,000																	

Certificate No : 570117608491

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
 City and County of Denver its elected and appointed officials, employees and volunteers are added as Additional Insured as respects the General Liability and Automobile Liability as required per written contract. A waiver of subrogation in favor of Additional Insured as respect the General Liability, Auto Liability and Workers Compensation pursuant to a written contract.

CERTIFICATE HOLDER City and County of Denver 201 W. Colfax Avenue Denver CO 80202 USA	CANCELLATION SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE <div style="text-align: center; font-family: cursive;"> Aon Risk Services Northeast, Inc. </div>
---	--



CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
10/01/2025

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Aon Risk Services Northeast, Inc. One Liberty Plaza, 165 Broadway, Suite 3201 New York, N.Y. 10006	CONTACT NAME: PHONE (A/C. No. Ext): 312-381-1000 FAX (A/C. No) 312-381-7007 E-MAIL ADDRESS: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 80%;">INSURER(S) AFFORDING COVERAGE</th> <th style="width: 20%;">NAIC #</th> </tr> <tr> <td>INSURER A: Columbia Casualty Company</td> <td></td> </tr> <tr> <td>INSURER B:</td> <td></td> </tr> <tr> <td>INSURER C:</td> <td></td> </tr> <tr> <td>INSURER D:</td> <td></td> </tr> <tr> <td>INSURER E:</td> <td></td> </tr> <tr> <td>INSURER F:</td> <td></td> </tr> </table>	INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A: Columbia Casualty Company		INSURER B:		INSURER C:		INSURER D:		INSURER E:		INSURER F:	
INSURER(S) AFFORDING COVERAGE	NAIC #														
INSURER A: Columbia Casualty Company															
INSURER B:															
INSURER C:															
INSURER D:															
INSURER E:															
INSURER F:															
INSURED Baker Tilly US, LLP & Baker Tilly Advisory Group, LP P.O. Box 7398 4807 Innovate Lane Madison WI 53707-7398 USA															

COVERAGES

CERTIFICATE NUMBER:

REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS. Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
	COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> OCCUR <hr/> GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PROJECT <input type="checkbox"/> LOC OTHER:						EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG
	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)
	<input type="checkbox"/> UMBRELLA LIAB <input type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input type="checkbox"/> RETENTION						EACH OCCURRENCE AGGREGATE
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y / N	N / A				<input type="checkbox"/> PER STATUTE <input type="checkbox"/> OTHER E.L. EACH ACCIDENT E.L. DISEASE-EA EMPLOYEE E.L. DISEASE-POLICY LIMIT
A	Professional Liability Insurance			ABF-188122608	01-Oct-25	01-Oct-26	Not less than US \$1,000,000 per claim and in the annual aggregate.

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER

CANCELLATION

City and County of Denver 201 W. Colfax Avenue, 705 Denver, CO, 80202	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE <i>Aon Risk Services Northeast, Inc.</i>
---	---