FAST HOSTING SERVICES

FAST HOSTING SERVICES, LLC AGREEMENT

This Agreement is made this 3rd day of June, 2021 by and between Fast Hosting Services, LLC ("FHS") and Louisville Metro Revenue Commission (the "Client"), for the provision of hosting services by FHS to the Client. FHS has its principal office at 7229 S. Alton Way, Centennial, CO 80112. The Client has its principal office at 617 W. Jefferson Street, Louisville, KY 40202.

The parties agree as follows:

1. SERVICES. FHS agrees to provide Hosting and other Services under this Agreement as detailed in Attachment A (FHS Services) and Attachment C (FAST Monitoring Services Statement of Work).

2. AGREEMENT TERM AND RENEWAL OPTIONS. The initial term of this Agreement will begin on February 1, 2022 and extend through June 30, 2022. This Agreement may be renewed for the next fiscal year – July 1, 2022 through June 30, 2023 and on each subsequent anniversary thereafter. In the event that, during the term of this Agreement, the Agency's Louisville Metro Council fails to appropriate funds for the payment of the Agency's obligations under this Agreement, the Agency's rights and obligations herein shall terminate on the last day for which an appropriation has been made. The Agency shall deliver written notice to FAST of any such non-appropriation.

3. COSTS INCLUDED IN THIS AGREEMENT. Costs for FHS Services are detailed in Attachment B to this Agreement.

4. FAST SOFTWARE. "FAST Software" is software owned and licensed by Fast Enterprises, LLC and may be provided by FHS to Client.

5. CLIENT DATA
   - 5.1. "Client data" means all data, including Personally Identifiable Information, Federal Tax Information, and other legally defined and regulated types of data, that is provided to FHS by, or on behalf of, Client through the use of FHS Services.
   - 5.2. Client agrees to allow FHS, for the sole purpose of its performance hereunder, to receive, store, transmit and process Client's Data.
   - 5.3. Client retains all right, title and interest in Client data, and FHS is not granted any ownership rights, title, or license thereto. Client will secure and maintain all rights in Client data necessary for FHS to provide FHS Services without violating the rights of any third party or otherwise obligating FHS to Client or to any third party. FHS exercises only as much control

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

over Client data as is necessary for the provision of FHS Services and will not assume any obligations with respect to Client data other than as expressly set forth in this Agreement or as required by law.

6. SECURITY. FHS's sole obligations with respect to security of a hosted system are identified in Attachment A. Further, Client agrees to comply with all security procedures in place at any data center and shall be liable for any loss or damage caused by the Client not following such procedures. FHS will also comply with IRS Publication 1075 requirements included as Attachment E.
7. WARRANTY EXCLUSIONS. FHS Services are provided "as-is", with no warranties, express or implied, other than those specifically listed in this Agreement. FHS specifically disclaims any warranties related to quality, non-infringement, accuracy, completeness, and any warranties that might be implied from a course of performance, dealing, or trade usage, and warranties of merchantability and fitness for a particular purpose. Warranties related to timeliness, response times, uptimes, and application availability are listed in Attachment A, and those warranties are the extent of FHS's obligation related to those subjects.

8. LIMITATION OF LIABILITY.
   8.1. FHS's entire aggregate liability to Client under this Agreement shall not exceed the annual value of the Contract during the contract year the cause of action arose. In no event will FHS be liable for any consequential, incidental, indirect, special, or punitive damages incurred by Client and arising out of FHS's performance of this Agreement, including, but not limited to, loss of good will and lost profits or revenue, whether or not such loss or damage is based in contract, warranty, tort, negligence, strict liability, indemnity, or otherwise, even if FHS has been advised of the possibility of such damages.
   8.2. Data/Confidentiality Breach. FHS maximum liability for any data/confidentiality breach will be the amount actually reimbursed by the insurance carrier under FHS's applicable insurance policy up to $5,000,000.
   8.3. This Agreement does not transfer from Client to FHS any liability Client has or would have under applicable State or Federal laws. The liability cap established above does not apply to direct damages caused by the willful misconduct or gross negligence of FHS, as defined by Black's Law Dictionary. Direct damages related to willful misconduct or gross negligence shall not exceed $5,000,000.

9. TERMINATION
   9.1. TERMINATION FOR CONVENIENCE. Either party may terminate the Agreement upon sixty (60) days written notice to the other party.

9.2. TERMINATION FOR CAUSE. Either party may terminate the Agreement for cause (and/or any order issued pursuant to the Agreement) when the other has been provided written notice of default or non-compliance and has failed to cure the default or non-compliance within a reasonable time, not to exceed thirty (30) calendar days, after receipt of such notice.

9.3. In the event of Termination, FHS will provide the means to securely transfer all active Client data to a new hosting provider. FHS will work collaboratively with the Client in the migration process to minimize downtime and ensure data integrity. If Client's exit from FHS Services is for any reason other than a material breach of this Agreement by FHS, which is left uncured for more than 30 days after Client provides FHS with notice, FHS is entitled to keep all fees paid and is not obligated to provide a refund for any unused portion of the contract period.

10. INDEPENDENT CONTRACTORS. The parties hereby acknowledge and agree that each is an independent contractor, that no party shall be considered to be the agent, representative, employer or employee of any other party for any purpose whatsoever, and that no party has any authority to enter into any contract, assume any obligations or to give any warranties or representations on behalf of any other party. Nothing in this Agreement shall be construed to create a relationship of partners, joint venturers, fiduciaries, or any other similar relationship between the parties.

11. TAXES. If any of the services or products provided under this Agreement are subject to any Taxes, such Taxes will be payable by the Client. If, after the effective date of this Agreement, a governmental entity or any political subdivision thereof assesses, or attempts to assess, Taxes not applicable or in existence at the time this Agreement becomes effective, the Client will be responsible for such Taxes, after reasonable time to appeal.

12. FHS RESPONSIBILITY. FHS shall assume responsibility for production and delivery of all services offered as a result of this Agreement. Further, FHS will be the sole point of contact on contractual matters, including payment of charges resulting from this Agreement.

13. ASSIGNMENT/SUBCONTRACTING. This Agreement may not be assigned, transferred, or sublicensed by Client, in whole or in part. FHS may assign, subcontract, transfer or sublicense this Agreement upon the consent of Client, which consent may not be unreasonably withheld. Consent is not required in the assignment, subcontract, transfer, or sublicense is to another entity in FHS's corporate family, including Fast Enterprises, LLC, whether existing now or created in the future.

14. CONFIDENTIAL INFORMATION. Pursuant to this Agreement, FHS and the Client may disclose to each other information that each may regard as proprietary or confidential and it is hereby agreed as follows:

14.1. **Definitions.**

14.1.1. "Confidential Information" will mean any non-public information that the disclosing party (the "Disclosing Party") specifically marks and designates, in writing, as confidential or which, under the circumstances surrounding the disclosure, ought to be treated as confidential. "Confidential Information" includes, but is not limited to, Client

data, designs, inventions, specifications, techniques, models, data, source code or object code, trade secrets, know-how and information relating to the technology, customers, business plans, promotional and marketing activities, pricing policies, finances and other business affairs of the Disclosing Party. For avoidance of doubt, FAST Software and its associated documentation ("Documentation") are Confidential. Further, information related to FHS's co-location data center provider(s) is also Confidential under this Agreement.

14.1.2. "Confidential Information" will not include any information which the receiving party (the "Receiving Party") can demonstrate: (i) was, at the time of disclosure, generally available to the public; (ii) was, at the time of disclosure, known to the Receiving Party and not subject to an existing agreement of confidentiality between the parties; (iii) is furnished by the Disclosing Party to third parties without restriction; (iv) is furnished to the Receiving Party by a third party who legally obtained said information and the right to disclose it; (v) is approved for release by written authorization of the Disclosing Party; or (vi) is developed independently by the Receiving Party where the Receiving Party can document such independent development.

14.1.3. "Confidential Materials" will mean all tangible materials containing Confidential Information, including but not limited to drawings, schematics, written or printed documents, computer disks, tapes, and compact disks, whether machine or user readable.

14.1.4. Any information which falls within the definitions of Confidential Information or Confidential Materials and which was disclosed or provided to the Receiving Party by the Disclosing Party or an agent of the Disclosing Party prior to the Receiving Party's signing of this Agreement will be deemed to be included in and covered by the terms and conditions of this Agreement.

14.2. **Restrictions**

14.2.1. The Receiving Party will hold all Confidential Information and Confidential Materials in confidence, will use the Confidential Information and Confidential Materials only for the purpose for which they are disclosed, will reproduce the Confidential Information and Confidential Materials only to the extent necessary for such purpose, and will not disclose the Confidential Information or Confidential Materials to any third party without the Disclosing Party's prior written consent.

14.2.2. The Receiving Party will take reasonable security precautions, at least as great as the precautions it takes to protect its own confidential information, to keep confidential the Confidential Information and Confidential Materials.

14.2.3. The Receiving Party may disclose Confidential Information or Confidential Materials only to the Receiving Party's employees or consultants on a need-to-know basis. The Receiving Party will have executed or will execute appropriate written agreements with its employees and consultants sufficient to enable it to comply with all the provisions of this Agreement.

14.2.4. If the Receiving Party becomes legally obligated to disclose Confidential Information or Confidential Materials by any governmental entity with jurisdiction over it, the Receiving Party will give the Disclosing Party prompt written notice sufficient to allow the

Disclosing Party to seek a protective order or other appropriate remedy. The Receiving Party will disclose only such information as is legally required and will use its reasonable best efforts to obtain confidential treatment for any Confidential Information or Confidential Materials that is so discloses.

14.2.5. The Receiving Party will not reverse engineer, decompile or disassemble any of the Confidential Materials without the prior written consent of the Disclosing Party.

14.2.6. At no time, under any circumstance, will any FHS Confidential Materials be removed from Client property without the prior written consent of FHS.

14.2.7. These provisions should be read to reconcile with applicable Public Records or Freedom of Information laws, and the restrictions listed here apply to the maximum extent allowable under such laws.

14.3. **Rights and Remedies**

14.3.1. The Receiving Party will notify the Disclosing Party immediately upon discovery of any unauthorized use or disclosure of the Confidential Information or Confidential Materials (including an imminent disclosure compelled by applicable Public Records or Freedom of Information laws),, or any other breach of this Agreement by the Receiving Party, and will cooperate with the Disclosing Party in every reasonable way to help the Disclosing Party regain possession of the Confidential Information or Confidential Materials and prevent its further unauthorized use. This includes not opposing any motions for preliminary or permanent injunction filed for the protection of Confidential Information or Confidential Materials.

14.3.2. All Confidential Information and Confidential Materials will remain the sole and exclusive property of the Disclosing Party. Receiving Party will upon written request from the Disclosing Party: (i) cease using the Confidential Information and Confidential Materials; (ii) return the Confidential Information and Confidential Materials and all originals, copies, reproductions and summaries of Confidential Information and Confidential Materials to the Disclosing Party within sixty (60) days of receipt of demand; and (iii) upon request of the Disclosing Party, certify in writing that the Receiving Party has complied with the obligations set forth in this paragraph.

14.4. **Miscellaneous**

14.4.1. Nothing contained in this Agreement will be construed: (i) as requiring the Disclosing Party to disclose to the Receiving Party any particular information; (ii) as granting to the Receiving Party a license, either express or implied, under any patent, copyright, trade secret or other intellectual property right, now or hereafter owned, obtained or licensed by the Disclosing Party; or (iii) as a representation or warranty as to the accuracy, completeness or reliability of the Confidential Information or Confidential Materials.

14.4.2. The Disclosing Party will not be liable for any damages arising out of the use of Confidential Information or Confidential Materials disclosed under this Agreement.

14.4.3. A Non-Disclosure Agreement provided by FHS shall be signed by the Client's agents, contractors, contractors' employees, and any other third parties (non-Client employees) who may be exposed to or gain access to FHS Confidential Information.

FAST HOSTING SERVICES

15. OWNERSHIP. Nothing in this Agreement modifies the ownership of either party's Confidential Information or intellectual property. Further, nothing in this Agreement assigns or transfers to Client any ownership in any concepts, know how, techniques, or other intellectual property related to FHS Services, regardless of whether developed as a result of this Agreement.

16. COMPLIANCE WITH LAWS. Both parties agree to comply with all applicable federal and state laws.

17. USE OF THE JURISDICTION NAME. The Client agrees that FHS may, prior to, in the course of performance of this Agreement (or any order), or thereafter use the Client's name in advertising and promotional media as a customer or client of FHS.

18. WAIVER. None of the provisions of this Agreement will be deemed to have been waived by any act or acquiescence by any party, but only by an instrument in writing signed by an authorized representative of the waiving party. No waiver of any provision of this Agreement will constitute a waiver of any other provision or of the same provision on another occasion. Failure to enforce any provision of this Agreement will not constitute waiver of such provision or any other provisions of this Agreement.

19. ENTIRE AGREEMENT. This Agreement represents the entire agreement between the parties regarding its subject matter, superseding any prior oral or written agreements or understandings relating thereto.

20. SEVERABILITY. If any provision of this Agreement is or becomes void or unenforceable by law, the other provisions remain valid and enforceable.

21. BINDING NATURE; NO THIRD PARTY BENEFICIARY. The terms and provisions of this Agreement shall be binding upon and inure to the benefit of the parties, and their respective successors and assigns, and is made solely and specifically for their benefit. No other person shall have any rights, interest or claims hereunder or be entitled to any benefits under or on account of this Agreement as a third-party beneficiary or otherwise.

22. PRECEDENCE. If any term of this Agreement is in contradiction with another agreement on a different subject matter between the parties, the terms of the later executed agreement shall prevail, without regard to any contrary provisions in the other agreement.

23. AMENDMENT. This Agreement may only be enlarged, altered, voided or modified by a written amendment signed by FHS and the Client.

24. HEADINGS. Descriptive headings and Section/Paragraph numbering in this Agreement are for convenience only and shall not affect the construction or meaning of contractual language.

25. SURVIVAL OF CERTAIN AGREEMENT TERMS. Notwithstanding anything herein to the contrary, the parties understand and agree that all terms and conditions of this Agreement and the attachment

hereto which may require continued performance, compliance, or effect beyond the termination or expiration date of the Agreement shall survive such termination or expiration date and shall be enforceable by the parties as provided herein in the event of a failure to perform or to comply by either party. Without limiting the generality of the foregoing, this specifically includes all provisions in this Agreement that relate to disclaimer of warranties, limitation of liability, confidentiality, and payment for FHS Services, all of which shall survive the termination of this Agreement.

26. FORCE MAJEURE. Neither party shall be liable or deemed to be in default for any Force Majeure delay in performance occasioned by unforeseeable causes beyond the control and without the fault or negligence of the parties, including, but not restricted to, acts of God or the public enemy, government actions, public disturbances, labor disturbances, fires, floods, epidemics, quarantines, restrictions, freight embargoes or unusually severe weather.

27. NOTICES. All deliveries, notices, requests, demands or other communications related to this Agreement that either party may be required or may desire to give to the other will be deemed received by the recipient when delivered personally; or by registered or certified mail, return receipt requested; or by overnight carrier; or upon telephone confirmation to sender of receipt of a facsimile communication which is followed by a mailed hard copy from sender. Communications should be addressed as follows:

FHS:
Fast Hosting Services, LLC
Attn: Legal
7229 S. Alton Way
Centennial CO 80112
Tel: (303) 770-3700
Email:

CLIENT:
Name: Amit Sarkar
Title: Executive Administrator Revenue Commission
Address: 617 W. Jefferson Street, Louisville, KY 40202
Telephone: 503.574.4898
Fax: 502.574.4818
Email: amit.sarkar@metrorevenue.org

28. GOVERNING LAW. This Agreement shall be construed and governed in accordance with the laws of the State of Kentucky without giving effect to Kentucky's choice of law provisions. The Agency and FAST: (i) submit to the jurisdiction of the State and federal courts located in Kentucky as the case may be; (ii) waive any and all objections to jurisdiction and venue; and (iii) will not raise forum non conveniens as an objection to the location of any litigation

29. RECORDS AUDIT. FAST shall maintain during the course of the work, and retain not less than three years from the date of final payment on the Contract, complete and accurate records of all of FAST's costs which are chargeable to Agency under this Agreement; and Agency shall have the right, at any reasonable time, to inspect and audit those records by authorized representatives of its own or of any public accounting firm selected by it. The records to be thus maintained and retained by FAST shall include (without limitation): (a) payroll records accounting for total time distribution of FAST's employees working full or part time on the work (to permit tracing to payrolls and related tax returns), as well as canceled payroll checks, or signed receipts for payroll payments in cash; (b) invoices for purchases receiving and issuing documents, and all the other unit inventory records for FAST's stores stock or capital items pertaining to the work; and (c) paid invoices and canceled checks for materials purchased and for subcontractors ' and any other third parties' charges pertaining to the work.

30. ETHICAL STANDARDS Pursuant to KRS 45A.455:
(1) It shall be a breach of ethical standards for any employee with procurement authority to participate directly in any proceeding or application; request for ruling or other determination; claim or controversy; or other particular matter pertaining to any contract, or subcontract, and any solicitation or proposal therefor, in which to his knowledge:
(a) He, or any member of his immediate family has a financial interest therein; or
(b) A business or organization in which he or any member of his immediate family has a financial interest as an officer, director, trustee, partner, or employee, is a party; or
(c) Any other person, business, or organization with whom he or any member of his immediate family is negotiating or has an arrangement concerning prospective employment is a party. Direct or indirect participation shall include but not be limited to involvement through decision, approval, disapproval, recommendation, preparation of any part of a purchase request, influencing the content of any specification or purchase standard, rendering of advice, investigation, auditing, or in any other advisory capacity.
(2) It shall be a breach of ethical standards for any person to offer, give, or agree to give any employee or former employee, or for any employee or former employee to solicit, demand, accept, or agree to accept from another person, a gratuity or an offer of employment, in connection with any decision, approval, disapproval, recommendation, preparation of any part of a purchase request, influencing the content of any specification or purchase standard, rendering of advice, investigation, auditing, or in any other advisory capacity in any proceeding or application, request for ruling or other determination, claim or controversy, or other particular matter, pertaining to any contract or subcontract and any solicitation or proposal therefor.
(3) It is a breach of ethical standards for any payment, gratuity, or offer of employment to be made by or on behalf of a subcontractor under a contract to the prime contractor or higher tier subcontractor or any person associated therewith, as an inducement for the award of a subcontract or order.
(4) The prohibition against conflicts of interest and gratuities and kickbacks shall be conspicuously set forth in every local public agency written contract and solicitation therefor.
(5) It shall be a breach of ethical standards for any public employee or former employee knowingly to use confidential information for his actual or anticipated personal gain, or the actual or anticipated personal gain of any other person.

FAST HOSTING SERVICES

31. FAST shall reveal any final determination of a violation by FAST or its subcontractors within the previous five (5) year period pursuant to KRS Chapters 136, 139, 141, 337, 338, 341 and 342 that apply to FAST or its subcontractor. FAST shall be in continuous compliance with the provisions of KRS Chapters 136, 139, 141, 337, 338, 341 and 342 that apply to FAST or its subcontractor for the duration of this Agreement.
32. FAST shall comply with the insurance requirements attached hereto and fully incorporated herein as Attachment D.

IN WITNESS WHEREOF, the parties have executed this Agreement on the day and year first above written.

Fast Hosting Services, LLC

DocuSigned by:
Todd Mortenson
14527EFD81DE48C...
Signature

Todd Mortenson
Print Name and Title
President

[Client] Louisville Metro Revenue Commission

DocuSigned by:
Angela Dunn
45C28170E2C3457...
Signature

Angela Dunn
Print Name and Title
Director

FAST HOSTING SERVICES

ATTACHMENT A

Hosting Specifications

Introduction

Fast Hosting Services LLC (FHS) commits to provide services to our clients that meet the specifications defined in this document.

Definitions

- **Actual Uptime**: total hours in the calendar quarter minus the number of hours in the calendar quarter during which the FHS Business Service is substantially unavailable and such unavailability is outside of the Scheduled Downtime;
- **Availability**: Suitable or ready for use; readily obtainable; accessible;
- **Business Continuity Plan**: a document that contains the critical information a business needs to stay running despite adverse events;
- **Disaster**: A force majeure event that destroys part or all of an FHS business service, including IT equipment, and prevents continued operations;
- **Disaster Recovery Plan**: a documented process and/or set of procedures to recover and protect an IT business service in the event of a disaster;
- **Force Majeure Event**: An unforeseeable event due to natural or man-made causes that results in the inability of a party to meet its contractual obligations;
- **FHS Business Service**: The group of applications, middleware, security, storage, networks and other supporting infrastructure that enables a comprehensive, end-to-end business process, transaction or exchange of information used to support the FAST application. The FHS Business Service does not include any inputs/outputs external to the FHS Business Service.
- **Major Incident**: an event which has significant impact or urgency on the FHS Business Service;
- **Planned Uptime**: total hours in the calendar quarter minus the Scheduled Downtime;
- **Recovery Time Objective (RTO)**: The maximum period of time that the production system, as provided through FHS's Business Service, can be down after a major incident or force majeure event has been declared;
- **Recovery Point Objective (RPO)**: the maximum period of time in which data might be lost from the FHS Business Service due to a major incident or force majeure event;
- **Scheduled Downtime**: A planned suspension of part or all of the FHS Business Service to perform maintenance or enhance system operations;
- **Service Hours**: The agreed hours, based on the availability SLA, when the FHS Business Service is to be available.
- **User Response Time:** User Response Time is the interval from the time a user transaction is received by the FHS servers, until the time that the FHS servers send a

response back to the client machine.

Data Center Facilities

1. FHS's secured racks are situated in colocation data center facilities in the continental United States;
2. Facilities are designed to meet or exceed Tier 3 data center specifications including redundancy and concurrent maintainability specifications;
3. Facilities provide geographic disparity in order to minimize risk from localized threats (earthquakes, floods, hurricanes, etc.) and leverage power and connectivity redundancies;
4. FHS's colocation data center providers will complete annual 3rd party compliance audits including SSAE 16 and the resulting SOC 2 Type II and SOC 3 reports. Evidence of these audits can be furnished to Client. However, Client may be required to sign an additional Non-Disclosure Agreement with the data center provider prior to receiving information related to the audit.

Hardware and Third-Party Software Are Included

- **Hardware and Infrastructure**:
    1. Compute, storage, network and connectivity devices within the hosted infrastructure.
    2. All equipment is kept in good working order and with active manufacturer warranties and/or support contracts.
- **Software**: FHS maintains the licenses and provides support services for third-party software utilized in the FHS Business Service, as necessary to fulfill the obligations of this Agreement. Examples include:
    1. Operating Systems
    2. Relational Database Management Systems
    3. Virtualization licensing (if applicable)
    4. Log aggregation utilities
    5. Security information and event management (SIEM) products
    6. Secure file transfer applications (if applicable)
    7. Remote access solutions
    8. End point security
    9. Backup and restore solution
    10. Disaster Recovery solution
    - FHS reserves the right to deploy, remove or modify software or hardware products at its sole discretion provided performance targets continue to be met. No tenant will be granted access to hosted systems beyond the FHS

Business Service.

Personnel

1. FHS provides managed services through dedicated staff to design, manage, administer, support and secure our hosted systems including:
    a. Systems engineers
    b. Network engineers
    c. Information security officers
    d. An FHS service manager will be the primary point of contact (POC) for FHS
2. A Client service manager will be appointed as the primary point of contact (POC) for Client

Hosted Environments Include

1. Development
2. Test
3. Training (if applicable)
4. Staging
5. Production
6. Conversion (if applicable)
7. Control (FCR)
8. Control Testing (FCS)

If applicable, eServices counterpart environments are included.

FHS sizes the underlying systems to meet the requirements of the customer. As such, FHS may make periodic adjustments to the underlying equipment. Also, environments may be combined to meet customer needs.

Important: Non-Production instances of the FAST application, including eServices, may only be used for gathering development feedback and acceptance testing. Conversion must be performed in a production environment. Mock conversions, however, may be run in a non-production environment. Any usage that exceeds the above language may result in additional costs, due to third party licensing constraints.

Backups

1. FHS maintains and monitors the system to ensure successful completion of data backups.
2. FHS conducts a backup recovery verification at least annually.

FAST HOSTING SERVICES

3. Backup data retention will meet or exceed applicable compliance or regulatory controls as appropriate for data classification or FHS policy.

Change Management

1. FHS will adhere to change management as prescribed in special publication NIST 800-53, Rev 4.
2. FHS leverages software tools to ensure changes are submitted, reviewed, and approved by a change approval board (CAB) prior to approval.
3. FHS will apply patches to the FHS Business Service during the defined Scheduled Downtime, and/or after providing advanced notice to Client.

Disaster Recovery (DR)

1. Disaster Recovery replication services will be provided for production systems only
    a. FHS will work with Client to bring additional environments on-line at the DR data center facility in the event that the primary data center is offline or unusable for more than twenty-one consecutive (21) days.
2. Redundant network paths are maintained between the primary data center facility and the secondary data center facility
3. Data will be replicated between primary and secondary data center facilities
4. Annual DR fail-over verification testing of the production environment of the FHS Business Service
    a. Verification will not include all interface inputs or outputs
    b. Backup restoration verifications are not in scope for annual DR verification
    c. During verification exercises, the system at the primary site may be offline. Data modification during the verification exercise will not be replicated from secondary (DR) site back to primary site. A Scheduled Downtime window may be required for the verification exercise and is in addition to the standard monthly maintenance window.
5. FHS will maintain a Disaster Recovery (DR) Plan that:
    a. Defines the FHS Business Service production environment and any dependencies that will be in scope for the DR protection.
    b. Defines the criteria, as mutually agreed between FHS and Client, for declaration of a disaster triggering execution of the DR plan.
    c. Lists cutover steps necessary to execute cutover of the production system to the DR facility.
6. Service Level commitments may be suspended for up to forty-five (45) days following the execution of the Disaster Recovery Plan.

Security

The agency is responsible for the application security as well as reviewing SQL audit logs. FHS is responsible for the security of the infrastructure, which includes, for example, the FHS networking equipment, hypervisors, backup storage, operating systems, and supporting third party software. The below information relates to the security of the infrastructure.

1. FHS's security program is designed to substantially meet the security controls and assessment procedures for the **Moderate-Impact Baseline** defined by the National Institute of Standards and Technology (NIST) in the special publication **NIST 800-53 (Rev 4).** The following are the NIST control families:
    a. For further information on NIST 800-53 (Rev 4) see: https://web.nvd.nist.gov/view/800-53/Rev4/home.
2. FHS services will comply with IRS Publication 1075 when FTI data is in scope.
    a. For details on IRS Publication 1075 compliance guidelines see https://www.irs.gov/pub/irs-pdf/p1075.pdf
3. FHS service security highlights:
    a. An annual 3rd party penetration test for FHS Business Services
        i. An executive summary will be furnished, upon request, to Client with remediation steps for any findings within twenty (20) business days following assessment completion
    b. Monthly vulnerability scan of internal hosted networks
    c. Monthly 3rd party vulnerability scan of external (public) facing endpoints
    d. Annual SOC 2 Type 2 report for the services that Fast Hosting Services provides
4. For purposes of compliance with the Payment Card Industry ("PCI") Data Security Standard ("DSS"), FHS does not store, transmit or process cardholder data as contemplated by PCI DSS requirements and FHS is not PCI certified. FHS understands that the Agency, as a merchant, may be subject to certain PCI DSS requirements. FHS agrees to provide to Agency information related to the subset of SAQ-A controls that are applicable to the FAST application, to aid the Agency in completing any PCI DSS assessment that the Agency may be undergoing.
5. The services provided by FHS comply with the Trust Services Criteria of security, availability, and confidentiality. FHS's compliance is verified annually by a SOC 2 examination. The latest SOC 2 Type 2 report will be made available for agencies to request.
6. FHS will support Agency audits by participating in audits performed by federal agencies as well as assisting with other security audits not addressed by the SOC 2 Type 2 Reports.

Service-Levels Commitments

1. Applicability: These service level commitments shall only apply while the primary hosting facility is being used as the production system. These service level commitments shall not apply in the event the production system has failed over to the secondary disaster recovery hosting facility.
2. Availability: Production FHS Business Services uptime will meet 99.80%, measured at the FHS perimeter over the course of each calendar quarter.
    a. The availability requirement will be calculated as follows:
        Actual Uptime ÷ Planned Uptime x 100
    b. Exceptions: No period of degradation or inoperability will be included in calculating availability to the extent that such downtime or degradation is due to any of the following exceptions:
        i. Failures of the Client or its authorized users' infrastructure, internal networks,
        internet connectivity or dedicated circuits;
        ii. Any downtime or degradation not related to the FHS Business Service or other services provided by FHS
        iii. Any downtime or degradation related to software, hardware, networks, systems, services, etc. not administered by FHS
        iv. Scheduled Downtime
3. Recovery Point Objective: RPO <= 4 hours
    a. Replication is configured to keep production data replicated every 5 minutes
4. Recovery Time Objective: RTO <= 12 hours
5. User Response Time: In the Production environment, User Response Time must be <= two (2) seconds 95% of the time measured across each calendar quarter following a ninety (90) day post roll-out period. In the Production environment User Response Time must be <= two (2) seconds 90% of the time during the initial ninety (90) days following a roll-out.
    a. Exclusions from User Response Time service level commitment:
        i. Reports (Reports, Data Cubes, AdHocs, MySearches)
        ii. Mail generation
        iii. Batch job processing
        iv. Customer software dependent on external systems
        v. Interfaces (transactions with call-outs to external systems)
        vi. Web Publishing
        vii. Logging in (including Single Sign On)
        viii. Whitelisted transactions

FAST HOSTING SERVICES

6. Scheduled Downtime: Scheduled downtimes for production FHS Business Services will not exceed twelve (12) hours per month without prior approval from Client.
    a. Scheduled downtimes for production FHS Business Services will be communicated in writing to client with a minimum of five (5) business days' notice.
        i. Situations may arise that require more urgent remediation (e.g. new security vulnerabilities), in which FHS and the client may shorten the notice, when there is mutual agreement
    b. Scheduled downtimes for non-production FHS Business Services will be coordinated to minimize impact to the Client.
7. Backups: FHS must ensure 95% of backup jobs complete successfully measured across each calendar quarter, including:
    a. Daily backups to local backup system
    b. Weekly backup to local backup system
    c. Weekly backups copied to remote disk or tape
8. Service-Level Reports: Service Level Reports will be provided to Client within ten (10) business days after the end of each calendar quarter. The report will describe the defined service level commitments for the prior calendar quarter as compared to the realized service levels.

Fast Monitoring

Fast will providing monitoring services as outlined in Attachment – C "Fast Monitoring Services Statement of Work".

Hosting Services Do Not Include

1. Printing equipment and services, including post-printing processes (folding, stuffing, etc.) or installation of printers on FHS servers
2. Telecom equipment and services
3. Client site internet circuits
4. Client dedicated network circuits
5. Client infrastructure and networking
6. Opening, scanning, data entry or processing of documents
7. End user workstations and software
8. User help-desk support

FAST HOSTING SERVICES

9. 3rd party software other than that which is required to deliver our standard services described above (E.g. MS Windows, MS SQL Server and virtualization software are included, but FAST application license is not. Additional client software for external interfaces such as IVR, are also not included)
10. Client Business Continuity Plan
11. Direct access to databases for purposes other than development or debugging purposes

FAST HOSTING SERVICES

ATTACHMENT B

PAYMENT SCHEDULE

Fast Hosting Pricing[1]	Dates	
Year 1, Day 1 (prorated)	February 1, 2022 – June 30, 2022	$159,205.00
Year 2, Day 1	July 1, 2022 – June 30, 2023	$390,000.00
Year 3, Day 1	July 1, 2023 – June 30, 2024	$390,000.00
Year 4, Day 1	July 1, 2024 – June 30, 2025	$390,000.00
Total		$1,329,205

FAST will invoice the Agency quarterly in accordance with the schedule below:

Quarterly Payment Schedule

Contract Year	Invoice Date	Amount
Year 1 – $159,205.00	2/1/22	$61,705.00
	4/1/22	$97,500.00
Year 2 - $390,000.00	7/1/22	$97,500.00
	10/1/22	$97,500.00
	1/1/23	$97,500.00
	4/1/23	$97,500.00
Year 3 - $390,000.00	7/1/23	$97,500.00
	10/1/23	$97,500.00
	1/1/24	$97,500.00
	4/1/24	$97,500.00
Year 4 - $390,000.00	7/1/24	$97,500.00
	10/1/24	$97,500.00
	1/1/25	$97,500.00
	4/1/25	$97,500.00

[1] This price includes FAST Monitoring Services as described in Attachment C as long as the Agency continues to purchase a minimum of 3 FAST Enterprises, LLC resources under the current Maintenance and Support Agreement with the Agency.

ATTACHMENT C

FAST ENTERPRISES

FAST Monitoring Services Statement of Work

FAST ENTERPRISES

Table of Contents

FAST ENTERPRISES

1 Overview

This document outlines the FAST Monitoring Services (FMS), along with specifications for its delivery. The objective of these services is to provide quality FAST system monitoring services that remove that burden from the client.

This document is intended to clarify the roles and responsibilities of the FAST Monitoring Services, to best meet the objectives of these services.

1.1 Termination of Service

Either party has the right to terminate these services by giving at least 30 days' notice in writing to the other party. Either party may terminate these services by written notice to the other at any time if the other party commits a breach of service and, in the case of a breach capable of remedy, fails to remedy the breach within 14 days of being requested to do so.

1.2 Performance

FMS will provide its services under the following guidelines:

- All work will be performed by FAST employees.
- No part of these services will be subcontracted.
- All monitoring will be performed from within the United States.
- All FMS operators will be submitted by FAST to the client for provisioning and authorization.
- FAST will maintain a list of employees' authorized access. Clients will be provided a list of FMS operators, along with any recent changes, in a monthly report.
- FMS operators are restricted to only batch monitoring-related functionality with extremely limited access to application data. The operators have been trained and informed that if client data is inadvertently accessed, then it shall be treated as confidential and not be divulged or made known in any manner to any person except as necessary in the performance of their duties.
- FMS will provide monitoring coverage.
    - In the unlikely event that there is an issue preventing batch monitoring from occurring in the FAST Development Center, FAST should provide as much warning as possible to the client.
    - Batch monitoring will occur from the FAST Development Center.
    - In cases where batch monitoring from the FAST Development Center is not possible or if the FAST Development Center is closed, batch monitoring may be able to be done by remote VPN access to the FAST domain or requests to on-site FAST project resources for backup batch monitoring support. If neither the FAST Development

Center nor the on-site FAST project resources can support batch processing, the client must perform one or more of the following tasks:

- Allow the job stream(s) to run without support from monitoring personnel;
- Cancel the job stream(s);
- Provide client resources to monitor the job stream(s).

- If FMS is unable to perform its obligations under the terms of this *Statement of Work* because of acts of God, strikes, failures of a carrier or utilities, equipment or transmission failures or damages that are reasonably beyond its control, or any other cause that is reasonably beyond its control, FMS shall not be liable for the unmonitored units of work and their associated damages. Performance under this *Statement of Work* shall resume when FMS is able to substantially perform its duties.

The client will have the right to terminate the services if FAST fails to provide the safeguards described above.

1.3 Scope of Work

FAST Monitoring Services can include the following types of tasks:

- Server Updates:
  - Viewing;
  - Adding;
  - Aborting.
- Job Streams:
  - Viewing;
  - Adding;
  - Stopping;
  - Scheduling and rescheduling;
  - Aborting;
  - Adjusting attributes, including, but not limited to:
    - Scheduled start dates
    - RunDates
    - Email specifications.
- Jobs:
  - Viewing;
  - Adding;
  - Scheduling and un-scheduling;
  - Adjusting attributes, including, but not limited to:
    - Threads
    - Email specifications
    - Documentation
    - Groups
    - Dependencies
    - Parameters
  - Examining errors and interventions;

FAST ENTERPRISES

  - Requeuing and archiving events, if required to address jobs that have stopped the stream;
  - Computing projected job durations.
- Monitoring:
  - Job streams that stop
  - Job streams stuck in inconsistent states
  - Job streams that will not complete in a timely fashion
  - Jobs that fail and stop the stream
  - Jobs that have excessive failure rates
  - Jobs that exceed their max duration calculations
  - Jobs that significantly exceed prior durations
- Issue Resolution:
  - Following the client's documented job procedures;
  - Escalating issues;
  - Assisting with troubleshooting:
    - Router monitor
    - SQL Trace
    - Errors, deadlocks, timeouts, counts, processed, etc.
- Reporting:
  - Sending completion reports that include failures, escalations, errors, and other key metrics.
- Monthly Summary Reporting:
  - Sending monthly summary reports that include general job stream trends and other key metrics.
- *Special Request Tickets*:
  - Implementing approved client special requests that fall into the scope outlined above.

1.4 Issue Resolution Procedures

FMS will follow the issue resolution procedures outlined below during batch monitoring:

Issue	Escalation Process	Escalation Timeframe
Server Update Failures	If a server update is associated with a job stream, then the stream will be delayed and escalation will occur. If the server update is not associated with any job streams, escalation will occur. For issues relating to server updates, the primary contacts will be the FAST or client Tech team that is configured in the Batch Monitoring work item.	Within 30 minutes of receiving a failure notification If no notification is received, before the stream start time
Server Updates Not Complete	If a server update is associated with a job stream, then the stream will be delayed and escalation will occur.	Within 30 minutes of receiving a failure notification

Issue	Escalation Process	Escalation Timeframe
	If the server update is not associated with any job streams, escalation will occur. For issues relating to server updates, the primary contacts will be the FAST or client Tech team that is configured in the Batch Monitoring work item.	If no notification is received, before the stream start time
Job Stream Issues	If a job stream is inaccessible or unresponsive, escalation will occur. If the job stream status is suspect, escalation will occur. If the job stream will not complete in a timely fashion and may run into the next business day or another scheduled job stream or server update, escalation will occur. For job stream-related issues, the respective contact escalation order will be the job stream's call tree and then the Batch Monitoring work item contacts. However, the contact escalation order may vary depending on client documentation.	Within 30 minutes
Stopped Job Streams Due to Job Failures	Operators will follow a specific job's instructions in the FAST application under the job stream's *Documentation* tab: • If there is no documentation, escalation will occur. • If documentation cannot be successfully implemented, escalation will occur. For job-related issues, the respective contact escalation order will be the job stream's call tree, the primary developer on the job, the secondary developer on the job, and then the Batch Monitoring work item contacts. However, the contact escalation order may vary depending on client documentation.	Within 30 minutes
Long-Running Jobs	The FMS team will review a specific job's specifications under the job stream's *Documentation* tab, which can be used to modify the default processes outlined below: • If the job's maximum duration is configured and the job's duration exceeds it, an examination will	Within 30 minutes or as documented on the job

Issue	Escalation Process	Escalation Timeframe
	be performed and, if required, escalation will occur. • If the job's maximum duration is not configured and the job's duration is 30 minutes over the historic average, escalation will occur. ℹ **Note**: FAST recommends that the client configure maximum durations to ensure that escalation occurs within its preferred timeframe. • If the job has excessive errors, deadlocks, or timeouts, escalation will occur. ℹ **Note**: FAST recommends that the client configure *Stop at Errors* and *Error Percentage* to ensure that the desired failure rates are noted. • If the job does not indicate that it will complete in a timely fashion and may run into the next business day or another scheduled job stream or server update (based on its estimated time of completion and events per minute), escalation will occur. For job-related issues, the respective contact escalation order will be the job stream's call tree, the primary developer on the job, the secondary developer on the job, and then the Batch Monitoring work item contacts. However, the contact escalation order may vary depending on client documentation.	
Special Request Issues	If there is a special request that cannot be implemented as requested, the respective contact escalation order will be the sender of the special request, the job stream's call tree, and then the Batch Monitoring work item contacts. However, the contact escalation order may vary depending on client documentation.	Within 30 minutes or as documented on the *Special Request Form*

If the escalation process that is listed above does not result in a successful client contact, the FMS operators will attempt to use the site contact information that is configured in the FAST FCR Batch Monitoring contacts.

1.5 Provisioning Requirements

Account provisioning and authorization are required for the FAST Monitoring Services (FMS) batch operators. FAST will comply with all client requirements and policies for provisioning. These requirements can include background checks, confidentiality agreements, and training.

FMS will provide advance notification to the client when additional FMS operators start. The client will make a best-effort attempt to provision the new accounts within 10 business days of receiving the required paperwork. If the client does not provision an operator within that timeframe and there are FMS scheduling problems, FMS may not be able to perform its monitoring duties.

FMS will notify clients within one business day if employment is ceased for an FMS operator. The client is responsible for ceasing the operator's corresponding accounts.

1.6 Inspection

The client will have the right to inspect the FAST facilities and operations where the FMS services are performed. Client must provide FAST with at least 10 business days' notice prior to visiting any FAST facility.

1.7 References

The following documents are references for this *Statement of Work*:

- *FAST Monitoring Services Preparation - Batch Monitoring Units of Work Setup Guide*
- *FAST Monitoring Services Preparation - Batch Monitoring Application*
- *Batch Monitoring Application Site Features Security*
- *Memo FAST Monitoring Services - Batch Application Communication Security*
- *FAST Monitoring Services Preparation - Transition Plan Template*
- *FAST Monitoring Services Preparation - Client Configuration Review*
- *FAST Monitoring Services Preparation - Job Stream Monitoring Data*
- *FAST Monitoring Services Preparation – User Status Check Scan Job*
- *Account Provisioning Tool Guide*

2 Service Prerequisites

To successfully transition to the FAST Monitoring Services (FMS), the following prerequisites need to be completed:

Prerequisite	Description
Provision Accounts	Provision and authorize the FMS operators. Necessary client forms and instructional steps should be configured in FAST FCR. This will provide a centralized location to manage or view account provisioning updates or changes. Project sites should confirm documented client approval to create batch operator accounts in case they need to be referenced in the future. This should typically be handled by the client account provisioning process, however this may differ from site to site. **Note**: Refer to the *Account Provisioning Tool Guide*.
Monitor Units of Work	Determine and configure the batch monitoring units of work. These units of work are configured in FAST FCR and typically include server updates (for the FAST application and e-Services) before nightly job streams and job streams that run outside of business hours. Information such as the batch monitoring application URL, site holidays, site contacts should also be configured. **Note**: Refer to the *FAST Monitoring Services Preparation - Batch Monitoring Units of Work Setup Guide*.
FAST Batch Monitoring Application	This is generally configured as a separate FAST application from the Production environment, which will be used by FMS operators to monitor client job streams. The Batch Monitoring application should be set up with the appropriate security to allow the FMS operators to fulfill their monitoring responsibilities. This security may vary depending on the client's monitoring requirements. **Note**: Refer to the *FAST Monitoring Services Preparation - Batch Monitoring Application* and *Batch Monitoring Application Site Features Security*.
FAST Batch Monitoring Application Communication Security	Because FMS operators will be monitoring job streams remotely, the Batch Monitoring application is required to be externally accessible. Security is an important concern and, in order to mitigate the risks of exposing external endpoints, several key security procedures, processes, and technologies are recommended to be set in place. **Note**: Refer to the *Memo FAST Monitoring Services - Batch Application Communication Security*.

Prerequisite	Description
FAST Monitoring Services PowerPoint	Have project batch monitoring resource review with on-call staff and developers the *FAST Monitoring Services PowerPoint*. This will help set expectations for the service and go overs tips on how to maintain a streamlined batch monitoring process. Note: Refer to the *FAST Monitoring Services* PowerPoint.
Transition Plan	During the FMS transition process, there will be three phases. The *Transition Plan* is used to provide a structured cutover period during which communication lines are opened and the FMS operators can validate the client's stream. **Note**: Refer to the *FAST Monitoring Services Preparation - Transition Plan Template*.
Client Configuration Review	The client configuration review helps ensure that the configuration and documentation are appropriate for the work the FMS team will perform. **Note**: Refer to the *FAST Monitoring Services Preparation - Client Configuration Review*.
User Status Check Scan Job Implementation	The client implementation of this scan job for FMS operators will help do a status check on their users. The notifications from this job assist in preventing and remediating issues such as ceased or expired accounts/passwords. **Note**: Refer to the FAST Monitoring Services Preparation – User Status Check Scan Job
Check Server Update Scan Job Implementation	The client implementation of this scan job for checking successfully completed server updates as the first job in any job streams dependent on a server update. **Note**: Refer to the FAST Monitoring Services Preparation – Check Server Update Scan Job
Job Stream Monitoring Data	Sending client job stream monitoring data to FAST is a prerequisite for transitioning to FMS. This data supplements the batch monitoring process as FAST will utilize it for both alerting and reporting purposes. **Note**: Refer to the *FAST Monitoring Services Preparation - Job Stream Monitoring Data*.

3 Monitoring Escalation

In the event that an escalation is required by the FMS operators, the hierarchy for determining client contacts is outlined below:

3.1 Job Stream Call Tree

The FAST application's call trees in the Job Stream manager contain contact information that is related to each specific job stream. The call tree is generally the primary resource for FMS operators in the event of an issue with a job stream.

If the staff rotation schedule is simple enough to express in words, these instructions can be entered in each contact's **Note** field. For example, the **Note** field could state *Monday-Thursday* for one user and *Friday* for another to indicate their availabilities.

> **Note**: FAST recommends that the client review the job stream on the first business day of each week to ensure that the call tree data is accurate.

3.2 Job-Specific Contact Information

For critical job stream jobs, the primary and secondary developers can be specified with documented instructions on how to contact these individuals. The **Primary Developer** and **Secondary Developer** fields can be completed to ensure that issues are escalated directly to the responsible on-site resources.

If the developers should be first point of contact before the job stream call tree, this can be documented in the job stream documentation.

3.3 FAST FCR Batch Monitoring Contacts

The Batch Monitoring contacts that are specified by the client in the FAST FCR Batch Monitoring control will be used when there is an issue preventing access to the FAST application call tree list or a notification via the call tree list was unsuccessful.

> **Note**: FAST recommends that contacts in this list be reviewed annually by on-site FAST resources.

4 FAST Batch Operator Contact Information

The recommended method to initiate contact with the FMS operators is to use the information listed below:

4.1 General Night Operators Group Contact Information

The FAST Night Operators group should be reached using the following contact information:

By Email	• NightOps@fastenterprises.com

By Phone	• Business Cell: (720) 390-8952 • Business Voice Over Internet Protocol (VoIP): (303) 773-4099 • International Toll-Free for New Zealand and Finland: +800 33771337

4.2 Monthly Batch Monitoring Summary Report Contact Information

In the unlikely event that there is no response from the Night Operators group, the contact information in the *Monthly Batch Monitoring Summary Report* can also be used. This report contains a list of active FMS operators along with their contact information. The client will try reaching each contact, in order, until a response is received.

4.3 FAST Monitoring Services Leadership Contact Information

The list below includes the FAST Monitoring Services leadership. These individuals do not require client provisioning or access to the Batch Monitoring application. This contact list should be used by the client in emergency situations after other channels to contact the FMS operators have been attempted. The client may also contact these individuals to address client concerns or discuss changes to the FAST Monitoring Services.

Name	Role	Phone Number	Email Address
Andy Tran	Project Manager	(626) 478-8729	atran@gentax.com
Latigo Biggins	Director	(720) 284-9894	lbiggins@gentax.com

5 Special Request (SPR) Ticket

FMS operators should be notified by the client of special requests that need to be performed. Special requests should be submitted by emailing NightOpsSPRTicket@fastenterprises.com or adding a NightOps Special Request ticket through FAST FCR's Ticket Manager. FMS operators will make a best-effort attempt to support last-minute requests and handle special requests when the functionality to implement them is available to FAST.

Note: FAST recommends that ticket be submitted with a least two hours of notice.

FMS should acknowledge its receipt of a *Special Request Ticket* as soon as possible by assigning it out and setting a due date on the ticket. FMS should also update the status of the request once it has been completed and communicate with the ticket submitter.

Note: FAST recommends that the client avoid the use of the SPR process, when possible, by implementing desired adjustments themselves.

SPRs are generally intended for activities such as:

- Delaying batch processing;

- Making minor adjustments when it is not possible to make them in advance (e.g., adjustments related to functionality that is migrated to the Production environment in the same night);
- Running streams that are not normally monitored.

SPR requirements include:

- Approval by someone on the client call tree;
- Clear and complete instructions;
- FMS operators with sufficient access to implement the SPRs.

In the event that it is not possible to implement an SPR, the job streams will not be started, and client escalation will occur.

FAST HOSTING SERVICES

ATTACHMENT D – INSURANCE REQUIREMENTS

Prior to commencing work, FAST shall obtain at its own cost and expense the following types of insurance through insurance companies licensed in the State of Kentucky. Insurance written by non-admitted carriers will also be considered acceptable, in accordance with Kentucky Insurance Law (KRS 304.10-040). Workers' Compensation written through qualified group self-insurance programs in accordance with Kentucky Revised Statutes (KRS 342.350) will also be acceptable. FAST shall not commence work under this Contract until all insurance required under the Contract Document has been obtained and until copies of policies or certificates thereof are submitted to Louisville/Jefferson County Metro Government's Purchasing Division and approved by the Louisville/Jefferson County Metro Government's Risk Management Division. FAST shall not allow any subcontractor's to commence work until the insurance required of such subcontractor's has been obtained and copies of Certificates of Insurance retained by FAST evidencing proof of coverages.

Without limiting FAST's indemnification requirements, it is agreed that FAST shall maintain in force at all times during the performance of this agreement the following policy or policies of insurance covering its operations, and require subcontractors s, if subcontracting is authorized, to procure and maintain these same policies until final acceptance of the work by the Louisville/Jefferson County Metro Government (Metro). Metro may require FAST to supply proof of subcontractor's insurance via Certificates of Insurance, or at Metro's option, actual copies of policies.

A. The following clause shall be added to FAST's (and approved subcontractor's Commercial General Liability Policies:

1. "The Louisville/Jefferson County Metro Government, its elected and appointed officials, employees, agents and successors are added as an "Additional Insured" as respects operations of the Named Insured performed relative to the contract."

B. The insurance to be procured and maintained and minimum Limits of Liability shall be as follows, unless different limits are specified by addendum to the contract (and such minimum limits shall not limit access to the full amount of insurance available (whether through primary, excess or umbrella policies) on FAST's or subcontractors policy(ies), if that/those policy(ies) provide for Limits above the minimum):

1. COMMERCIAL GENERAL LIABILITY, via the Occurrence Form, primary, non contributory, with a $10,000,000 Combined Single Limit for any one Occurrence and $10,000,000 aggregate for Bodily Injury, Personal Injury, Property Damage, and Products/Completed Operations including:

    a. Premises - Operations Coverage
    b. Products and Completed Operations
    c. Contractual Liability

d. Broad Form Property Damage
e. Personal Injury

2. PROFESSIONAL LIABILITY (Errors and Omissions Including Cyber Liability Insurance), with limits not less than $5,000,000 per occurrence or claim, $5,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by FAST in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property including copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. In the event that the FAST's policy is written on a "Claims Made" Form, the FAST shall, after work has been completed, furnish evidence that the liability coverage has been maintained for at least two years after completion of work, either by submitting renewal policies with a Retroactive Date of not later than the date work commenced under this contract, or by evidence that the FAST has purchased an Extended Reporting Period Endorsement that will apply to any and all claims arising from work performed under this contract.

3. WORKERS' COMPENSATION insuring the employers' obligations under Kentucky Revised Statutes Chapter 342 at Statutory Limits, and EMPLOYERS' LIABILITY - $100,000 Each Accident/$500,000 Disease - Policy Limit/$100,000 Disease - Each Employee.

C. ACCEPTABILITY OF INSURERS

Insurance is to be placed with Insurance Companies with an A. M. Best Rating of no less than "A-VI", unless proper financial information relating to the Company is submitted to and approved by Metro's Risk Management Division.

D. MISCELLANEOUS

1. FAST shall procure and maintain insurance policies as described herein and for which the Louisville/Jefferson County Metro Government's Purchasing Division shall be furnished Certificates of Insurance upon the execution of the Contract. The Certificates shall include the name and address of the person executing the Certificate of Insurance as well as the person's signature. If policies expire before the completion of the Contract, renewal Certificates of Insurance shall be furnished to Metro at least fifteen (15) days prior to the expiration of any policy(s).

2. Upon execution of the contract, Certificates of Insurance as required above shall be furnished to:

FAST HOSTING SERVICES

Louisville/Jefferson County Metro Government
Office of Management and Budget
Purchasing Division
611 West Jefferson Street
Louisville, Kentucky 40202

3. Upon Renewal of insurance coverage (s), Certificates of Insurance evidencing renewal shall be furnished to:

Louisville/Jefferson County Metro Government
Office of Management and Budget
Risk Management Division
611 West Jefferson Street
Louisville, Kentucky 40202

4. CANCELLATION OR MATERIAL CHANGE OF COVERAGE: FAST shall notify Metro's Risk Management Division of any policy cancellation within thirty (30) business days of its receipt of same. Upon any material change (changes that reduce/restrict limit or terms and conditions to your insurance coverage) in coverage as required above, FAST shall notify Metro's Risk Management Division within thirty (30) business days. If FAST fails to notify Metro as required by this Agreement, FAST agrees that such failure shall be a breach of this Agreement. Metro reserves the right to require the insurance policy(s) required above to be specifically endorsed to provide notice of cancellation and/or material change of coverage in accordance with policy provisions. When requested by the Metro Government, a copy of the policy endorsement shall be provided to Metro's Risk Management Division.

5. Approval of the insurance by Metro shall not in any way relieve or decrease the liability of FAST hereunder. It is expressly understood that Metro does not in any way represent that the specified Limits of Liability or coverage or policy forms are sufficient or adequate to protect the interest or liabilities of FAST.

Attachment E - IRS Publication 1075

Non-Disclosure Agreement between Fast Data Services and the Louisville Metro Revenue Commission

Fast Hosting Services (Contractor) hereby agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the contractor or the contractor's employees.

(2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

(3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

DocuSigned by: Todd Mortenson 14527EFD81DE48C...
Todd Mortenson
Fast Hosting Services
6/4/2021

DocuSigned by: Angela Quinn 45C28170E2C3457...
6/4/2021

(7) All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.

(8) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.

(9) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.(10) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material

in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A. The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

APPROVED:

Fast Hosting Services

DocuSigned by:
Todd Mortenson
14527EFD81DE48C...

Todd Mortenson

Fast Hosting Services
Fast Hosting Services

6/3/2021
Date

LOUISVILLE METRO REVENUE COMMISSION

DocuSigned by:
Angela Dunn
45C28170E2C3457...

Angela Dunn
Secretary/Treasurer
Louisville Metro Revenue Commission

6/3/2021
Date