

TechShare Local Government Corporation and Tarrant County

Mental Health Alert System Development and Implementation Project Addendum

1. Background and Purpose

- 1.1. This Development Project Addendum for the development of TechShare.Mental Health Alert System (herein after “this Addendum”) is an addendum to the Master Interlocal Agreement for Stakeholder Participation in TechShare.
- 1.2. This Addendum is entered by and among TechShare Local Government Corporation hereinafter (“TechShare LGC”)and the Participants.
- 1.3. Each of the undersigned Participants is a signatory to the Master ILA.
- 1.4. To the extent that any provision of this Addendum conflicts with the terms and conditions of any provision of the Master ILA, then this Addendum governs.

2. Definitions.

Capitalized terms used in this Addendum have the meanings as set forth in the Master ILA. The following capitalized terms, not otherwise fully defined within this Addendum, have the following meanings:

- 2.1. Development Project: The project to develop TechShare Mental Health Alert System pursuant to the Project Addendum to the TechShare Master ILA for the Development of TechShare.Mental Health Alert System
- 2.2. Master ILA: The Master Interlocal Agreement for Stakeholder Participation in in the TechShare Program, which was effective on January 1, 2019.
- 2.3. Participants: Participants is defined as all local governments executing this Addendum.
- 2.4. Parties: Parties is defined as the Participants and and TechShare.
- 2.5. Production Environment: Production Environment is defined as the TechShare Azure CJIS Compliant Government Tenant designed to operate TecShare.Mental Health Alert System for Participants.
- 2.6. Production Version: Production Version is defined as that version of TechShare.Mental Health Alert System that is made available for use by Participants.
- 2.7. TechShare.Mental Health Alert System: TechShare.Mental Health Alert System is defined as the full-featured mental health alert system, including all versions, to be utilized by the Participants.

3. Term of Addendum

- 3.1. This Addendum shall be effective from the date it is approved by both parties through the completion of the scope of work as set forth in Attachment A.

4. TechShare.Mental Health Alert System Funding Formula

- 4.1. The funding formula for TechShare.Mental Health Alert System shall be based on population.

5. Role and Responsibilities of TechShare

- 5.1. TechShare will not provide services beyond the scope of work and time estimates established by this Addendum. TechShare will negotiate in good faith with Tarrant County to amend this Addendum to accommodate changes to the Addendum's scope of work and time estimates, in the event either will be exceeded.
- 5.2. The TechShare Team will comply with all rules and regulations regarding appropriate use of Tarrant County property, including Tarrant County facilities. Tarrant County shall provide such rules and regulations to TechShare in writing.
- 5.3. TechShare shall limit access to Tarrant County's confidential, proprietary information solely to those persons or entities to whom such disclosure is necessary to perform the purposes stated herein.
 - 5.3.1. TechShare agrees that under no circumstances shall TechShare permit disclosure, access, distribution, copying, review, or examination of Tarrant County's confidential or proprietary information by any other party not authorized herein.
 - 5.3.2. All reasonable security precautions, at least as great as the precautions TechShare takes to protect its own confidential information, but no less than reasonable care, shall be taken by TechShare to prevent unauthorized use or disclosure of Tarrant County's confidential or proprietary information.
 - 5.3.3. TechShare shall require all contractors to commit to the same responsibilities regarding Tarrant County's confidential or proprietary information as borne by TechShare under this Addendum.

6. Compensation of TechShare

- 6.1. TechShare shall be compensated as set forth in Attachment A.
- 6.2. Payments as set forth in the Project Budget included in Attachment A are due from Tarrant County as specified in the Payment Schedule.

7. Access to Source Code

- 7.1. Representatives from each Participant shall be given continuing access to the source code for TechShare.Mental Health Alert System as well as access to any other software needed to compile and/or build TechShare.Mental Health Alert System, in the source code repository maintained by the TechShare LGC.

8. Miscellaneous

- 8.1. This Addendum may not be amended except in a written instrument specifically referring to this Addendum and signed by the Parties hereto.
- 8.2. Each Party represents that it has, as of the date of the execution of this Addendum, obtained all requisite approvals and authority to enter into and perform its obligations under this Addendum, including the funds necessary to satisfy its obligations herein.
- 8.3. In the event any term or provision of this Addendum conflicts with any provision of law or is declared to be invalid or illegal for any reason, this Addendum will remain in full force and effect and will be interpreted as though such invalid or illegal provision were not a part of this Addendum. The remaining provisions will be construed to preserve the intent and purpose of

this Addendum and the Parties will negotiate in good faith to modify any invalidated provisions to preserve each Party's anticipated benefits.

- 8.4. The parties to this Addendum will encourage the prompt and equitable settlement of all controversies or claims between them. The parties agree to negotiate their differences directly and in good faith for a period of no less than thirty days after receiving written notification that there is a dispute. If the dispute is not resolved within thirty days after written notification of the existence of a dispute, the parties agree to submit their dispute to an experienced mediator who is located in Tarrant County, Texas to work with them to resolve their differences with non-binding mediation. This mediation is a compromise negotiation for purposes of Rule 408 of the Federal Rules of Evidence and Texas Rules of Evidence and is an alternative dispute resolution procedure subject to Texas Civil Practice & Remedies Code section 154.073.
- 8.5. This instrument contains the entire addendum, with respect to implementation, between the parties relating to the rights granted and the obligations assumed. Any prior implementation addendums or representations not expressly set forth in this addendum are of no force.
- 8.6. This addendum does not create any relationship between the parties other than that of independent entities contracting with each other solely for the purpose of effecting the provisions of this addendum. Agents or employees of any party will not be deemed the employee or agent of another party.
- 8.7. Participants and TechShare agree that each is responsible for its own proportionate share of any liability for the negligent acts or omissions of its employees, agents, contractors, or subcontractors arising out of, connected with, or as a consequence of its performance under this Addendum. Neither party will be liable to the other for any indirect, special, incidental, punitive, or consequential damages, including for loss of business, revenue, profits, or other economic advantage. This is regardless of how the damage arises, whether in action of contract, negligence, tort, or other action, arising out of or in connection with this contract, even if advised of its possibility.
- 8.8. Entities that Boycott Israel and Prohibition against Involvement with Iran, Sudan, and Foreign Terrorist Organizations. In compliance with Texas Government Code Section 2252.152, TechShare verifies that it does not boycott Israel and will not boycott Israel during the term of this Agreement. TechShare further verifies that it is not engaged in business with Iran, Sudan, or any foreign terrorist organization. The term "foreign terrorist organization" means an organization designated as a foreign terrorist organization by the United States Secretary of State as authorized by 8 U.S.C. Section 1189.
- 8.9. Compliance with Laws. In providing the services required by this Agreement, TechShare must observe and comply with all applicable federal, state, and local statutes, ordinances, rules, and regulations, including, without limitation, workers' compensation laws, minimum and maximum salary and wage statutes and regulations, and non-discrimination laws and regulations. TechShare shall be responsible for ensuring its compliance with any laws and regulations applicable to its business, including maintaining any necessary licenses and permits.
- 8.10. Trade Associations. In compliance with Section 2274.002 of the Texas Government Code, TechShare certifies it does not boycott energy companies and shall not boycott energy companies during the terms of this Agreement. "Boycott energy company" is defined in Section 809.001(1) and means, without an ordinary business purpose, refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations with a company because the company: (A)

engages in the exploration, production, utilization, transportation, sale, or manufacturing of fossil fuel-based energy and does not commit or pledge to meet environmental standards beyond applicable federal and state law; or (B) does business with a company described by subsection (A).

- 8.11. Discrimination against Firearm Entities or Firearm Trade Associations Prohibited. In compliance with Section 2274.002 of the Texas Government Code, TechShare certifies that it does not have a practice, policy, guidance or directive that discriminates against a firearm entity or firearm trade association; and will not discriminate during the term of the above described contract] against a firearm entity or firearm trade association. “Discriminate against a firearm entity or firearm trade association” is defined in Section 2274.001(3) and means, with respect to the entity or association, to: (i) refuse to engage in the trade of any goods or services with the entity or association based solely on its status as a firearm entity or firearm trade association; (ii) refrain from continuing an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association; or (iii) terminate an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association; the term *does not include*: (i) the established policies of a merchant, retail seller, or platform that restrict or prohibit the listing or selling of ammunition, firearms, or firearm accessories; and (ii) a company’s refusal to engage in the trade of any goods or services, decision to refrain from continuing an existing business relationship, or decision to terminate an existing business relationship: (aa) to comply with federal, state, or local law, policy, or regulations or a directive by a regulatory agency; or (bb) for any traditional business reason that is specific to the customer or potential customer and not based solely on an entity’s or association’s status as a firearm entity or firearm trade association.

9. Attachments Incorporated

- 9.1. Attachment A: Statement of Work is incorporated into this Addendum as if fully set forth herein.
- 9.2. Attachment B: Federal Bureau of Investigation Criminal Justice Information Services Security Addendum.

This Addendum may be executed in multiple counterparts each of which will be deemed an original, but all multiple counterparts together will constitute one and the same instrument.

[Signature Page to Follow]

SIGNED AND EXECUTED this _____ day of _____, 2024.

**COUNTY OF TARRANT
STATE OF TEXAS**

By: _____

Tim O'Hare, County Judge

APPROVED AS TO FORM:

Kimberly Colliet Wesley

Criminal District Attorney's Office*

*By law, the Criminal District Attorney's Office may only approve contracts for its clients. We reviewed this document as to form from our client's legal perspective. Other parties may not rely on this approval. Instead those parties should seek contract review from independent counsel.

CERTIFICATION OF FUNDS IN THE AMOUNT OF \$ _____

_____ Date: _____

AUDITOR

TECHSHARE LOCAL GOVERNMENT CORPORATION

BY: _____

Title: Executive Director

Date: _____

Name and Address for Purposes of Notice:

Executive Director
TechShare Local Government Corporation
500 W. 13th Street
Austin, TX 78701

TechShare.Mental Health Alert System

Attachment A

STATEMENT OF WORK

TARRANT COUNTY

Introduction

This document outlines the mutual understanding between TechShare LGC and Tarrant County regarding the scope, objectives, and deliverables of the TechShare.Mental Health Alert System Development and Implementation Project. The purpose of this SOW is to ensure clarity, alignment, and accountability throughout the project lifecycle, enabling both parties to effectively collaborate towards successful outcomes. By detailing the project's goals, milestones, timelines, and responsibilities, this document serves as a roadmap for execution and evaluation.

Throughout this SOW, you will find a comprehensive overview of the project's scope, including specific tasks, deliverables, acceptance criteria, and any relevant assumptions or constraints. Additionally, we have outlined the roles and responsibilities of each party involved, ensuring clear communication channels and accountability at every stage.

Our mutual commitment to transparency, communication, and excellence will be instrumental in achieving the desired results outlined in this document. We look forward to a productive partnership and the successful execution of the development and implementation of TechShare.Mental Health Alert System.

Scope of Work

Article 16.22 of the CCP prescribes the procedures for early identification of individuals suspected of having a mental illness or intellectual disability. The law requires magistrates to order an interview and 16.22 report regarding the individual if the magistrate has reasonable cause to believe the individual has a mental illness or is a person with an intellectual disability. Magistrates are also required to give notice of the report to several parties to ensure early identification and treatment.

The primary objective of this effort is to develop a comprehensive and integrated software solution within the existing TechShare Suite that ensures Tarrant County's compliance with the Criminal Code of Procedures (CCP) 16.22. In addition, the software will be designed to facilitate the efficient and effective management of mental health procedures within the criminal justice system. TechShare.Mental Health Alert System will provide a streamlined process for mental health recommendations on assessments, reports, and notices, ensuring that all procedures align with the stipulations of CCP 16.22 and 17.032.

Objectives

- The primary objective of this effort is to develop a comprehensive and integrated software solution within the existing TechShare Suite that ensures Tarrant County's compliance with the Criminal Code of Procedures (CCP) 16.22.
- Facilitate the efficient and effective management of mental health procedures within the criminal justice system.
- Provide a streamlined process for mental health recommendations on assessments, reports, and notices.
- Ensure that all procedures are in alignment with the stipulations of CCP 16.22 and 17.032.

Software Requirements

The following table lists the identified software requirements for this project:

ID	Requirement
FR001	<p>The solution must include a feature that provides a robust Search capability. This feature should allow users to look up individuals based on various criteria, enhancing the efficiency and effectiveness of referral management. The search criteria should include, but not be limited to, the following:</p> <ul style="list-style-type: none">a. CID: The unique identifier for the individual.b. First, Middle, and Last Name: The full name of the individual.c. Status: The status of the individual's referral.d. Court: The court handling the individual's case.e. Date Range: A specific range of dates relevant to the individual's referral.f. Offense Type: The type of offense committed by the individual, categorized as either a felony or a misdemeanor. <p>The search feature should support complex queries, allowing users to combine multiple criteria for more refined results. It should also provide quick and accurate results, ensuring that users can find the information they need without unnecessary delay</p>
FR002	<p>The solution must incorporate a Time Tracking Feature that adheres to the following criteria:</p> <ul style="list-style-type: none">a. Accurate Time Tracking: The feature must accurately track the duration from the moment an order is issued and signed by the Magistrate or District Judge, until MHMR completes an interview and the 16.22 report.b. Task-Specific Countdown: The feature should compute the remaining time for each task and prominently display it on the respective queues.c. Task-Specific Timeframes: The feature must adhere to the following timeframes:d. Individuals in custody: MHMR has 96 hours to conduct the interview and complete the 16.22 report.e. Individuals out of custody: MHMR has 30 days to conduct the interview and complete the 16.22 report.f. Precision and Reliability: The time tracking feature must be precise and reliable to ensure all stakeholders have a clear understanding of the timelines involved.g. Configurable Settings: The feature should support configurable settings to accommodate different timeframes for different tasks.h. Alerts and Notifications: The solution must provide alerts or notifications as deadlines approach, assisting in efficient workflow management and timely completion of tasks. <p>This requirement ensures that the solution aids in efficient workflow management and timely completion of tasks, while providing clear visibility of task timelines to all stakeholders</p>

TechShare.Mental Health Alert System

Attachment A

STATEMENT OF WORK

TARRANTCOUNTY

ID	Requirement
FR003	<p>The Search Results interface must be designed to display the following columns:</p> <ul style="list-style-type: none">a. CID: A unique identifier for each record.b. Name: The name associated with each record.c. Court: The court involved in each case.d. Notification Status: The current status of the notification for each referral/order.e. Notification Status Date and Time: The date and time when the notification status was last updated.f. Order Attachment: An attachment containing the order details for each CID/referral.g. 16.22 Report Results Attachment: An attachment containing the results of the 16.22 report for each CID/referral from MHMR.h. Search Details: an expandable link that when clicked displays the summary of the progress of the referral including Notification Information, Other Bookings/Case Information, MHMR Results Information and Recommended Treatment. <p>This requirement ensures that users have access to comprehensive and relevant information for each case in the search results.</p>
FR004	<p>The solution must incorporate a feature that provides a link to the Search Details page from the Search Results and queues. On this page, a summary of the referral/CID information must be displayed. Additionally, the solution must support the functionality to export and print this summary in both Excel and PDF formats. Here's an example the summary from the current MHMR Alert System application: This requirement ensures that users can easily access, export, and print critical referral/CID information as needed.</p>
FR005	<p>The solution must include a feature that allows for the configuration of various statuses to track the progress of a workflow. These statuses should reflect the following stages:</p> <ul style="list-style-type: none">a. New: This status is assigned when a CID is received from the jail staff.b. Under Review: This status indicates that the supporting documentation is currently being reviewed by the Magistrate or District Judge.c. Issued: This status is assigned when an order for an interview and a 16.22 report has been issued.d. Denial: This status is assigned when an order has not been issued and the request for the interview and 16.22 report has been determined unnecessary by the Magistrate/District Judge.e. Not Required: This status is assigned when an order is not required because a 16.22 report has been completed in the last 12 months.f. In Progress: This status indicates that MHMR is currently working on the interview and producing the 16.22 report.g. Completed: This status is assigned when MHMR has completed the interview and produced the 16.22 report.h. Cancelled: This status is assigned when a previously issued order was withdrawn or cancelled per the request of the Magistrate or District Judge. <p>Each status should be easily configurable to allow for adjustments as the workflow evolves. The solution should also provide clear visibility of these statuses to relevant stakeholders for efficient tracking and management.</p>

TechShare.Mental Health Alert System

Attachment A

STATEMENT OF WORK

TARRANTCOUNTY

ID	Requirement
FR006	<p>The solution must include a feature that allows for the configuration of various user roles, each with distinct permissions and access levels. These roles should include the following:</p> <ul style="list-style-type: none">a. Administrator: This role should have full access to all features and settings, including user management and system configuration.b. District Judge: This role should have access to review and approve documentation, issue orders, and view case progress.c. Magistrate: This role should have similar access as the District Judge but within their jurisdiction.d. Court Coordinator: This role should have access to schedule and manage court proceedings, and coordinate with other roles.e. Magistrate Support Officer (MSO): This role should have access to assist the Magistrate in reviewing documentation and managing cases.f. MHMR Staff: This role should have access to conduct interviews, produce reports, and update case progress.g. View Only: This role should have read-only access to view case progress and reports. <p>Each role should be easily configurable to allow for adjustments as the system evolves. The solution should also provide clear visibility of these roles to relevant stakeholders for efficient tracking and management.</p>
FR007	<p>The solution must include a feature that provides configurable queues, also known as work lists, for Magistrates, District Judges and MHMR staff. These queues should contain comprehensive information about individuals suspected of having a mental illness or intellectual disability, as provided by the Jail Staff. The information in these queues should include, but not be limited to, the following:</p> <ul style="list-style-type: none">a. CID: The unique identifier for the individual.b. Name: The full name of the individual.c. List of Booking Number(s): All relevant booking numbers associated with the individual.d. CID Custody Status: The current custody status of the individual.e. Case Number(s): The case number(s), whether filed or unfiled, when available.f. List of Offense(s): A comprehensive list of offenses associated with the individual.g. Capital Murder Offense Alert/Indicator: An alert or indicator when one or more offenses associated with the CID are identified as capital murder offenses.h. Court: The court handling the individual's case, when available.i. Commitment Category: The category of commitment for the individual.j. Attachments: Any supporting documentation related to the individual's case. <p>The solution should ensure that these queues are easily accessible and manageable by the Magistrates, District Judges and MHMR staff. It should also provide the ability to update the status of each individual (i.e., CID) in the queue as their case progresses</p>
FR008	<p>The solution must include a feature that allows users to design and implement customizable web-based forms. This feature should support various form fields, validation rules, and user interactions. The solution must have the capability to generate comprehensive documents based on the data collected through these forms. The document generation process should be automated and support multiple formats for user convenience.</p>

TechShare.Mental Health Alert System

Attachment A

STATEMENT OF WORK

TARRANTCOUNTY

ID	Requirement
FR009	<p>The solution shall be capable of delivering, through an integrated system, the Order (attachment) from the Magistrate/District Judge and the 16.22 Report Results from MHMR to the following stakeholders:</p> <ul style="list-style-type: none">a. Magistrate Clerk: The solution must deliver the Order and 16.22 Report to the Magistrate Queue for all unfiled offenses in TechShare Court.b. District Clerk: The solution must deliver the Order and 16.22 Report to the Clerk Queue for filed felony offenses in TechShare Court.c. County Clerk: The solution must deliver the Order and 16.22 Report to the Clerk Queue for filed misdemeanor offenses in TechShare Court.d. Sheriff: The solution must deliver the Order and 16.22 Report to the CID Book-In Files for all offenses in TechShare Jail.e. Prosecutor: The solution must deliver the Order and 16.22 Report to the Incident/Case Evidence for all offenses in TechShare Prosecutor. <p>This requirement ensures that all relevant stakeholders receive the necessary documents in a timely and organized manner, facilitating efficient case management and legal proceedings.</p>
FR010	<p>The solution must have capable of generating an automated email to deliver the Order & 16.22 Report Results from MHMR to the following stakeholders:</p> <ul style="list-style-type: none">a. Defense Counsel Email Inboxb. CSCD Email Inbox: If the individual has been released on bond (not in custody).
FR011	<p>The solution should provide an efficient and user-friendly interface that enables the Magistrate or District Judge to swiftly access the supporting documents related to the mental health or intellectual disability status of the individual under consideration as well as any previous reports completed in the last 12 months.</p>
FR012	<p>The solution should facilitate a swift and straightforward process for generating an ORDER that requests an interview and a 16.22 report. It should also accommodate electronic signatures and possess the capability to efficiently route or transmit the signed order to the relevant parties.</p> <p>Sample Order:</p>
FR013	<p>The solution should facilitate a swift and straightforward process for generating an order to NOT REQUIRE an interview and a 16.22 report. It should also accommodate electronic signatures and possess the capability to efficiently route or transmit the signed order to the relevant parties.</p> <p>Sample Order:</p>
FR014	<p>The solution should facilitate a swift and straightforward process for generating an order finding no reasonable cause (i.e., DENYING) an interview and a 16.22 report. It should also accommodate electronic signatures and possess the capability to efficiently route or transmit the signed order to the relevant parties.</p>
FR015	<p>The solution should enable Magistrates and District Judges to initiate the cancellation of previously issued orders. Upon such a request, the system must update to reflect the cancellation and dispatch notifications to all relevant parties.</p>
FR016	<p>The solution must provide a Case Assessment web-based form/page for MHMR to enter the results from the interview and 16.22 report. Below is an example of the input fields we have available today:</p>

TechShare.Mental Health Alert System

Attachment A

STATEMENT OF WORK

TARRANTCOUNTY

ID	Requirement
FR017	The solution must incorporate a feature that enables users to authenticate documents using electronic signatures. This feature should be versatile, allowing users to create electronic signatures both directly on the platform and using an external signature pad. The electronic signature process should be secure, user friendly, and comply with relevant legal standards. Furthermore, the solution should support the storage and management of these electronic signatures for future use
FR018	<p>The solution must include a feature that provides a comprehensive dashboard. This dashboard should display real-time status updates for each individual (i.e., CID) referred by the Jail Staff. The statuses should</p> <p>reflect the progress of each order, including those that are new, issued, denied, not required, cancelled, in progress, and completed. In addition, the dashboard is required to present a comparative analysis of the number of capital murder offenses against all other types of offenses. It should also differentiate and display the count of misdemeanor offenses in contrast to felony offenses.</p> <p>The dashboard should be user-friendly and intuitive, allowing users to easily navigate and understand the status of each individual case. It should also provide filtering and sorting capabilities to manage and prioritize the cases effectively. Furthermore, the dashboard should support customizable views to cater to the specific needs of different user roles.</p> <p>The solution should ensure that the data displayed on the dashboard is accurate and up to date, reflecting the real-time status of each individual case. It should also provide clear visibility of these statuses to relevant stakeholders for efficient tracking and management.</p>
DR001	Data stored in the current application for the last 24 months must be extracted, cleaned, and migrated into the new solution.
TR001	All production data should be hosted in a government cloud certified environment in compliance with the International Traffic in Arms Regulations (ITAR), the Federal Risk and Authorization Management Program (FedRAMP), the Federal Information Security Management Act (FISMA), Criminal Justice Information Services (CJIS), and the Health Insurance and Accountability Act (HIPAA).
TR002	The proposed solution must support the Role Based Access Control (RBAC).
TR003	The solution MUST be compatible with Tarrant County-preferred Internet browsers (Microsoft Edge, Chrome Enterprise, and/or Mozilla Firefox Extended Support Release) with minimal or no loss of functionality based on browser selected, when applicable.
TR004	The solution should be able to integrate with TechShare Jail, TechShare Court, and TechShare Magistrations portal.
TR005	The MHMR application must support anytime, anywhere access to stored content. This includes strong encryption of data traffic while in transit and at rest, for sensitive data, when applicable.
TR006	The solution should support County user single sign-on (SSO) capability facilitated through a hosted government cloud-certified environment.
TR007	The solution must ensure that any data transmitted beyond the confines of the physically secure location is immediately safeguarded through encryption. Specifically, Criminal Justice Information (CJI) should be encrypted using a cryptographic module that complies with FIPS 140-2 standards and employs a symmetric cipher with a minimum key strength of 128 bits

TechShare.Mental Health Alert System

Attachment A

STATEMENT OF WORK

TARRANTCOUNTY

ID	Requirement
TR008	The solution must ensure that any data at rest (i.e., stored digitally) outside the confines of the physically secure location is safeguarded through encryption. Specifically, Criminal Justice Information (CJI) at rest should be encrypted either by adhering to the standards used for CJI in transit or by employing a symmetric cipher that complies with FIPS 197 certification (AES) and has a minimum key strength of 256 bits.
TR009	The storage of CJI should only be permitted in cloud environments (e.g., government or third party/commercial datacenters, etc.) which reside within the physical boundaries of the U.S., U.S. territories, Indian Tribes, and Canada and legal authority of U.S. federal/state/territory agencies, Indian Tribe agencies, or the Royal Canadian Mounted Police (RCMP).
TR010	The solution must ensure that metadata derived from unencrypted Criminal Justice Information (CJI) is protected with the same level of security as CJI itself. Furthermore, this metadata must not be utilized for advertising or any other commercial activities by any cloud service provider or associated entity
TR011	Cloud service providers must be able to demonstrate security assurances through recognized authorizations such as FedRAMP, StateRAMP, SOC Type 2, or equivalent certifications.
TR012	TechShare must provide onsite “train the trainer” and/or remote end-user training options
IR001	The solution must seamlessly integrate with the existing TechShare suite, including: a. TechShare Jail b. TechShare Court c. TechShare Magistration d. TechShare Prosecutors
IR002	The solution must facilitate bi-directional data exchange with the TechShare suite: Outbound Data: a. Orders generated by the solution shall be transmitted to the relevant TechShare application (Jail, Court, Magistration, or Prosecutors) in real-time or near real-time. b. 16.22 reports generated by the solution shall be transmitted to the appropriate TechShare application for storage and retrieval. Inbound Data: a. The solution shall be able to retrieve relevant data from the TechShare suite to support its functionalities.
IR003	The integration must be designed to handle the expected data volume and transaction frequency without compromising performance or system stability. The solution shall be scalable to accommodate future growth in data and user activity.
IR004	The solution vendor must provide comprehensive documentation for the integration process, including API specifications, data formats, and testing procedures. Ongoing support for integration troubleshooting and maintenance must be available
RR001	The solution should be capable of generating a comprehensive report that includes the number of referrals from the jail, the count of orders issued, denied, and not required, along with the status of each referral. This report should be customizable based on a specified date range.
DR001	The system should securely migrate the cleaned data to the designated target location, ensuring no loss or corruption of data during the process.
DR002	The system should have the capability to accurately identify and segregate data that is older than a 2-year threshold from the specified sources and archive it.

TechShare.Mental Health Alert System

Attachment A

STATEMENT OF WORK

TARRANTCOUNTY

ID	Requirement
DR003	The system should securely archive the identified data, ensuring its integrity and accessibility for future audit and historical reference purposes. The archived data should be stored in a manner that allows for efficient retrieval when required.

Quality Assurance Standards

Below describes the quality assurance services to be provided by the TechShare team to ensure the delivery of high-quality software which meets user expectations and performance requirements.

1. **Test Plan** Development of a comprehensive test plan and strategy which outlines the approach, scope, objectives, and resources for testing activities throughout the software development lifecycle.
2. **Development Testing** employed within the development team, TechShare utilizes unit testing and peer reviews to ensure the developed software has the quality, maintainability, and adherence to standards.
3. **Internal Quality Assurance** testing of the feature upon incorporation into a new build.
4. **Product Owner** testing as new builds are deployed to the project environment.
5. **Acceptance Testing** to validate the software meets the acceptance criteria defined by stakeholders and fulfills the business requirements to go live on the software.

Timeline/Schedule

The projected timeline for this project spans six (6) months. Specific tasks and their corresponding milestones are detailed in the table provided below, aligning with the established period for project completion. There are no anticipated adjustments to the time for this effort.

Task	1	2	3	4	5	6
	Kick Off	Develop	Develop	Develop & Test	Test & Train	Train & Go Live
Validate Requirements						
Status Reports						
Development						
Environment and Application Configuration						
Data Migration						
Test Plan						
Implementation Initiation						
Training Plan						

TechShare.Mental Health Alert System

Attachment A

STATEMENT OF WORK

TARRANTCOUNTY

Task	1	2	3	4	5	6
	Kick Off	Develop	Develop	Develop & Test	Test & Train	Train & Go Live
User Acceptance Testing						
Training						
Go Live						

Roles and Responsibilities

The below **RACI** chart provides clarity on who is **Responsible**, **Accountable**, **Consulted** and **Informed** for each task within this Statement of Work.

Project Task	TS Product Manager	TS Sr. Business Analyst	TS Developer	TS DBA	TS QA	TC Business Product Owner	TC Stakeholder	TC ITD
Product Management Services	R	I	I	I	I	I	I	I
Validate Requirements	R	A	I	I	I	C	I	I
Design and Architecture	R	I	A	I	I	I	I	I
Development	R	C	A	I	I	I	I	I
Data Conversion	R	C	I	A	I	I	I	I
Configuration	R	A	C	C	I	I	I	C
Testing/QA	R	I	I	I	A	A	I	I
Deployment	A	I	I	I	I	I	I	R
Release Notes	R	R	I	I	I	I	I	I
Sprint Review	R	A	A	A	A	I	I	I
Change Management	R	I	I	I	I	I	A	A
Communication and Reporting	R/A	I	I	I	I	I	I	I
Test Plan	R	A	I	I	A	I	I	I
Training Plan	R	A	I	I	A	A	I	I

TechShare.Mental Health Alert System

Attachment A

STATEMENT OF WORK

TARRANTCOUNTY

Project Task	TS Product Manager	TS Sr. Business Analyst	TS Developer	TS DBA	TS QA	TC Business Product Owner	TC Stakeholder	TC ITD
Implementation Plan	R	I	I	I	I	I	I	I
Implementation Readiness Sign Off	I	I	I	I	I	A	R	I
Go Live Sign Off	I	I	I	I	I	A	R	I
Knowledge Transfer	R	A	A	A	C	I	I	A
Post Go Live Activities	R	A	A	A	A	A	I	A

Change Management Process

By following a structured change management process, software development projects can effectively manage changes while minimizing disruptions and maintaining alignment with project goals. While there are no changes to the scope of work or timeline for this effort envisioned, should there be any, they will be managed collaboratively by TechShare and Tarrant County to develop a Change Request for review and approval by Stakeholders in advance of deviating from the original scope or timeline of this project.

Assumptions and Constraints

1. The Mental Health Alert System will be developed as a standalone TechShare application.
2. Development, Project Management, and Implementation Services are provided by TechShare.
3. Development meetings will be conducted by TechShare with designated Tarrant County business team members to complete development of the MHMR system (on-site and remote.)
4. TechShare will provide application configuration services of the application in the Tarrant County environment.
5. TechShare will coordinate quality assurance and user acceptance testing activities.
6. Training will be provided by TechShare with options for in-person and remote sessions.
7. TechShare will provide transition information for Tarrant County including a review of the architecture with Tarrant County and a knowledge transfer session on how to access any artifacts of the project.

TechShare.Mental Health Alert System

Attachment A

STATEMENT OF WORK

TARRANTCOUNTY

Acceptance Criteria

1. The system meets all functional requirements outlined in the project scope.
2. The system meets all non-functional requirements such as performance, reliability, security, usability, and scalability. This includes adequate response time, system up time, data security, and the user experience.
3. Historical data as specified in the Scope of Work has been migrated and is available in the system.
4. System integration with TechShare.Jail, TechShare.Court, TechShare.Magistration and TechShare.Prosecutor is complete.
5. Documentation for training and use of the system.
6. Documentation for technical support of the System.

Deliverables

1. Weekly Status Report to include project updates, metrics regarding development, and implementation progress, costs, issues & risks, action Items, upcoming milestones, dependencies, and overall project health.
2. Working Software based on the requirements described in the Scope of Work
3. Training Materials for Train the Trainer Sessions.
4. Train the Trainer Sessions.
5. Test Plan for User Acceptance Testing.
6. Facilitation of User Acceptance Testing.
7. Technical Training for Tarrant County ITD and access to project artifacts for the development of the system.

Payment Terms

The total cost of this effort is \$172,500. The following describes the payment terms including the amount due based on the identified milestones:

No	Milestone	Amount	Payment Term
1	Development of TechShare.Mental Health Alert System	\$103,500	Sixty percent (60%) due upon signing of agreement and in advance of starting the project
2	Implementation of TechShare.Mental Health Alert System	\$51,750	Thirty percent (30%) due upon sign off for Implementation Readiness
3	Go Live Services	\$17,250.	Ten percent (10%) due upon a go decision to proceed with go live of the system

Attachment B
FEDERAL BUREAU OF INVESTIGATION CRIMINAL
JUSTICE INFORMATION SERVICES SECURITY
ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

- 1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.
- 1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

- 2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes.

3.00 Responsibilities of the Contractor.

- 3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

- 4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

- 4.02 Security violations can justify termination of the appended agreement.
- 4.03 Upon notification, the FBI reserves the right to:
- a. Investigate or decline to investigate any report of unauthorized use;
 - b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CJA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

- 5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

- 6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.
- 6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.
- 6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.
- 6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.
- 6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director
Criminal Justice Information Services Division,
FBI 1000 Custer Hollow Road
Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Contractor

TechShare Local Government Corporation

Signature of Contract Representative

Date

G.K. Maenius, Executive Director

Printed Name and Title