FIFTH AMENDATORY AGREEMENT

THIS FIFTH 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 **FAST ENTERPRISES, LLC**, a limited liability company registered to do business in Colorado, whose address is 7229 S. Alton Way, Centennial, CO 80112, (the "Contractor"), collectively "the parties".

WITNESSETH:

A. The City and Contractor entered into an Agreement dated January 13, 2009, as amended by Amendatory Agreement dated June 25, 2012, Second Amendatory Agreement dated December 14, 2014, a Third Amendatory Agreement dated November 20, 2015, and a Fourth Amendatory Agreement dated December 13, 2018 (collectively the "Agreement").

B. The City and Contractor wish to amend the Agreement to extend the term, and increase the maximum contract amount, and expand the scope of the service to include the FAST Audit Service, a cloud based product, as set forth below.

C. The FAST Audit Service is managed by a third party and is provided by Contractor through this Amendment. The terms governing the delivery of the FAST Audit Service are set out in the document entitled FAST DATA SERVICES SUBSCRIBER AGREEMENT, attached hereto and incorporated herein along with the document entitled ATTACHMENT 1, attached hereto and incorporated herein.

The preceding statements are binding upon the parties and are incorporated into this Amendment. The parties agree as follows:

1. Exhibit A-6, entitled "quote –07/06/2021" attached to this Fifth Amendatory Agreement and incorporated herein by this reference, sets forth the maximum amounts to be paid for maintenance and supportservices for the period beginning January 1, 2022 through December 31, 2026. All references to "…Exhibit A…" in the Agreement shall be amended to read: "Exhibit A, A-1, A-2, A-3, A-4, A-5, and A-6 as applicable…".

2. All references to "…Exhibit B…" in the Agreement shall be amended to read: "…Exhibit B and B-1…" as applicable. The statement of work marked as Exhibit B-1 attached to this Amendatory Agreement is hereby incorporated by reference.

3. Paragraph 2 of the Agreement, entitled "**TERM**", is amended to read as follows:

"2. TERM:
The Term of this Agreement shall commence on January 13, 2009 and shall expire on December 31, 2026.

4. Paragraph **3.D.1** of the Agreement, entitled "**Maximum Contract Liability**", is amended to read as follows:

"**D. Maximum Contract Liability:**

(1) Any other provision of this Agreement notwithstanding, in no event shall the City be liable to pay for services rendered and expenses incurred by the Contractor under the terms of this Agreement, if all Renewal Terms are exercised, for any amount in excess of **Twenty-Four Million Twenty-Six Thousand Five Hundred Dollars ($24,026,500.00)** (the "Maximum Contract Amount") payable in accordance with Exhibits A, A-1, A-2, A-3, A-4, A-5, and A-6. The Contractor acknowledges that the City is not obligated to execute an amendment to this Agreement for any services and that any services performed by the Contractor beyond that specifically described herein are performed at Contractor's risk and without authorization under this Agreement.

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

6. This Fifth Amendatory Agreement will not be effective or binding on the City until it has been fully executed by all required signatories of the City and County of Denver, and if required by Charter, approved by the City Council.

[SIGNATURE PAGES AND EXHIBITS A-6 AND B-1 FOLLOW THIS PAGE]

Contract Control Number: TECHS-202159876-05 (CE06001-05)
Contractor Name: FAST ENTERPRISES LLC

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

SEAL

CITY AND COUNTY OF DENVER:

ATTEST:

By: _____

_____

APPROVED AS TO FORM:

Attorney for the City and County of Denver

By: _____

REGISTERED AND COUNTERSIGNED:

By: _____

By: _____

Contract Control Number: TECHS-202159876-05 (CE06001-05)
Contractor Name: FAST ENTERPRISES LLC

By: DocuSigned by: James G. Harrison D7ED57F740404E7...

Name: James G. Harrison
(please print)

Title: Member
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)

QUOTE

To: Joe Saporito and Kelly Petersen, City and County of Denver, Colorado
From: Nikki Nguyen
CC: Eric Deffenbaugh
Date: 7/6/2021
Re: Quote for Maintenance, Production Support, and FAST Audit Services

Joe and Kelly,

Thank you for allowing FAST to continue supporting the City and County of Denver and your interest in FAST Audit Services (FAS). Below you will find pricing information for the maintenance and support of GenTax and eBiz assuming the same terms and conditions as the current contract, and for the cost of the FAS subscription.

YEAR	MAINTENANCE	SUPPORT	TOTAL	FAS	TOTAL
2022	$444,000	$967,000	$1,411,000	$100,000	$1,511,000
2023	$457,000	$996,000	$1,453,000	$100,000	$1,553,000
2024	$470,000	$1,025,000	$1,495,000	$200,000*	$1,695,000
2025	$484,000	$1,055,000	$1,539,000	$206,000*	$1,745,000
2026	$498,000	$1,086,000	$1,584,000	$212,000*	$1,796,000
	TOTAL		$7,482,000		$8,300,000

*This amount is only an estimate. The annual cost of the FAS subscription after the initial two years will be determined by the level of effort needed to fulfill Treasury's audit needs and will require a mutual scope agreement.

Please feel free to contact me or Eric Deffenbaugh with any questions or clarifications needed.

Thank you,

Nikki Nguyen
nnguyen@gentax.com
(720) 238-2532

7229 South Alton Way
Centennial, CO 80112
(1) 303.770.3700
fastenterprises.com

STATEMENT OF WORK

This Statement of Work (SOW) describes the services Fast Enterprises, LLC ("FAST") will provide to the City and County of Denver ("Agency" or "Client") to successfully implement and deliver FAST Audit Services ("FAS").

Contents

SECTION I. INTRODUCTION

FAST Audit Services (FAS) provides fully managed cloud-based audit selection and remote tax audit support. FAS includes built-in, ready-to-go audit selection analytics that target agency-specific audit issues. The remote audit tools allow taxpayers to securely upload audit documents via the Agency's e-Services site. FAS significantly reduces an Agency's required work effort to implement and maintain an analytics-based audit selection program. The Agency has full access to and control of FAS.

The key features of FAS are built in analytics, a selection repository, rules management, reporting and analysis, document upload, questionnaires, and supporting and training from the FAS team for the agency staff.

FAS is a service-based, FAST-hosted product installed outside the Agency's GenTax environment. The Agency's local GenTax installation securely transmits data to FAS and receives results back from the service. After receiving the results, GenTax creates audit cases in GenTax to be worked via the Agency's existing audit processes. FAST grants authorized Agency personnel access to FAS controls to perform administrative tasks related to the analytics models.

7229 South Alton Way
Centennial, CO 80112
(1) 303.770.3700
fastenterprises.com

Approach

Since Agency funding will not be available until January 2022, FAST and Agency agree to prepare the Agency's GenTax system for FAS, in advance, according to the schedule below. FAST will provide access to the FAS test environments to accomplish setup activities at no cost.

FAST shall use its proprietary implementation methodology (also referred to as "FAST Implementation Methodology") to implement FAS and to conduct the project. The FAST Implementation Methodology addresses numerous aspects of project execution. For example:

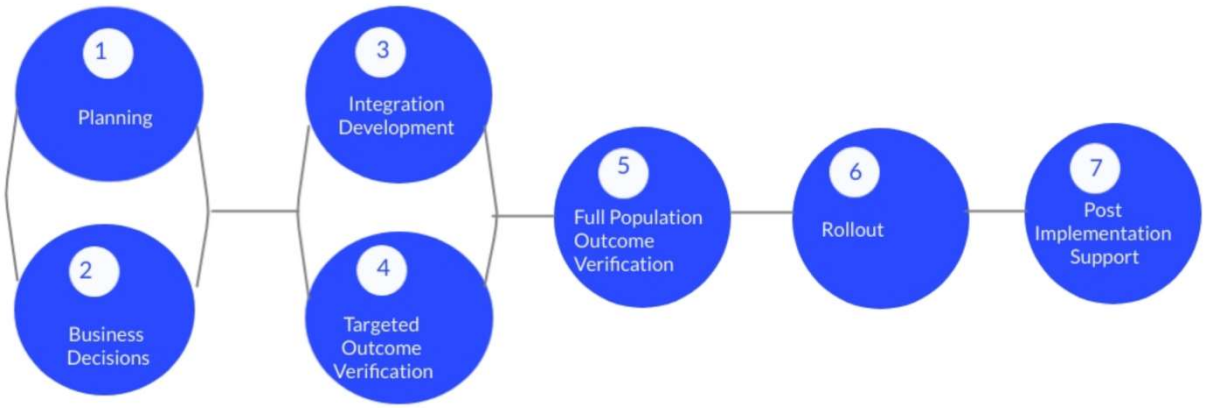
- Deliverables
- Work Products
- Project Management
- Oversight
- Status Reporting
- Risk Management
- Communication
- Organizational Change Management
- Training
- Testing
- Implementation
- Production Support
- Resource Planning
- Resource Allocation
- Work Monitoring
- Work Tracking

FAST shall use its proprietary tools to manage all aspects of project execution, including the project schedule, work tasks, project documentation, and the maintenance of the project decision and risk registers. Some of the tools the team will use include the Delivery Workbench, the FAST Central Repository (FCR), and the Solution Request System (SQR).

Where inconsistencies, contradictions, and lack of clarity exist between FAST's Implementation Methodology, such shall be resolved by mutual agreement between FAST and Agency. Where mutual agreement cannot be reached, the FAST's proprietary implementation methodology shall prevail.

In all cases, the parties may adjust the implementation methodology through mutual agreement.

FAST Methodology for FAST Data & Analytics Services Implementation is shown below:



Scope

In addition to the business requirements identified in this SOW, FAST and Agency will work together to use FAS as it was designed and intended to be used, to deliver the necessary business capabilities in GenTax. FAST and Agency will seek to improve Agency business processes and not replicate legacy processes. All services and deliverables under this SOW, including FAS rollout, are subject to Agency's acceptance.

Scope includes implementing FAS for Sales Tax. Over time, additional programs may be available within FAS, including Use Tax and OPT. Implementing additional programs into FAS can be accomplished using the mechanisms in place for GenTax changes within FAST's current support and maintenance contract(s) with Agency. FAS subscription rate charges may apply which will be agreed upon before implementation.

High-Level Schedule and System Releases

FAST and Agency will implement FAS in one rollout addressing Sales Tax audit programs. Key project dates are as shown below. The dates will be adjusted through mutual agreement of the Parties and once the start date is known.

Key Project Milestone	Start	Completion	Duration
Project Start	7/19/2021	1/26/2022	30 weeks
Project Preparation	7/19/2021	7/30/2021	2 weeks
Development for Integration with FAS	7/26/2021	9/3/2021	6 weeks
Sandbox for Integration with FAS	8/23/2021	9/17/2021	4 weeks
Targeted Outcome Verification	9/20/2021	10/29/2021	6 weeks
Full Outcome Verification & Performance Testing	11/1/2021	12/24/2021	8 weeks
Rollout to Production	12/27/2021	1/4/2022	1 week
Final Acceptance		1/11/2022	1 week
Post-Implementation Support	1/12/2022	1/26/2022	2 weeks

Milestones

The following tables identify the phases, milestones, work products, deliverables, and tasks within the FAST Implementation Methodology. The implementation phases are described in Section II.

Deliverable/Milestone*	Deliverable/Milestones Description
Sandbox for Integration with FAS Complete	The Testing Preparation Complete Milestone is achieved when the project is positioned to begin verifying the outcomes from FAS as outlined in the FAST Implementation Methodology. This includes preparing the outcome verification plan, identifying a testing approach (including facilities, if required), establishing test data, and identifying the following: testers, business test conditions, business test cycles, approach to executing business verification, full population outcome verification approach, and acceptance criteria. The FAS team will prepare the agency for the outcome verification process by ensuring they are familiar with FAS and the outcome verification process. FAST will continue to complete outstanding functionality while testing begins.
System Acceptance At Rollout	The activities completed for System Acceptance are the Implementation Rollout milestones including the tasks in the integration Development, Outcome Verification, User Familiarization, and Rollout phases and the following documents: Outcome Verification Plan, User Familiarization Plan, and Rollout Plan. The Production Rollout Milestone is achieved when the Agency makes the decision to go-live and the system is placed into production.

*Rollout deliverables are the two Deliverable/Milestones identified in this table.

Phase	Implementation Team Tasks and Activities	Example Work Products
Preparation Phase	• Establish team resources • Project planning and scheduling • Confirm infrastructure • Install FAST software and/or Technical items required for Integration • Develop Communication Plan	• Organization Chart • Implementation Plan • Communication Plan
Business Decision Phase	• Business decision meetings • Prepare and verify decision & FAS parameter meetings	• Business decision and parameter items in Delivery Workbench • Meeting Minutes
Integration Development Phase	• Perform development tasks • Develop interfaces • Begin to verify integration in Sandbox	• Development Items in Delivery Workbench
Outcome Verification Phase	• Prepare outcome verification plan • Prepare outcome verification scenarios • Set up test environment(s) • Identify and familiarize testers • Conduct targeted outcome verification • Conduct performance testing • Conduct full population outcome verification	• Outcome verification plan • Test scenarios • Outcome verification results
User Familiarization Phase	• Prepare user familiarization plan • Prepare user familiarization material • Train users	• User familiarization plan
Rollout Phase	• Prepare Cutover Checklist • Prepare post-rollout (temporary) Help Desk and Deskside Support Plan • Move configurations and software to production environment • Production cutover	• Cutover Checklist
Production Support Phase	• Perform deskside support • Support and maintain production system • Support system operations	• System Maintenance and Support Overview

Acceptance

FAST shall perform activities as described within each phase of the FAST Implementation Methodology. The Agency shall verify that activities within each phase have been completed.

Any delay in the acceptance of any work products, milestones, or deliverables shall not delay the progress of the project.

SECTION II. IMPLEMENTATION METHODOLOGY

This section describes the FAST Implementation Methodology in more detail.

Phase	Phase Name	Phase Description
1.	Preparation Phase	Develops the roadmap defining how the implementation is to be executed.
2.	Business Decisions	Defines the business decisions necessary to deliver the functionality for the line of business.
3.	Integration Development Phase	Gathered business decisions are used to produce work packages for developers specifying parameters, select options, thresholds, and other types of configurations, enhancements, or programming.
4.	Outcome Verification Phase	Ensures that the production system delivers outcomes within expected range.
5.	Training/Familiarization Phase	Ensures agency users are familiar and confident using FAST Audit Services.
6.	Rollout Phase	Delivers the lines of business to production.
7.	Production Support Phase	Provides desk-side support and solution-specific help-desk support during the initial production period. When Maintenance and Support Operations options are exercised this phase includes the operation and maintenance of the solution in production over the long term.

FAST DATA SERVICES

FAST DATA SERVICES SUBSCRIBER AGREEMENT

This Subscriber Agreement ("Agreement") is entered into as of the date indicated below, by and between THE CITY AND COUNTY OF DENVER, a government agency ("Subscriber"), and FAST Enterprises, LLC ("FAST") effective on the date of approval of Subscriber's Application for Services. Subscriber and FAST may be referred to herein as "Party" or "Parties."

The services will be provided by Fast Data Services, LLC as a subcontractor to FAST and may include, but are not limited to, identity and location services, fraud detection, public records searching, audit and collection services, data exchange services for the provision of intelligence, and additional services that FDS develops and integrates into its business from time to time. The services provided by FDS are called "FDS Services." All obligations, warranties, and representations of FDS under this subscriber agreement shall be considered the obligations, warranties, and representations of FAST for purposes of this Agreement regarding FDS Services.

In the provision of FDS Services, the parties anticipate a two-way exchange of data records between FDS and the Subscriber. These data records may contain public records, personally identifiable information, information regulated under one or more federal laws, the results of proprietary data analyses, and confidential business intelligence.

1. Subscriber Rights and Obligations.

As detailed below, the Subscriber will receive a license to use FDS services, subject to certain security and compliance conditions, if the Subscriber opts-in to Base FDS Services.

1.1 Restricted License. FDS grants to Subscriber a restricted personal, non-exclusive, non-transferable, non-sublicenseable, revocable license to obtain and use certain public record products and other products and services provided by FDS Services as permitted by this Agreement and all applicable laws, rules, regulations and regulatory directives. Subscriber may obtain and use FDS for Subscriber's own internal business purposes consistent with this Agreement and for no other purpose. Except for the limited access and use rights granted in this Agreement, FDS retains all right, title and interest in FDS Services and Subscriber is not granted any ownership rights or title thereto. FDS may immediately terminate this Agreement upon notice to Subscriber if:

Fast Data Services, LLC
7229 South Alton Way
Centennial, CO 80112
(1) 303.770.3700
fastenterprises.com

- Subscriber has breached its obligations under this Agreement, and the breach (if capable of being remedied) is not remedied to FDS satisfaction within thirty (30) calendar days, or some other mutually agreed upon time frame, of Subscriber's receipt of written notice of the breach; or
- FDS reasonably believes that Subscriber is not in compliance with, or causes FDS or any third party not to be in compliance with, applicable federal or state laws and regulations.

1.2 Audit. Upon reasonable notice and subject to Subscriber's access and security policies and procedures, FDS may audit once per calendar year (but more frequently if the annual audit reveals a compliance issue) Subscriber's use of FDS Services for the purpose of investigating and confirming that Subscriber's use of the FDS Services is in compliance with this Agreement and applicable law. Subscriber will cooperate and provide FDS all documentation reasonably requested relating to Subscriber's account. Violations discovered in any audit may be subject to immediate action including, but not limited to, suspension of the provision of FDS Services and/or termination of the license. If the FDS Services are suspended, they will be reinstated immediately upon satisfactory resolution or remediation of any violations triggering the suspension.

1.3 Security Incident Response. Subscriber will promptly (but in no event later than within twenty-four hours after becoming aware of the occurrence) notify FDS of any breach of security in which an unauthorized person has gained access to the FDS Services.

Subscriber will develop and maintain an Incident Response Plan. Subscriber will be solely responsible for responding to breaches originating from Subscriber's infrastructure, hardware, users, or user accounts or credentials, whether valid, stale, expired, spoofed or otherwise invalid. FDS has no liability for such breaches or the response to them.

2. FDS Rights and Obligations

In addition to providing the license referenced above, FDS has certain rights and obligations under this agreement, as detailed below.

2.1 Provision of Services. FDS shall maintain and use Confidential Information to provide the FDS Services in accordance with this Agreement and for no other purpose. Except for the limited access and use rights granted in this Agreement, Subscriber retains all right, title and interest in its Confidential Information and FDS is not granted any ownership rights or title thereto. Subscriber may immediately terminate this Agreement upon notice to FDS if:

- FDS has breached its obligations under this Agreement, and the breach (if capable of being remedied) is not remedied to Subscriber's satisfaction within thirty (30) days, or some other mutually agreed upon time frame, of FDS's receipt of written notice of the breach; or
- Subscriber reasonably believes that FDS is not in compliance with, or causes Subscriber or any third party not to be in compliance with, applicable federal or state laws and regulations.

2.2 Right to Use Subscriber Data. FDS Services are provided in part by applying analytic tools to the pooled data of all subscribers, associated public records, and other data. FDS may maintain data it receives from Subscriber in the FDS data warehouse, and may only use such data as described herein. Upon written request from Subscriber, FDS will return or destroy all Subscriber data in its possession.

2.2.1 Base FDS Services.

(i) Base FDS Services are services whereby subscribers' data, models derived from subscribers' data and/or other data are used to answer a question and/or return and indicator.

(ii) Base FDS Services do not involve the distribution of Subscriber's data to other subscribers.

(iii) FDS may use Subscriber data to provide FDS Services to subscriber and FDS Base Services to other subscribers.

2.2.2 Cross Subscriber Services.

(i) Some FDS Services may be provided by using Subscriber Data from multiple subscribers ("Cross Subscriber Services").

(ii) Subscriber will be given the option to opt-in to any Cross Subscriber services before Subscriber data is used to provide Cross Subscriber Services to any other subscriber.

(iii) Opting-in to receive Cross Subscriber services requires opting-in to contribute towards Cross Subscriber Services.

2.2.3 FDS Summary Information.

(i) FDS may de-identify, anonymize and aggregate data related to Subscriber's usage of FDS services, collectively referred to as "FDS Summary Information". FDS Summary Information will not contain Personally Identifiable Information ("PII").

(ii) FDS may compile, combine, or incorporate such Summary Information with or into FDS Summary Information obtained from other users of FDS services, and may generate, use, reproduce, publicize or otherwise leverage the FDS Summary Information in any manner consistent with FDS's business needs.

Without limiting the above, FDS can use the FDS Summary Information to develop and improve FDS products and services, to create and distribute reports and other materials, to provide additional services to its customers, to advertise the benefits of FDS services, and for additional services that FDS develops and integrates into its business from time to time.

(iii) FDS Summary Information that identifies the Subscriber will not be distributed, publicized or shared without the consent of the Subscriber.

(iv) FDS is the owner of all right, title and interest in and to Summary Information. The rights listed in this provision survive expiration and termination of the Subscriber Agreement, and FDS is not required to return or destroy any Summary Information. This provision should not be read to conflict with any other contract terms in this or any other contract documents; rather, this provision supplements or supersedes, as appropriate, all contract terms related to the same or similar subject matter.

2.3 Security. FDS will not breach or permit the breach of the security of Personal Information which FDS receives under this Agreement. FDS will maintain a security posture substantially compliant with the moderate baseline security controls contained in NIST 800-53, Rev.4. FDS agrees to subject its systems to annual third-party assessments, including penetration testing and vulnerability assessments. FDS also agrees to leverage industry leading security software to protect and assess the security of FDS systems, and to leverage native tools to track security and compliance tasks and evidence. FDS is not an owner or licensee of Subscriber's Confidential Information. FDS will notify Subscriber of any security incident involving Personal Information contained in Subscriber's Confidential Information immediately after the discovery of a security incident where misuse of the Personal Information occurred or is likely to occur. FDS will cooperate with Subscriber by sharing information relevant to the incident, and in any other way required by law. These security measures are FDS's only responsibility with respect to the security of Subscriber's Confidential Information.

2.4 Disclaimer of Warranties. FDS Services are provided "as-is", with no warranties of any kind, whether express, implied in fact or by operation of law or statute, including without limitation, those as to quality, non-infringement, accuracy, completeness, timeliness, response times, uptimes, application availability or currentness, and those warranties that might be implied from a course of performance or dealing or trade usage and warranties of merchantability and fitness for a particular purpose. FDS and its representatives, including parents, subsidiaries, and affiliates, shall not be liable to Subscriber or other third parties for any claim relating to FDS's procuring, compiling, collecting, interpreting, reporting, communicating, or delivering FDS Services.

2.5 Insurance. FDS will always carry at least as much insurance as it had in place on the Effective Date of the Agreement, as evidenced by the certificate of insurance attached as Exhibit A.

3. Mutual Clauses

3.1 Confidentiality

3.1.1 Services Information. Subscriber shall hold in confidence and shall not disclose, in whole or in part, information relating to FDS's business, including, without limitation, products, services, systems, processes, data sources, test results, and other FDS technical and financial information, as well as FDS Services and information derived from the FDS Services ("Services Information"), and any analyses, compilations and reports derived from any of the foregoing. Subscriber may not disassemble, decompile, or in any way reverse engineer any information derived from FDS Services.

3.1.2 Confidential Information. The Parties acknowledge that they and their employees or agents may, in the course of performing the Services under this Agreement, be exposed to or acquire information that is confidential to the other Party or the other Party's clients or vendors. Any and all information of any form obtained by a Party or its employees or agents in the performance of this Agreement shall be deemed to be confidential information of the disclosing Party, including Subscriber Data and Personally Identifiable Information (PII), collectively called "Confidential Information". Any reports or other documents or items (including software) that result from the use of the Confidential Information by the receiving Party shall be treated in the same manner as Confidential Information. Confidential Information shall be deemed not to include information that (a) is or becomes (other than by disclosure by the receiving Party) publicly known; (b) is furnished by the disclosing Party to others without restrictions similar to those imposed by this Agreement; (c) is rightfully in the receiving Party's possession without the obligation of nondisclosure prior to the time of its disclosure under this

Agreement; (d) is obtained from a source other than the disclosing Party without the obligation of confidentiality, (e) is disclosed with the written consent of the disclosing Party, or; (f) is independently developed by employees, agents, or subcontractors of the receiving Party who can be shown to have had no access to the Confidential Information.

3.1.3 Non-Disclosure. The Parties agree to hold Confidential Information in confidence, using at least the same degree of care that the receiving Party uses in maintaining the confidentiality of its own confidential information, and not to copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties (other than its subcontractors), or use Confidential Information for any purposes whatsoever other than the provision of Services to Subscriber hereunder, and to advise each of its employees and agents of their obligations to keep Confidential Information confidential. The Parties will each use commercially reasonable efforts to assist the other Party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, the receiving Party will advise the disclosing Party immediately in the event that it learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Agreement, and the receiving Party will, at its expense, cooperate with the disclosing Party in seeking injunctive relief or other equitable relief in the name of the disclosing Party or the receiving Party against any such person. The receiving Party agrees that, except as directed by the disclosing Party, it will not at any time during or after the term of this Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Agreement, and that upon termination of this Agreement or at Subscriber's request, the receiving Party will turn over to the disclosing Party all documents, papers, and other matter in its possession that embody Confidential Information. Notwithstanding the foregoing, the receiving Party may keep one copy of such Confidential Information necessary for quality assurance, audits, and evidence of performance or receipt of the Services.

3.1.4 Security and Access Policies and Procedures. The Parties each agree to comply with all reasonable requests by the other Party to ensure the confidentiality and non-disclosure of a disclosing Party's Confidential Information, including without limitation (i) obtaining non-disclosure agreements from the receiving Party's employees and agents who are performing or accessing Services and providing copies of such agreements to the disclosing Party; (ii) performing criminal background checks on each of its employees and agents who are performing or accessing Services, and maintaining records of those background checks in the Party's files for a period of six years past the contract expiration or termination; (iii) at Subscriber's sole discretion and expense, requiring FDS employees who are

physically present in Subscriber's state to submit to a criminal background check through the state's chief law enforcement agency; and (iv) complying with the security and access policies and procedures related to Federal Tax Information pursuant to IRS Publication 1075.

3.1.5 Access Restrictions. The Parties may only use FDS Services, Services Information, and Confidential Information as permitted under this Agreement. FDS Services may only be accessed from within the United States. Subscriber must not access and/or use the FDS Services via mechanical, programmatic, robotic, scripted or other automated search means, other than through batch or machine-to-machine applications approved by FDS.

Each Party will:

- limit access to FDS Services, Services Information, and Confidential Information to only those employees who have a need to access in connection with the duties and obligations of their employment;
- advise its employees having access to FDS Services, Services Information, or Confidential Information of the proprietary and confidential nature thereof and of the obligations set forth in this Agreement;
- safeguard the Services Information and Confidential Information using reasonable and appropriate administrative, technical, and physical security safeguards at least as strong as those used to protect the Party's own data;
- employ appropriate policies and procedures to control access and security of usernames, passwords, and terminal access for FDS Services and Confidential Information;
- track and monitor its access to FDS Services, Services Information, and Confidential Information and maintain logs evidencing such tracking and monitoring for at least 2 years;
- prevent any use not in conformance with this Agreement; and
- maintain records sufficient to demonstrate compliance with its obligations under this Agreement.

3.1.6 Injunctive Relief. The breach of this Section 3.1, including disclosure of any Confidential Information, will cause irreparable injury to the disclosing Party that is inadequately compensable with monetary damages. Accordingly, a Party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Each Party acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of the other Party and are reasonable in scope and content.

3.2 Compliance with Law. The Parties understand and agree that FDS Services may contain sensitive information that is governed by various state and federal laws. The Parties each certify that each will comply with all applicable federal, state, and local laws. Regulations, policies, and ordinances may be adopted or amended from time to time, including, but not limited to:

3.2.1 Gramm-Leach-Bliley Act Data. The Gramm-Leach-Bliley Act (15 U.S.C. §6801-6809) and its implementing regulations (collectively, "GLBA") is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals. Data provided by FDS Services may include private financial information from Financial Institutions, subject to the GLBA. Subscriber hereby certifies that the specific purpose(s) for which such FDS Services will be requested, obtained and used by Subscriber is one or more of the following permitted uses under the GLBA:

- To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;
- To comply with federal, state, or local laws, rules, and other applicable legal requirements.

3.2.2 Drivers Privacy Protection Act Data. The Driver's Privacy Protection Act (18 U.S.C. §2721, *et seq.*) and related laws (collectivley, "DPPA") is a federal law that governs the privacy and disclosure of personal information gathered by State Departments of Motor Vehicles. Data provided by FDS Services may include data subject to DPPA. Subscriber hereby certifies that it will request, obtain, and use such FDS Services only for one of the following permissible uses under the DPPA:

- Use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a federal, state, or local agency in carrying out that agency's functions.
- Use in connection with any civil, criminal, administrative, or arbitral proceeding, in any federal, state, or local court or agency, or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a federal, state, or local court.

3.2.3 Death Master File ("DMF") Data. Certain data provided by FDS as part of FDS Services may include information obtained from the Limited Access Death Master File (LADMF) made available by the US Department of Commerce National Technical Information Service (NTIS) and subject to regulations found at 15 CFR Part 1110. All FDS subscribers

are required to comply with all applicable laws and, if Subscriber is granted access to LADMF data, Subscriber will be certified compliant with 15 CFR 1110 prior to receiving LADMF data.

3.2.4 Fair Credit Reporting Act. FDS is not a "consumer reporting agency," as defined by the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.) ("FCRA") and FDS Services do not constitute a "consumer report," as defined by FCRA and shall not be subject to the FCRA requirements relating to disputes, access, accuracy or otherwise. FDS Services may not be used in whole or in part as a factor in determining eligibility for credit, insurance, or employment or for any other purpose contemplated by the FCRA.

3.2.5 Federal Tax Information. Federal Tax Information (FTI) is a term of art defined in IRS Publication 1075, and consists of federal tax returns and return information (and information derived from it) that is in Subscriber's possession or control. Subscriber retains liability for FTI, and should make every effort to not transmit it for storage by FDS. FDS does not intend to store FTI.

3.3 N/A

3.4 Right to Suspend or Terminate Services.

3.4.1 In addition to the termination rights set forth in this Agreement, upon notice to Subscriber (which notice shall be delivered to Subscriber as soon as practicable under the circumstances), FDS may suspend delivery of the FDS Services, in whole or in part: (i) if Subscriber has breached its material obligations, or failed to satisfy the material requirements of, this Agreement, (ii) the requirements of applicable law, rule or regulation have not or will not be met, or (iii) to investigate, respond to and/or remedy a suspected or actual concern on information security, privacy, defamation, criminal activity or legal compliance, until such breach, non-compliance or investigation is remedied to FDS' reasonable satisfaction.

3.4.2 Either Party may terminate this Agreement upon thirty (30) days prior written notice in the event of either Party's failure to perform.

3.4.3 Subscriber may terminate this Agreement upon written notice in the event Subscriber fails to receive funding, appropriations, limitations, allotments, or other expenditure authority sufficient to allow Subscriber, in the exercise of its reasonable administrative discretion, to meet its payment obligations under this Agreement.

Appendix 1
Opt-Ins

Base FDS Services

☐ Subscriber wishes to participate in Base FDS Services – annual fee applies

Cross Subscriber Services

DEX

DEX is a data exchange service which Subscribers can use to submit data for cross-referencing by other Subscribers. Such information often includes information such as names, SSNs, IP addresses, and bank accounts connected with fraudulent activity. FDS interacts with DEX only as necessary to facilitate its security, storage, and transfer. Each Subscriber owns the data it contributes to DEX, and FDS claims no rights, title or interest in it. A Subscriber's data can be deleted from the data exchange if the Subscriber opts out of DEX at any time.

☐ Subscriber wishes to participate in DEX

ATTACHMENT 1

1. **DEFINITIONS**. Whenever used herein, any schedules, exhibits, order forms, or addenda to this Agreement, the following terms shall have the meanings assigned below unless otherwise defined therein. Other capitalized terms used in this Agreement are defined in the context in which they are used.

1.1. **"City Data"** means all information, whether in oral or written (including electronic) form, created by or in any way originating with the City . City Data also includes Confidential Information disclosed to Contractor. City Data does not include Summary Information.

1.2. "**Confidential Information**" means all records or data that is disclosed in written, graphic or machine recognizable form and is marked, designated, labeled or identified at the time of disclosure as being confidential or its equivalent, or, if the information is in verbal form, it is identified as confidential or proprietary at the time of disclosure and is confirmed in writing within thirty (30) Calendar Days of the disclosure and is not subject to disclosure under CORA. Confidential Information shall include, but is not limited to, PII, financial, or Personally Identifiable Information and/or Personal Information as described in the C.R.S 24-73-101, *et seq*; . Confidential Information does not include information which: (a) is public or becomes public through no breach of the confidentiality obligations herein; (b) is disclosed by the party that has received Confidential Information (the "Receiving Party") with the prior written approval of the other party; (c) was known by the Receiving Party at the time of disclosure; (d) was developed independently by the Receiving Party without use of the Confidential Information; (e) becomes known to the Receiving Party from a source other than the disclosing party through lawful means; (f) is disclosed by the disclosing party to others without confidentiality obligations; or (g) is required by law to be disclosed.

1.3. **"CORA"** means the Colorado Open Records Act, §§ 24-72-200.1, *et seq*., C.R.S.

1.4. **"Data Incident"** means any accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of any information resources of the City. Data Incidents include, without limitation (i) successful attempts to gain unauthorized access to City information regardless of where such information is located; (ii) unwanted disruption or denial of service; It shall also include any actual or reasonably suspected unauthorized access to or acquisition of

computerized City Data that compromises the security, confidentiality, or integrity of City Data, or the ability of the City to access City Data.

1.5. **"Deliverable"** means the Products or Services or documents or tangible work products described in an Order Form to be provided to the City by Contractor or the outcome to be achieved or output to be provided, in the form of a tangible object or software that is produced as a result of Contractor's work that is intended to be delivered to the City by Contractor under this Agreement.

1.6. Deleted.

1.7. **"Downtime"** means any period of time of any duration that the Services are not made available by Contractor to the City for any reason, including scheduled maintenance or Enhancements.

1.8. **"Enhancements"** means any improvements, modifications, upgrades, updates, fixes, revisions and/or expansions to the Services that Contractor may develop or acquire and incorporate into its standard version of the Services or which Contractor has elected to make generally available to its customers.

1.9. "**Equipmen**t" means any hardware, machinery, device, tool, computer, computer component, computer system, including add-ons, or peripherals of tangible form together with the necessary supplies for upkeep and maintenance, and other apparatus, owned by Contractor under this Agreement.

1.10. "**Erro**r" means any defect, problem, condition, bug, or other partial or complete inability of a Product to operate in accordance with the applicable Specifications.

1.11. **"Intellectual Property Rights"** includes without limitation all right, title, and interest in and to all (a) Patent and all filed, pending, or potential applications for Patent, including any reissue, reexamination, division, continuation, or continuation in part applications throughout the world now or hereafter filed; (b) trade secret rights and equivalent rights arising under the common law, state law, and federal law; (c) copyrights, other literary property or authors rights, whether or not protected by copyright or as a mask work, under common law, state law, and federal law; and (d) proprietary indicia, trademarks, trade names, symbols, logos, and/or brand names under common law, state law, and federal law.

1.12. Deleted.

1.13. Deleted.

1.14. **"PII"** means personally identifiable information including, without limitation, any information maintained by the City about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. PII includes, but is not limited to, all information defined as personally identifiable information in §§ 24-72-501 and 24-73-101, C.R.S.

1.15. Deleted.

1.16. **"Protected Information"** includes, but is not limited to, personally-identifiable information, defined under § 24-72-101 *et seq*., and personal information that is subject to local, state or federal statute, regulatory oversight or industry standard restricting the use and disclosure of such information. The loss of such Protected Information would constitute a direct damage to the City.

1.17. **"Services"** means Contractor's computing and software solutions, accessed by the City pursuant to this Agreement, that provide the functionality and/or produce the results described in the Documentation, including without limitation all Enhancements thereto and all interfaces.

1.18. Deleted.

1.19. "**Specifications**" means the Contractor's most current cumulative statement of capabilities and functionality.

1.20. **"Subcontractor"** means any third party engaged by Contractor to aid in performance of the work or the Service. Contractor shall provide to the City upon request a list of Subcontractors providing material services to the Service.

1.21. "Summary Information" means the de-identified City Data that FDS shall use as an input to further analytics models and summary reporting.

1.22. "**System**" means the operational combination of all Products and Services to be provided by Contractor to the City under this Agreement.

1.23. **"Third Party"** means persons, corporations and entities other than Contractor, the City or any of their employees, contractors or agents.

1.24. **"Third-Party Host"** means the entity where the physical location of the server(s) of the Contractor's software resides.

2. RIGHTS AND LICENSE IN AND TO DATA

2.1. The Parties agree that as between them, all rights in and to City Data shall remain the exclusive property of the City, and Contractor has a limited, nonexclusive license to access and use City Data as provided in this Agreement solely for the purpose of performing its obligations hereunder.

2.2. All City Data created and/or processed by the Service is and shall remain the property of the City and shall in no way become attached to the Service, nor shall Contractor have any rights in or to the City Data without the express written permission of the City and may not include Protected Information.

2.3. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

2.4. The City retains the right to use the Service to access and retrieve data stored on Contractor's Service infrastructure at any time during the term of this Agreement at its sole discretion.

2.5. FAST is the owner of all right, title and interest in and to Summary Information. The rights listed in this provision survive expiration and termination of the Agreement, and FAST is not required to return or destroy any Summary Information. This provision should not be read to conflict with any other contract terms in this or any other contract documents; rather, this provision supplements or supersedes, as appropriate, all contract terms related to the same or similar subject matter.

3. <u>DATA PRIVACY</u>

3.1. Contractor will use City Data only for the purpose of fulfilling its duties under this Agreement and for the City's sole benefit and will not share City Data with or disclose it to any Third Party without the prior written consent of the City or as otherwise required by law. By way of illustration and not of limitation, Contractor will not use City Data for Contractor's own benefit and, in particular, will not engage in "data mining" of City Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the City.

3.2. Contractor will provide access to City Data only to those Contractor employees, contractors and Subcontractors ("Contractor Staff") who need to access City Data to fulfill Contractor's obligations under this Agreement. Contractor will ensure that, prior to being granted access to City Data, Contractor Staff who perform work under this Agreement have all undergone

and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of City Data they will be handling.

3.3. If Contractor receives Protected Information of a Colorado resident under this Agreement, Contractor shall implement and maintain reasonable written security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of Contractor's business and its operations. Unless Contractor agrees to provide its own security protections for the information it discloses to a third-party service provider, Contractor shall require all its third-party service providers to implement and maintain reasonable written security procedures and practices that are appropriate to the nature of the personal identifying information disclosed and reasonably designed to help protect the personal identifying information subject to this Agreement from unauthorized access, use, modification, disclosure, or destruction. Contractor and its third-party service providers that maintain electronic or paper documents that contain Protected Information under this Agreement shall develop a written policy for the destruction of such records by shredding, erasing, or otherwise modifying the Protected Information to make it unreadable or indecipherable when the records are no longer needed.

3.4. Contractor may provide City Data to its agents, employees, assigns, and Subcontractors as necessary to perform the work under this Agreement, but shall restrict access to Confidential Information to those agents, employees, assigns, and Subcontractors who require access to perform their obligations under this Agreement. Contractor shall ensure all such agents, employees, assigns, and 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 at all times the agent, employee, assign, or Subcontractor has access to any Confidential Information. Contractor shall provide copies of those signed nondisclosure provisions to the City upon execution of the nondisclosure provisions if requested by the City.

4. DATA SECURITY AND INTEGRITY

4.1. All facilities, whether Contractor hosted or Third-Party Hosted, used to store and process City Data will implement and maintain administrative, physical, technical, and procedural

safeguards and best practices at a level sufficient to provide and secure City Data from unauthorized access, destruction, use, modification, or disclosure appropriate for City Data. FAST bases its security program on IRS Publication 1075 and NIST 800.53 R4.

4.2. Contractor warrants that all City Data will be encrypted in transmission (including via web interface) and in storage by a mutually agreed upon National Institute of Standards and Technology (NIST) approved strong encryption method and standard.

4.3. 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 and intrusion detection and reporting in providing Services under this Agreement. Contractor shall ensure that any underlying or integrated software employed by the Service is updated on a regular basis and does not pose a threat to the security of the Service.

4.4. Contractor shall, and shall cause its Subcontractors, to do all of the following:

4.4.1. Provide physical and logical protection for all hardware, software, applications, and data that meets or exceeds industry standards and the requirements of this Agreement.

4.4.2. Maintain network, system, and application security, which includes, but is not limited to, network firewalls, intrusion detection (host and network), annual security testing, and improvements or enhancements consistent with evolving industry standards.

4.4.3. Comply with State and federal rules and regulations related to overall security, privacy, confidentiality, integrity, availability, and auditing.

4.4.4. Provide that security is not compromised by unauthorized access to workspaces, computers, networks, software, databases, or other physical or electronic environments.

4.4.5. Promptly report all Data Incidents, including Data Incidents that do not result in unauthorized disclosure or loss of data integrity.

4.4.6. Delete.

4.4.7. Subject to Contractor's reasonable access security requirements and upon reasonable prior notice, Contractor shall provide the City with scheduled access for the purpose of inspecting and monitoring access and use of City Data, maintaining City systems, and evaluating physical and logical security control effectiveness.

4.4.8. Contractor shall perform current background checks on all of its respective employees and agents performing services or having access to City Data provided under this Agreement, including any Subcontractors or the employees of Subcontractors. A

background check performed within 30 days prior to the date such employee or agent begins performance or obtains access to City Data shall be deemed to be current.

4.4.9. Upon request by the City, Contractor will provide notice to the security and compliance representative for the City indicating that background checks have been performed. Such notice will inform the City of any action taken in response to such background checks, including any decisions not to take action in response to negative information revealed by a background check.

4.4.10. Contractor will not have access to Federal Tax Information under the Agreement.

4.5. If applicable, Contractor shall use, hold, and maintain Confidential and Protected Information in compliance with all applicable laws and regulations only in facilities located within the United States, and shall maintain a secure environment that ensures confidentiality of all Confidential and Protected Information.

4.6. Prior to the Effective Date of this Agreement, Contractor, will at its expense conduct or have conducted the following, and thereafter, Contractor will at its expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Data Incident:

4.6.1. A SSAE 16/SOC 2 or other mutually agreed upon audit of Contractor's security policies, procedures and controls;

4.6.2. Deleted;

4.6.3. A formal penetration test, performed by a process and qualified personnel of Contractor's systems and facilities that are used in any way to deliver Services under this Agreement.

4.7. Contractor will provide the City the reports or other documentation resulting from the above audits, certifications, scans and tests upon request.

4.8. Based on the results and recommendations of the above audits, certifications, scans and tests, Contractor will, within thirty (30) calendar days of receipt of such results, promptly modify its security measures to meet its obligations under this Agreement and provide the City with written evidence of remediation.

4.9. The City may require, at its expense, that Contractor perform additional audits and tests, the results of which will be provided to the City within seven (7) business days of Contractor's receipt of such results.

4.10. Deleted.

5. RESPONSE TO LEGAL ORDERS, DEMANDS OR REQUESTS FOR DATA

5.1. Except as otherwise expressly prohibited by law, Contractor will:

5.1.1. If required by a court of competent jurisdiction or an administrative body to disclose City Data, Contractor will notify the City in writing immediately upon receiving notice of such requirement and prior to any such disclosure;

5.1.2. Consult with the City regarding its response;

5.1.3. Cooperate with the City's reasonable requests in connection with efforts by City to intervene and quash or modify the legal order, demand or request; and

5.1.4. Upon request, provide the City with a copy of its response.

5.2. If the City receives a subpoena, warrant, or other legal order, demand or request seeking data maintained by Contractor, the City will promptly provide a copy to Contractor. Contractor will supply the City with copies of data required for the City to respond within forty-eight (48) hours after receipt of copy from the City and will cooperate with the City's reasonable requests in connection with its response.

6. DATA INCIDENT RESPONSE

6.1. Contractor shall maintain documented policies and procedures for Data Incident and breach reporting, notification, and mitigation. If Contractor becomes aware of any Data Incident, it shall notify the City immediately and cooperate with the City regarding recovery, remediation, and the necessity to involve law enforcement, as determined by the City. If there is a Data Incident impacting residents of Colorado or any other jurisdiction, Contractor shall cooperate with the City to satisfy notification requirements as currently defined in either federal, state, or local law. Unless Contractor can establish that neither Contractor nor any of its agents, employees, assigns or Subcontractors are the sole cause or source of the Data Incident, Contractor shall be responsible for the cost of notifying each person who may have been impacted by the Data Incident as required by law.

6.2. Contractor shall report, either orally or in writing, to the City any Data Incident involving City Data, or circumstances that could have resulted in unauthorized access to or disclosure or use of City Data, not authorized by this Agreement or in writing by the City, including any reasonable belief that an unauthorized individual has accessed City Data. Contractor shall make the report to the City immediately upon discovery of the unauthorized disclosure, but in

no event more than forty-eight (48) hours after Contractor reasonably believes there has been such unauthorized use or disclosure. Oral reports by Contractor regarding Data Incidents will be reduced to writing and supplied to the City as soon as reasonably practicable, but in no event more than forty-eight (48) hours after oral report.

6.3. Immediately upon becoming aware of any such Data Incident, Contractor shall fully investigate the circumstances, extent and causes of the Data Incident, and report the results to the City and continue to keep the City informed daily of the progress of its investigation until the issue has been effectively resolved.

6.4. Contractor's report discussed herein shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the data used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure (if known), (iv) what Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.

6.5. Within five (5) calendar days of the date Contractor becomes aware of any such Data Incident, Contractor shall have completed implementation of corrective actions to remedy the Data Incident, restore the City's access to the Services as directed by the City, and prevent further similar unauthorized use or disclosure.

6.6. Contractor, at its expense, shall cooperate fully with the City's investigation of and response to any such Data Incident.

6.7. Except as otherwise required by law or as necessary to keep other Contractor clients utilizing the system informed, 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.

6.8. Deleted.

7. DATA RETENTION AND DISPOSAL

7.1. Using appropriate and reliable storage media, Contractor will regularly backup data and retain such backup copies consistent with the Contractor's data retention policies.

7.2. Contractor will securely destroy any City Data in active Contractor databases. Contractor will supply the City a certificate indicating the records disposed of, the date disposed of, and the method of disposition used.

7.3. Contractor will immediately preserve the state of the data at the time of the request and place a "hold" on data destruction or disposal under its usual records retention policies of records that include data, in response to an oral or written request from the City indicating that those records may be relevant to litigation that the City reasonably anticipates. Oral requests by the City for a hold on record destruction will be reduced to writing and supplied to Contractor for its records as soon as reasonably practicable under the circumstances. The City will promptly coordinate with Contractor regarding the preservation and disposition of these records. Contractor shall continue to preserve the records until further notice by the City.

8. DATA TRANSFER UPON TERMINATION OR EXPIRATION

8.1. Upon expiration or earlier termination of this Agreement or any Services provided in this Agreement, City shall cease to use Contractor's system, and Contractor shall return or destroy City data present in the system subject to the process described in Section 7.2.

8.2. Except for Summary Data, upon the expiration or termination of this Agreement, Contractor shall return City Data provided to Contractor in a common and readily usable format if requested by the City or destroy City Data and certify to the City that it has done so, as directed by the City, subject to the process described in Section 7.2. If Contractor is prevented by law or regulation from returning or destroying Confidential Information, Contractor warrants it will guarantee the confidentiality of, and cease to use, such Confidential Information. To the extent that Contractor is requested to perform any services beyond the return of the City's Data in connection with termination assistance, the same shall be performed pursuant to a written statement of work under this Agreement and paid for by the City, applying Contractor's then-current rates for daily/hourly work, as the case may be.

9. COMPLIANCE WITH APPLICABLE LAWS AND CITY POLICIES.

10.1 Contractor will comply with all applicable laws in performing the Services under this Agreement. Any Contractor personnel visiting the City's facilities will comply with all applicable City policies regarding access to, use of, and conduct within such facilities. The City will provide copies of such policies to Contractor upon request. Any City personnel visiting Contractor's facilities will comply with all applicable Contractor policies regarding access to, use of, and conduct within such facilities. Contractor will provide copies of such policies to Contractor upon request.

10. SOFTWARE AS A SERVICE, SUPPORT AND SERVICES TO BE PERFORMED

10.1. Contractor, under the general direction of, and in coordination with, the City's Chief Information Officer or other designated supervisory personnel (the "Manager") agrees to provide the Services listed on Exhibit B-1 and perform the technology related services described on attached Exhibit B-1 (the "Statement of Work" or "SOW").

10.2. As the Manager directs, Contractor shall diligently undertake, perform, and complete all of the technology related services and produce all the deliverables set forth on Exhibit B-1 to the City's satisfaction.

10.3. Contractor is ready, willing, and able to provide the technology related services and the Services required by this Agreement.

10.4. Contractor shall faithfully perform the technology related services in accordance with the standards of care, skill, training, diligence, and judgment provided by highly competent individuals performing services of a similar nature to those described in the Agreement and in accordance with the terms of the Agreement.

10.5. User ID Credentials. Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:

10.5.1. Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation);

10.5.2. Account credential lifecycle management from instantiation through revocation;

10.5.3. Account credential and/or identity store minimization or re-use when feasible; and

10.5.4. Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expire able, non-shared authentication secrets).

10.6. Vendor Supported Releases. Contractor shall maintain the currency all third-party software used in the development and execution or use of the Service including, but not limited to: all code libraries, frameworks, components, and other products (e.g., Java JRE, code signing certificates, .NET, jQuery plugins, etc.), whether commercial, free, open-source, or closed-source; with third-party vendor approved and supported releases.

10.7. Deleted.

11. DELIVERY AND ACCEPTANCE

11.1. Right to Perform Acceptance Testing. Prior to accepting Deliverables, the City shall have the right to perform Acceptance Testing to evaluate the Deliverable(s) to ensure they meet Acceptance Criteria, if any, set forth on the applicable Order Form or Statement of Work. Contractor shall cooperate with the City in the development of Acceptance Criteria that shall be codified in the applicable Order Form or Statement of Work that will set forth the location, date, and other specifications of the Acceptance Testing, if any. Acceptance Testing may occur in one or more phases, depending on the integration of contingent products, scalability, performance tuning or other measurable features or milestones.

11.2. After an Acceptance Test and if at any time the Service does not conform, the City will notify Contractor in writing within sixty (60) days and will specify in reasonable detail the identified failures and possible reasons for failure. Contractor will, at its expense, repair or replace the nonconforming product within fifteen (15) days after receipt of the City's notice of deficiency.

11.3. If the City issues an Acceptance Certificate for an "Acceptance with Exception(s)" the City will list the exception(s) and the date for Contractor's correction of the Error(s). If Error(s) are corrected by the listed date(s) the City agrees to commence further Acceptance Testing of the Deliverable or affected portion(s). If the Deliverable passes the Acceptance Tests, the City will issue an Acceptance Certificate.

11.4. If a Deliverable fails a second or subsequent Acceptance Test (or in the event of a single Acceptance Test, the Acceptance Test) in no event shall there be an increase to the original price agreed to by the Parties for the Deliverable.

11.5. The foregoing procedure will be repeated until the City accepts or finally rejects the Deliverable, in whole or part, in its sole discretion. In the event that the Service does not perform to the City's satisfaction, the City reserves the right to repudiate acceptance. If the City finally rejects the Service, or repudiates acceptance of it, Contractor will refund to the City all fees paid, if any, by the City with respect to the Service.

11.6. If the City is not satisfied with Contractor's performance of the technology related services described in the Statement of Work, the City will so notify Contractor within thirty (30) days after Contractor's performance thereof. Contractor will, at its own expense, re-perform the service within fifteen (15) days after receipt of City's notice of deficiency. The foregoing procedure will be repeated until City accepts or finally rejects the technology related service

in its sole discretion. If City finally rejects any technology related service, Contractor will refund to City all fees paid by City with respect to such technology related service.

11.7. Contractor warrants that during the term of this Agreement that the Service and any associated components will not materially diminish during the subscription Term.

12. <u>COMPLIANCE FOR IN-SCOPE SERVICES</u>. Contractor covenants and agrees to comply with all applicable information security and privacy obligations imposed by any federal, state, or local statute or regulation. Such obligations may arise from:

IRS Publication 1075

Contractor further agrees to exercise reasonable due diligence to ensure that all of its service providers, agents, business partners, contractors, Subcontractors and any person or entity that may have access to City Data under this Agreement maintain compliance with and comply in full with the terms and conditions set out in this Section. Notwithstanding Force Majeure, the respective processing, handling, and security standards and guidelines referenced by this section may be revised or changed from time to time or City Data may be utilized within the Services that change the compliance requirements. If compliance requirements change, Contractor and the City shall collaborate in good faith and use all reasonable efforts to become or remain compliant as necessary under this section. If compliance is required or statutory and no reasonable efforts are available, the City at its discretion may terminate the agreement.

13. <u>ON-LINE AGREEMENT DISCLAIMER</u>. Notwithstanding anything to the contrary herein, the City shall not be subject to any provision included in any terms, conditions, or agreements appearing on Contractor's or a Subcontractor's website or any provision incorporated into any click-through or online agreements related to the work unless that provision is specifically referenced in this Agreement.

14. <u>PROHIBITED TERMS</u>. Any term included in this Agreement that requires the City to indemnify or hold Contractor harmless; requires the City to agree to binding arbitration; limits Contractor's liability for damages resulting from death, bodily injury, or damage to tangible property; or that conflicts with this provision in any way shall be void ab initio. Nothing in this Agreement shall be construed as a waiver of any provision of § 24-106-109 C.R.S.