USER AGREEMENT TO PURCHASE DRIVER RECORDS OR DRIVER RECORD MONITORING SERVICES

This Agreement is made between the Department of Public Safety of the State of Texas (DPS), the state administrator for driver license and identification card records (referred to as Driver Records), and the entity purchasing records identified below (Entity).

Entity Name: Fort Bend County

Address: 301 Jackson Street, Ste. 224, Richmond, TX 77469

BACKGROUND

Texas law authorizes DPS to sell Driver Records individually or in bulk for specified permissible purposes and to establish an Interactive System to provide the release of Driver Records under the authority of Texas Transportation Code Chapters 521 and 730.

Additionally, Texas Transportation Code § 521.062 allows DPS to establish an optional program for Driver Records Monitoring Services (referred to as Monitoring Services) that will notify any participating entities of any updates or changes to an individual's Driver Record that is being monitored by any entity that elects to participate in the program. These changes may include convictions for a traffic offense or any driver license status change.

Texas law requires each prospective Entity using the Interactive System to sign an agreement with DPS containing safeguards that DPS considers necessary to ensure that Driver Records purchased are used only for permissible purposes and that the rights of the individuals and DPS are protected before Entity receives any Driver Records.

DPS will sell and deliver the Driver Records or Monitoring Services in an interactive format to Entity subject to the following terms and conditions.

SCOPE

1. **Definitions**
   a. **Driver Records** means a record that pertains to a motor vehicle operator or driver license or permit, or identification document issued by DPS for all license holders in Texas as described in Texas Transportation Code § 521.050.

   b. **Interactive System** means the process by which DPS supplies Driver Records and Monitoring Services in an electronic format to Entity, including real-time and batch web-based applications.

c. Personal Information means information within Driver Records that identifies an individual by the following: an individual's photograph or computerized image, Social Security number, date of birth, driver identification number, name, address but not zip code, email address, telephone number, and medical or disability information or as is defined by the federal Driver's Privacy Protection Act(18 U.S.C. § 2721, *et seq.*), the Identity Theft Enforcement and Protection Act (Texas Business and Commerce Code Ch. 521), and the Texas Motor Vehicle Records Disclosure Act (Texas Transportation Code Ch. 730). Personal Information may also include sensitive personal information as defined in Texas Business and Commerce Code § 521.002(2), which includes:

1) An individual's first name or first initial and last name in combination with a driver license number or government-issued identification number if the name and the items are not encrypted.
2) Information that identifies an individual and relates to:
   a) The physical or mental health or condition of the individual; or
   b) The provision of health care to the individual.

d. Entity means a person or governmental or private entity who is eligible to receive Driver Records as an Authorized Recipient under Texas Transportation Code Chapter 730.

e. Breach of System Security means the unauthorized access of computerized data that compromises the security, confidentiality, or integrity of personal information Entity maintains under this Agreement, including data that is encrypted if Entity's employee or agent accessing the data has the key required to decrypt the data. Good faith acquisition of personal information by an employee, agent, or client of Entity for the purposes of performing under this Agreement is not a breach of system security unless the employee, agent, or client of Entity uses or discloses the personal information in an unauthorized manner.

f. Confidential Data means information as defined in Texas Administration Code § 202.1 (5) that is collected and maintained by the Department that must be protected against unauthorized disclosure and is not subject to public disclosure under the provisions of applicable state or federal law or other legal agreements.

g. Cyber Security means the Department's Cyber Security Unit, which is responsible for agency information technology security.

h. **Department or DPS** means the Department of Public Safety of the State of Texas.

i. **Regulated Data** means information that is collected and maintained by the Department that requires the Department to implement specific privacy and security safeguards as mandated by Federal and State law.

j. **Secure Location** means a facility, conveyance, or area with security controls sufficient to protect sensitive or confidential information and associated information systems.

k. **Sensitive Data** means information that is collected and maintained by the Department that must be protected against unauthorized disclosure, except for public release under the provisions of applicable state or federal law or other legal agreements.

l. **System Failure** means a breakdown of any system hardware, operating system, or application software which prevents the accomplishment of the system's intended function.

m. **User(s)** means an entity/person who is accessing Driver Records from a web-based, desktop, or mobile device interface.

n. **Wireless Local Area Network** (WLAN) means a wireless computer network that links two or more devices using a wireless distribution method within a limited area.

2. Purchase of Driver Records

Entity may purchase Driver Records of individuals, which includes Personal Information, solely for a permissible use as identified in the section of this Agreement entitled "Certification of Permissible Use."

3. Purchase of Monitoring Services

Upon enrollment in the Driver Record Monitoring Service, Entity agrees to immediately purchase a record of any driver identified with a "not eligible" status (Type 2). If the purchase is made for the purpose of insurability, the driver is eligible for monitoring by the organization that purchased the record. The Monitoring Services will include notification to Entity on a bi-weekly basis of any change in the individual's driver license status or when any conviction for a traffic offense is reported to DPS during the term of this Agreement.

4. Fees

Entity must pay to DPS the applicable fee set by statute or rule for purchasing Driver Records or Monitoring Services. Entity also must pay any interactive transaction fees. Payment for the interactive transfer must be handled in an electronic format. Entity must remit payment immediately upon receipt of billing. Failure to remit timely payment may result in termination of this Agreement, denial of additional Driver Records and Monitoring Services, or the cancellation of Monitoring Services for any specific Driver Record until all payments are received. In the event that the Monitoring Services for a specific Driver Record is cancelled, Entity must purchase the Driver Record again in order to reinitiate the monitoring service for that specific Driver Record.

Under Tex. Transp. Code § 521.049, DPS will not charge a fee for Driver Records disclosed to a law enforcement or other governmental agency for an official purpose, unless the governmental agency requests Driver Records sold in bulk for research purposes. If Entity is a governmental agency and wishes to obtain Driver Records in bulk for research purposes, DPS will charge Entity the regular fees for those bulk Driver Records.

If Entity is monitoring a Driver Record for multiple Third Party Requestors, Entity must pay a monitoring fee for each Third Party Requestor. Entity must require a Third Party Requestor to monitor its entire customer base for Monitoring Services.

If Entity is purchasing Driver Records and Monitoring Services for its own use and will not provide to a Third Party Requestor as permitted herein, Entity must monitor its entire customer base under this Agreement.

5. Interactive System

The Interactive System for Driver Records and Monitoring Services, by which DPS supplies Driver Records and Monitoring Services in an electronic format including real-time and batch web-based applications, is operated and controlled by a State of Texas vendor. The vendor is the duly authorized service agent of DPS responsible for processing electronically submitted Driver Records requests and delivering Driver Records and Monitoring Services in the form of a report identifying changes in an individual's driver license status or when any conviction for a traffic offense is reported in a secure, electronic format using the Interactive System. Billing and payment for these services by Entity will also be conducted through the Interactive System. The vendor is obligated to specific performance level requirements, so the vendor has the authority to suspend any Entity account or access to the Interactive System when an Entity's access compromises the operation of the Interactive System. Suspension of such account or access will continue until the compromising condition is resolved to the satisfaction of DPS.

6. Certification of Permissible Use

Entity, by signing this Agreement, certifies compliance with all provisions of the federal Driver's Privacy Protection Act, the Texas Motor Vehicle Records Disclosure Act, the Identity Theft Enforcement and Protection Act, and with all other state and federal laws applicable to this Agreement. Entity certifies that its use of Driver Records purchased under this Agreement is for the following permissible purpose only and for no others.

Initial all that apply.

_____ 1. (Valid for Certified Abstract) For use by a government agency in carrying out its functions or a private entity acting on behalf of a government agency in carrying out its functions.

_____ 2. For use in connection with a matter of (a) motor vehicle or motor vehicle operator safety; (b) motor vehicle theft; (c); motor vehicle product alterations, recalls, or advisories; (d) performance monitoring of motor vehicles, motor vehicle parts, or

motor vehicle dealers; or (e) removal of nonowner records from the original owner records of motor vehicle manufacturers.

_____ 3. For use in the normal course of business by a legitimate business or an authorized agent of the business, but only (a) to verify the accuracy of personal information submitted by the individual to the business or the agent of the business; and (b) if the information is not correct, to obtain the correct information, for the sole purpose of preventing fraud by, pursuing a legal remedy against, or recovering on a debt or security interest against the individual.

_____ 4. (Valid for Certified Abstract) For use in conjunction with a civil, criminal, administrative, or arbitral proceeding in any court or government agency or before any self-regulatory body, including service of process, investigation in anticipation of litigation, execution or enforcement of a judgment or order, or under an order of any court.

_____ 5. For use in research or in producing statistical reports, but only if the personal information is not published, redisclosed, or used to contact any individual.

X
_____ 6. For use by an insurer, insurance support organization, or self-insured entity, or an authorized agent of an insurer, insurance support organization, or self-insured entity, in connection with claims processing or investigation activities, antifraud activities, rating or underwriting.

_____ 7. For use in providing notice to an owner of a vehicle that was towed or impounded and is in the possession of a storage facility.

_____ 8. For use by a licensed private investigator agency or licensed security service for a purpose permitted under this section.

X
_____ 9. (Valid for Certified Abstract) For use by an employer or an agent or insurer of the employer to obtain or verify information relating to a holder of a commercial driver's license that is required under 49 U.S.C. Chapter 313.

_____10. For use in connection with the operation of a toll transportation facility or another type of transportation project described by Section 370.003.

_____ 11. For use by a consumer reporting agency, as defined by the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.), for a purpose permitted under that Act.

_____12. For use by a motor vehicle manufacturer, dealership, or distributor, or an agent of or provider of services to a motor vehicle manufacturer, dealership, or distributor, for motor vehicle market research activities, including survey research.

_____13. For use in the ordinary course of business by a person or authorized agent of a person who: (a) holds a salvage vehicle dealer license issued under chapter 2302, Occupations Code; (b) holds an independent motor vehicle dealer or wholesale motor vehicle auction general distinguishing number issued under Chapter 503 of this code; (c) holds a used automotive parts recycler license issued under Chapter 2309, Occupations Code; or (d) is licensed by, registered with, or subject to regulatory oversight by the

Texas Department of Motor Vehicles, the Texas Department of Banking, the Department of Savings and Mortgage Lending, the Credit Union Department, the Office of Consumer Credit Commissioner, the Texas Department of Insurance, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Consumer Financial Protection Bureau, or the National Credit Union Administration.

_____14. For use by an employer, principal, general contractor, nonprofit organization, charitable organization, or religious institution to obtain or verify information relating to a person who holds a driver's license or the driving history of a person who holds a driver's license if the person is employed by, works under a contract with, or volunteers for the employer, principal, contractor, organization, or institution.

_____15. For use in the preventing, detecting, or protecting against identity theft or other acts of fraud. Prior to release of personal information may require additional information.

Entity must restrict access to, use of, and disclosure of Driver Records, including Personal Information, to designated personnel solely for the permissible purposes identified in this Agreement. Access to and use of Driver Records by Entity's personnel that are not authorized is strictly prohibited. Entity must comply with the Data Sharing Agreement (Attachment C) that is incorporated into this Agreement by reference. The Rules of Behavior for Individuals Accessing DPS Data (Attachment B) must be completed by the Entity's employees accessing Driver Records. Any access, use, or disclosure not required for the purposes of this Agreement or for any unofficial purpose are strictly prohibited. Violation of the federal Driver's Privacy Protection Act or the Texas Motor Vehicle Records Disclosure Act may result in civil and criminal penalties.

7. Resell or Re-disclosure

Entity may not resell re-disclose Driver Records obtained under this Agreement except as specifically provided in this Agreement. Entity may re-disclose Driver Records to a third party requestor (Third Party Requestor) who is an Authorized Recipient and only if Entity enters into a written contract with a Third Party Requestor that requires a Third Party Requestor's compliance with all Agreement requirements, including compliance with the federal Driver's Privacy Protection Act, the Identity Theft Enforcement and Protection Act, and the Texas Motor Vehicle Records Disclosure Act, andthat is for a use authorized by Texas Transportation Code § 730.007. If Driver Records are disclosed as part of Monitoring Services, Entity must require a Third Party Requestor to monitor its entire customer base for Monitoring Services. Any Driver Records or Monitoring Services purchased under this Agreement by Entity are for a single purpose use only and will not be repurposed or used more than one time. Entity will not use a specific Driver Record for multiple Third Party Requestors or multiple uses by a single Third Party Requestor.

If Entity resells or re-discloses Driver Records to someone who is not an Authorized Recipient, the Entity may be subject to civil and criminal penalties, including a civil suit that allows for damages or subject to committing an offense classified as a misdemeanor punishable by a fine not to exceed $100,000. If Entity resells or re-discloses Driver Records to Third Party Requestors, it must inform Third Party Requestors that they may not redisclose the personal information to a person who is not an Authorized Recipient.

8. Record Creation and Retention

Entity must create a record identifying each Third Party Requestor that obtained Driver Records or Monitoring Services (if applicable) from Entity and the legally permissible purpose for which Driver Records or Monitoring Services were obtained. Entity must ensure that each Third Party Requestor will comply with all federal and state laws on the release of the information and all terms, conditions, and obligations of this Agreement. Entity must retain these identifying records for five years following the transfer of any Driver Records or Monitoring Services to a Third Party Requestor of the following: the name of any person or entity to whom the release was made; the date the release was made; the permitted use for which Driver Records or Monitoring Services were released; the written agreement with the Third Party Requestor; and contact information for the Third Party Requestor.

9. Provide Copies of Records and Notification of Release

If Entity re-discloses any Driver Records obtained under this Agreement to a Third Party Requestor, Entity must provide access to or copies of those records required in the section entitled "Record Creation and Retention" to DPS immediately upon DPS's request. DPS retains the right to require the records in any applicable format, including electronic or paper. Entity will bear the expense of providing this information to DPS, including any postage or shipping charges.

10. Unauthorized Disclosure

Entity must immediately notify DPS of any inadvertent or unauthorized release, disclosure, breach, or compromise of Driver Records obtained under this Agreement as soon as Entity knows or should have known of such unauthorized or inadvertent release, disclosure, breach, or compromise of security. This obligation applies whether the action or omission was by Entity, its employees or agents, or by any person or entity that acquired Driver Records from Entity, either directly or indirectly.

If the Interactive System or an information system containing Driver Records is compromised or breached, Entity must provide notice to DPS as soon as possible following the discovery or reasonable belief that there has been unauthorized exposure, access, disclosure, compromise, or loss of sensitive or confidential information referred to as a "*Security Incident.*"

a. Within 24 hours of the discovery or reasonable belief of a Security Incident, Entity must provide a written report to DPS detailing the circumstances of the security incident, which includes at a minimum:

    1) A description of the nature of the Security Incident;
    2) The type and amount of Driver Records involved;
    3) Who may have obtained the Driver Records;
    4) What steps Entity has taken or will take to investigate the Security Incident;
    5) What steps Entity has taken or will take to mitigate any negative effect of the Security Incident; and
    6) A point of contact for additional information.

b. Each day thereafter until the investigation is complete, Entity must provide DPS with a written report regarding the status of the investigation and the following additional information as it becomes available:

1) Who is known or suspected to have gained unauthorized access to Driver Records;
2) Whether there is any knowledge if Driver Records have been abused or compromised;
3) What additional steps Entity has taken or will take to investigate the Security Incident;
4) What steps Entity has taken or will take to mitigate any negative effect of the Security Incident; and
5) What corrective action Entity has taken or will take to prevent future similar unauthorized use or disclosure.

c. Entity must confer with DPS regarding the proper course of the investigation and risk mitigation. DPS reserves the right to conduct an independent investigation of any Security Incident, and should DPS choose to do so, Entity must cooperate fully by making resources, personnel, and systems access available to DPS and its authorized representatives.

d. Subject to review and approval by DPS, Entity must at its own cost, provide notice that satisfies the requirements of Texas Business and Commerce Code Ch. 521 to individuals whose personal, confidential, or privileged information were compromised or likely compromised as a result of the Security Incident. If DPS, in its sole discretion, elects to send its own separate notice, then all costs associated with preparing and providing notice must be reimbursed to DPS by Entity. If Entity does not reimburse such costs within 30 calendar days of DPS written request, DPS will have the right to collect such costs.

11. Deletion of Information Required if not Authorized Recipient

Entity must delete from its records any personal information received from DPS if Entity becomes aware that Entity is not an Authorized Recipient of that information.

12. Data Protection

a. Entity must further protect Driver Records in accordance with 1 Texas Administrative Code Ch. 202 and Texas Business and Commerce Code Ch. 521.

b. Entity and its employees must comply with the requirements found in Attachments B and C.

c. Personal information does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

d. Entity must implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure of any sensitive personal information collected or maintained by Entity under this Agreement.

13. No Separate Database

Entity will not retain, store, combine, or link any information from Driver Records or Monitoring Services obtained under this Agreement with any other data or database without the prior written consent of DPS.

14. Acknowledgement and Disclaimer

Entity acknowledges that DPS is furnishing Driver Records on an "as is" basis and DPS makes no representation as to the accuracy of any Driver Records furnished. DPS expressly disclaims responsibility for any failure to deliver Driver Records in a timely manner, or at all, in the event of staff shortages, failures of appropriations, breakdown of equipment, compliance with new or amended laws, acts of authority exercised by a public official, acts of God or anything that may be classified as a type of *force majeure* incident that is beyond the reasonable control of DPS and that by exercise of due foresight DPS could not reasonably have been expected to avoid, and which by the exercise of all reasonable due diligence, DPS is unable to overcome, or any other circumstances which may delay or preclude furnishing Driver Records in a timely fashion.

15. Consumer Protection

Driver Records furnished under this Agreement must not be used by Entity to engage in any method, act, or practice that is unfair or deceptive, nor will Driver Records be used for marketing, solicitations, or surveys not authorized by law, which includes any prohibition under Texas Transportation Code Chapter 730.

16. Direct Access to Driver Records

Entity may not allow any member of the public or any person outside the direct employ or control of Entity direct access to Driver Records under this Agreement for any reason other than Entity's intended and legitimate use of Driver Records.

17. Assignability

Entity will not assign, license, or transfer any of its rights, duties, and obligations under this Agreement without the prior written consent of DPS. An attempted assignment in violation of this section is null and void. Any approved assignment will not relieve the assignor of any liability or obligation under this Agreement. Alternatively, if Entity does assign without prior written approval and a novation is impractical or impossible under the circumstances, but DPS does approve the assignment ultimately, then this Agreement will be binding on any successor or assignee.

18. Change of Status

This Agreement will automatically terminate if Entity ceases to conduct business, substantially changes the nature of its business, sells its business without a proper DPS-approved assignment, is deceased, if there is a significant change in its ownership, or ceases to qualify for Driver Records and Monitoring Services under the permissible use certified in the section entitled "Certification of Permissible Use" or as otherwise provided in this Agreement. Entity, its successor in interest, or its personal representative must immediately notify DPS in writing of any change in status that may implicate this section.

19. Suspension

If DPS has a reasonable suspicion or actual confirmation that Entity is not in contract compliance with any requirement for any reason, including data spillage or data breach, DPS reserves the right to immediately suspend access to Entity. DPS may reinstate access following suspension upon DPS's receipt of satisfactory assurances that Entity has corrected all non-compliance and has taken measures to prevent future non-compliance. DPS will not provide an Entity with any changes to a monitored record that occur during a period of suspension once services are reinstated; the DPS system does not have the ability to look back at or track any changes that may have occurred during the period of suspension. Failure to correct any violations to DPS's satisfaction or repeated violations could result in contract termination and permanent cancellation.

20. Incorporation of Other Documents

This Agreement, including "Attachment A, Entity's Information Form for Obtaining Interactive Driver Records and Monitoring Services", "Attachment B, Rules of Behavior for Individuals Accessing DPS Data", "Attachment C, Data Sharing Agreement", and Attachment D, Additional Requirements for Bulk Record Purchases under Texas Transportation Code § 521.050" constitutes the entire agreement between the Parties with regard to the matters made to the subject of this Agreement and no oral agreements are binding.

21. Termination

a. **For Convenience.** Either Party may terminate this Agreement for convenience at any time for any reason by giving the other Party 30 calendar days' written notice. If a Party elects to terminate this Agreement for convenience, all unfilled obligations, including the obligation to pay any applicable fees, will remain in full force. In no event will DPS be liable in any way if it terminates for convenience.

b. **For Cause.** DPS may immediately terminate this Agreement for cause for any violation of the terms of this Agreement or for any violation of any state or federal law, rule, or regulation relating to the subject matter of this Agreement. DPS will provide Entity with written notice to terminate this Agreement, which termination will become effective immediately upon Entity's receipt of the notice. If this Agreement is terminated for cause, DPS may refuse to provide Driver Records to Entity in any format.

22. Amendments

DPS may amend the terms and conditions of this Agreement from time to time in order to accommodate changes in the records or information furnished under this Agreement and for other reasons deemed appropriate by DPS.

23. INDEMNIFICATION (Does not apply to Governmental Entities)

ENTITY MUST DEFEND, INDEMNIFY, AND HOLD HARMLESS THE STATE OF TEXAS AND DPS, AND THEIR OFFICERS, AGENTS, EMPLOYEES, REPRESENTATIVES, CONTRACTORS, ASSIGNEES, OR DESIGNEES FROM ANY AND ALL LIABILITY, ACTIONS, CLAIMS, DEMANDS, OR SUITS, AND ALL RELATED COSTS, ATTORNEY FEES, AND EXPENSES ARISING OUT OF, OR RESULTING FROM ANY ACTS OR OMISSIONS OF ENTITY OR ITS AGENTS, EMPLOYEES, OR SUBCONTRACTORS, IN THE EXECUTION OR PERFORMANCE OF THIS AGREEMENT. THE DEFENSE MUST BE COORDINATED BY

ENTITY WITH THE OFFICE OF THE TEXAS ATTORNEY GENERAL (OAG) WHEN TEXAS STATE AGENCIES ARE NAMED DEFENDANTS IN ANY LAWSUIT AND ENTITY MAY NOT AGREE TO ANY SETTLEMENT WITHOUT FIRST OBTAINING THE CONCURRENCE FROM OAG. ENTITY AND DPS AGREE TO FURNISH TIMELY WRITTEN NOTICE TO EACH OTHER OF ANY SUCH CLAIM.

24. Applicable Law and Venue

This Agreement will be governed by and construed in accordance with the laws of the State of Texas as well as any relevant federal law regarding the subject matter. The venue for any suit arising under this Agreement is fixed in any court of competent jurisdiction in Travis County, Texas.

25. Notice

Any notice required or permitted under this Agreement will be directed to the Parties at the addresses shown below. The following contact person is designated by Entity to receive all notices regarding this Agreement:

Point of Contact: Director of Risk Management - Wyatt Scott

Alternate Point of Contact: Risk and Benefits Manager - Sharon Currie

Address: 301 Jackson Street, Ste. 224

City, State, Zip Code: Richmond, TX. 77469

Telephone Number: 281-341-8630

Cell Phone Number: 281-610-3273

Fax: 281-341-3751

Email: sharon.currie@fortbendcountytx.gov

All correspondence to DPS regarding this Agreement must be mailed to the following address:

Department of Public Safety
License and Record Service/Online Services
P.O. Box 4087
Austin, Texas 78773-0360
(512) 424-5967
Fax: (512) 424-7456
Email: E.eCommerce@dps.texas.gov

Notices to the Parties at the addresses shown above will be deemed received: (i) when delivered in hand and a receipt granted; (ii) three calendar days after it is deposited in the United States mail by certified mail, return receipt requested; or (iii) when received if sent by confirmed facsimile or confirmed email. Either of the Parties may change its address or designated individual(s) to receive notices by giving the other Party written notice as provided above, specifying the new address and/or individual and the date upon which it will become effective.

26. Compliance with Law

Entity must comply with all local, state, and federal laws, rules, and regulations applicable to the subject matter of this Agreement, including but not limited to, the federal Driver's Privacy Protection Act of 1994 and the Texas Motor Vehicle Records Disclosure Act, and any written instructions of DPS related to this Agreement. Violation of the federal Driver's Privacy Protection

Act or the Texas Motor Vehicle Records Disclosure Act by Entity may result in civil and criminal penalties. Violation of a term of this Agreement by Entity may be a false, misleading, or deceptive act or practice under Subchapter E, Chapter 17, Texas Business and Commerce Code or a Class B misdemeanor under Section 521.062 of the Texas Transportation Code.

27. Office of the Attorney General

Entity understands that under Texas Transportation Code § 521.062(d–g), the Office of the Attorney General may take certain actions against Entity for violations related to this Agreement.

28. Severability

Entity acknowledges that if a dispute between the parties arises out of this Agreement or the subject matter of this Agreement, including a dispute over possibly ambiguous language, they would want the court to interpret this Agreement as follows:

28.1 With respect to any provision that it holds to be unenforceable, by modifying that provision to the minimum extent necessary to make it enforceable or, if that modification is not permitted by law, by disregarding that provision;

28.2 If an unenforceable provision is modified or disregarded in accordance with this section, by holding that the rest of the Agreement will remain in effect as written;

28.3 By holding that any unenforceable provision will remain as written in any circumstances other than those in which the provision is held to be unenforceable; and

28.4 If modifying or disregarding the unenforceable provision would result in failure of an essential purpose of this Agreement, by holding the entire Agreement unenforceable.

29. Audit and Inspection

Entity is subject to audit and inspection, at any time during normal business hours and at a mutually agreed upon location, by the Texas State Auditor's Office, DPS, or any other department or agency responsible for determining that the Parties have complied with applicable law. Entity must provide all reasonable facilities and assistance for the safe and convenient performance of any audit or inspection and Entity must provide any such records and documents to DPS, the Texas State Auditor's Office, or applicable agency upon request. Entity must keep all records and documents regarding this Agreement for the term of this Agreement and for five years after the termination of this Agreement.

If DPS requests information from the Entity or a Third Party Requestor to determine if they have complied with applicable law or this Agreement, they must provide the requested information no later than the fifth business day after DPS submits the request unless DPS extends the deadline.

30. Survival

Any provisions of this Agreement that impose continuing obligations on Entity will survive the expiration or termination of this Agreement.

31. Term of Agreement

The term of this Agreement is effective on the last date signed in the Agreement section entitled "User Acceptance of Agreement" and will continue in full force and effect for a term of five years from that full execution date.

32. Acceptance of User Agreement

By signing this agreement, Entity agrees to the terms and conditions of this Agreement and all incorporated Attachments.

In order to receive any Driver Records and driver record monitoring services, an authorized signatory, the Chief Information Officer (CIO), and the Chief Information Security Officer (CISO) must sign this Agreement. Entity may not use the records if it does not accept the Agreement and all incorporated Attachments in their entirety.

Chief Information Security Officer *Insert signatory name and title here.*
Signature **Date:**

Chief Information Officer *Insert name and title here.*
Signature **Date:**

Entity's Authorized Representative *Insert signatory name and title here.*
KP George Fort Bend County Judge
Signature **Date:**

ATTACHMENT A
ENTITY'S INFORMATION FORM

D/B/A, if applicable (including names of all subsidiaries and companies comprising part of this Entity:

N/A

Federal Tax Identification Number:

List all web address internet sites (Uniform Resource Locator–URL), Facebook, or Twitter accounts used or possessed by Entity:

www.fortbendcountytx.gov

FaceBook - group Fort Bend County Risk Management

Nature of Entity's Business Activities and Practices:

County government

Detailed explanation of the intended use of Driver Records and Monitoring Services obtained from DPS (describe how the exemption qualifies for the purchase of Driver Records and Monitoring Services):

Fort Bend County Risk Management - MVR checks on pre-employment /employees to authorize drivers for business in all county departments. Authorized drivers are needed in county departments such as EMS, Sheriff, Road & Bridge, Drainage, etc. Only employees with acceptable driving history are eligible to drive for county business.

If Entity intends to release Driver Records to a Third Party Requestor, explain what safeguards or assurances are in place to meet the requirements of this Agreement and provide a copy of the written contract between Entity and the Third Party Requestor:

N/A - Fort Bend County Risk Management will not release records.

If Entity does not intend to release Driver Records to a Third Party Requestor, state so below:

Driver records will not be released to any third party requester, for internal use only

ATTACHMENT B

Rules of Behavior for Individuals Accessing DPS Data

Purpose

This document delineates the responsibilities and expected behavior of all individuals that use and have access to data provided by the Department of Public Safety of the State of Texas (DPS). Additionally, this document fosters the comprehensive knowledge of and compliance with the DPS rules of behavior as a condition for continued data access and sets forth requirements for verification of understanding with the rules as documented. DPS data users will be held accountable for their actions and are responsible for securing the data and resources in accordance with the DPS rules of behavior. All persons requiring access to DPS data must read, understand, and formally acknowledge those rules of behavior by signing this agreement prior to being granted access to DPS data.

User Rules of Behavior

1. I understand that I am required to perform my official duties when given access to DPS data.
2. I must restrict disclosure of DPS data to only those with a business need and are authorized to receive the information.
3. I must not send or store DPS sensitive or confidential information to a personal e-mail account.
4. I must take every precaution to prevent unauthorized individuals from observing display output. (Use privacy screens, keep computer screens from facing windows or doors, etc.)
5. I must log off or lock my workstation or laptop computer, or I must use a password-protected screensaver, whenever I step away from my work area, even for a short time.
6. I must not transmit DPS sensitive or confidential information unencrypted outside the secure network.
7. I must securely store all removable media containing DPS data when not in use.
8. I will ensure DPS sensitive or confidential data stored on removable or portable media is AES 256 encrypted, and the media is marked with the appropriate data classification.
9. I will comply with the DPS password policy.
10. I will immediately report security violations and incidents involving DPS data to my supervisor and DPS Cyber Security.

Acknowledgement

I acknowledge that I have read and received a copy of the signed Data Sharing Agreement signed by DPS and Entity. I acknowledge that I have read and understand the Rules of Behavior and must comply with them.

Name of User (printed):_____

Supervisor's Name: _____

_____ _____

(User Signature) (Date)

ATTACHMENT C

Data Sharing Agreement for Release of Driver Records

1.0 Data Sharing Statement

The requirement for data sharing between the Department of Public Safety of the State of Texas (DPS) and *Entity* exists for the sole purpose to deliver driver records under Texas Transportation Code Chapters 521 and 730.

2.0 Security

2.1 General Description of Information Sensitivity

Confidentiality, integrity, and availability requirements and standards are derived from the Criminal Justice Information Services (CJIS) Security Policy (http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/), 1 Texas Administrative Code §202.1 *et seq.*, and DPS General Manual Chapters 25, *Cyber Security*, and 26, *Information Resource Policy*. The DPS General Manual Chapters are incorporated by reference.

2.2 Trusted Behavior Expectations/Rules of Behavior

Entity must protect DPS data in accordance with this DSA. Entity will provide a copy of this DSA to all authorized personnel.

2.3 Formal Security Policy

DPS developed these procedures under this DSA to ensure the protection of DPS data when it is being provided to outside entities. Entity must comply with the procedures of this DSA for all systems used to store, process, or transmit DPS data. DPS may modify these requirements in its discretion, in accordance with its cyber security policies.

2.4 Administrative Security

Entity must comply with the following administrative security procedures:

a. Entity must use host systems that have an approved warning banner displaying a message of consent to monitoring and that unauthorized use is subject to criminal prosecution or criminal or civil penalties, prior to login.

b. Entity must ensure that host systems that contain any DPS data are used for official purposes only.
c. Entity must appropriately safeguard all DPS data and only release it to authorizedindividuals.
d. Entity may not share DPS's data with an entity except in accordance with the terms of this Agreement.

2.5 Identification and Authentication

The purpose of authentication is to provide reliable identification for access to data or information systems. Entity must maintain the identity of active users, linking actions to specific users, and all other identification and authentication requirements. Non-repudiation must be maintained for each user accessing DPS data.

2.6 Audit Trail and Review

An audit trail is a chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the final output. Entity must comply with the following audit trail procedures:

a. Entity information systems that process DPS data will produce an audit trail that records, for all users, the following at a minimum:
    - The identity of each person and device that accesses or attempts to access the system or application
    - Start-up and shutdown of the audit functions
    - Successful use of the user security attribute administration functions
    - All attempted uses of the user security attribute administration functions
    - Identification of which user security attributes have been modified
    - Successful and unsuccessful logons and logoffs
    - Unsuccessful access to security relevant files including creating, opening, closing, modifying, and deleting those files
    - Changes in user authenticators
    - Blocking or blacklisting user IDs, terminals, or access ports
    - Denial of access for excessive logon attempts
    - System access by privileged users (privileged activities at the system, either physical or logical consoles) and other system-level access by privileged users). Users may not have administrative privileges to local systems unless the systems are standalone.
    - Starting and ending times for each access to the system.

b. For analysis purposes, Entity must retain audit trails for at least one year or in accordance with Entity security policy, whichever is longer.

c. All audit trails must be protected from actions such as unauthorized access,modification, and destruction that would negate their forensic value.

2.7 Logical Access Control

Logical access controls provide a technical means to control user access to information and system resources. They control what information users can access, the programs they can run, and the modifications they can make. Entity must comply with the following logical access controls:

a. The identity of the user must be established before access to DPS data is granted.
b. Users will have access only to data to which they are entitled (the principle of least privilege will be enforced).
c. Entity information systems processing DPS data will automatically disconnect or otherwise deny access to a user after three failed logon attempts.
d. Entity information systems processing DPS data will initiate a session lock or termination after a maximum of 30 minutes of inactivity and require the user to reauthenticate to regain access.

2.8 Password Management

Password management includes the generation, issuance, and control of the passwords that support authentication. Entity must comply with the following password management for access to DPS information:

a. Password management must meet the requirements of DPS security policy at minimum; however, Entity is authorized to implement password requirements that exceed DPS security policy. To comply with DPS security policy, passwords must:
    (1) Be a minimum length of 8 characters;
    (2) Contain a mix of upper and lower case characters, numeric characters, and special characters;
    (3) Not be a dictionary word or proper name;
    (4) Not be the same as, or contain, the User ID;
    (5) Expire within a maximum of 90 calendar days;
    (6) Not be identical to the previous 10 passwords;
    (7) Never be displayed in clear text on the screen; and never be written down and stored physically.
b. Passwords considered re-usable must be encrypted during transmission.
c. Passwords must be stored in an encrypted form in a protected password file to ensure confidentiality.

d. If the security of a password is in doubt, the password must be changed immediately.

2.9 Software Security

Entity must use anti-virus protection software. Entity must manage the anti-virus protection software to include upgrades, updates, modifications, corrections, patches, plugins, etc., that may be required to keep the software current and effective.

2.10 Telecommunications Security

Telecommunications security is concerned with the protection of data during transmission. Entity must comply with the following telecommunication security requirements:

a. All data must be protected during transmission in compliance with Federal Information Processing Standard (FIPS) 140-2 approved cryptographic modules and 1 Texas Administrative Code § 202.1 *et seq*.
b. All passwords must be protected during transmission using a mechanism that is compliant with Federal Information Processing Standard (FIPS) 140-2 approved cryptographic modules and 1 Texas Administrative Code § 202.1 *et seq*.

2.11 Media Security

Entity must apply the following policies for marking and disposition of tapes, flash drives, hard drives, printouts, or any other media containing sensitive or confidential data: media containing sensitive or confidential data must be labeled with the appropriate data classification (e.g., Sensitive, Confidential). Prior to release or disposal, electronic media containing sensitive or confidential data must be completely erased or destroyed using DPS authorized methods, which align with CJIS Security Policy section 5.8.3.

2.12 Incident Response

An information system incident is an unexpected, unplanned event that could have a negative effect on information technology resources. A security incident is an event that violates security policies or circumvents security mechanisms (e.g., hostile probes, intrusions, malicious software), and may lead to the unauthorized exposure, access, disclosure, compromise, or loss of DPS information. Entity must comply with the following incident response policy:

a. In the event of a confirmed security incident, *Entity* must notify the DPS Chief Information Security Officer (CISO) in writing within four hours of discovering the incident or being notified of an incident that involves any DPS data.
b. If a security incident is suspected, but not yet confirmed, Entity must notify the DPS Chief Information Security Officer (CISO) in writing within 24 hours of discovering the potential incident or being notified of a potential incident that involves any DPS data.
c. In the event of a security incident where Entity has detected or confirmedan intrusion,

the DPS CISO, or the CISO's designated agent, will have authority to suspend the transmission of any DPS data to *Entity* until it has proven recovery to a secure state that can ensure the confidentiality of DPS data. In addition, Entity must also promptly provide DPS with a copy of any incident reports involving DPS data.

2.13 Training and Awareness

Entity must ensure that all Entity end users receive initial and annual DIR-certified security awareness training.In addition, Entity must ensure all users (persons and entities) sign the Rules of Behavior Agreement, Attachment B, prior to those users having access to any DPS data.

3.0 Roles and Responsibilities

3.1 *Entity* Responsibilities

Entity must:

a. Protect all Personal Identifying Information in accordance with Texas Business and Commerce Code § 521.001(1) and 1 Texas Administrative Code § 202.1 *et seq*.
b. Provide proof of compliance with security documents when requested to do so by DPS.
c. Ensure appropriate protection of all security documents.
d. Maintain copies of signed Rules of Behavior for every authorized user.
e. Have complete responsibility for all cyber security controls.
f. Have complete responsibility for encryption of all system components in accordance with Federal Information Processing Standard (FIPS) Publication 140-2.
g. Maintain all logical access controls and password management.
h. Maintain all system software, anti-virus protection, encryption, and operating systems, to include all upgrades, updates, patches, plugins, etc.
i. Only grant users access to data they need to perform their official functions.
j. Not share DPS's data outside Entity unless otherwise authorized under this Agreement.
k. Ensure that it, and any entity that it shares DPS's data with, complies with the requirements in this data agreement if Entity shares or sells DPS' data.
l. Report any security breaches involving Entity (or shared entity or users) to the DPS CISO.
m. Implement the necessary procedures to ensure that Entity is secure from any unauthorized use.
n. Ensure that any individual requesting access to DPS data is authorized to receive it. Unauthorized request or receipt of data could result in criminal proceedings brought against the Entity and the individuals or entities involved.
o. Ensure all users complete the required security awareness training prior to access, and annually thereafter.
p. Disseminate user manuals and other related publications as required.
q. Conduct investigations relating to possible fraud, waste, and abuse.

3.2 DPS Responsibilities

DPS will:

a. Protect all Personal Identifying Information in accordance with Texas Business and Commerce Code § 521.001(1) and 1 Texas Administrative Code § 202.1 *et seq*.
b. Ensure appropriate protection of all security documents.
c. Maintain communication with *Entity* to ensure operational needs are being met.
d. Manage security incident assessment and response.

ATTACHMENT D

Additional Requirements for Bulk Record Purchases under Texas Transportation Code § 521.050

Texas Transportation Code § 730.014 imposes additional requirements for Entities who purchase Driver Records in the bulk format under Texas Transportation Code § 521.050. These include the posting of a performance bond and providing proof of general liability and cyber-threat insurance coverage. The bond and insurance requirements do not apply to a governmental entity.

1.0 Bond for Bulk Record Purchase (not applicable to governmental entities)

A performance bond in the amount of $1,000,000 will be required before Entity can receive Driver Records in the bulk format under Texas Transportation Code § 521.050. Said bond will be solely for the protection of the State of Texas.

2.0 Insurance (not applicable to governmental entities)

Entity must provide proof of at least $3,000,000 in general liability and cyber-threat insurance coverage, but notwithstanding that minimum, the coverage must be reasonably related to the risks associated with unauthorized access and use of the Driver Records.

Entity must provide proof of and maintain for the term of the Agreement no less than the minimum insurance coverage specified. Proof of insurance and bond coverage may be provided in the form of current certificates of insurance. DPS does not accept "self-insurance" coverage.

All required insurance coverage must be issued from a company or companies with a Financial Strength Rating of "A" or better from A.M. Best Company, Inc.

All insurance policies for required coverage must be issued by companies authorized to do business under the laws of the State of Texas and in a form satisfactory to DPS. All required insurance contracts must: (1) be written on a primary and non-contributory basis with any other insurance coverages Respondent currently has in place; and (2) include a Waiver of Subrogation Clause.

Entity must:

A. provide all required written documentation under this section to DPS.
B. ensure all insurance policies and certificates of insurance for required coverage are written to include all the risks associated with unauthorized access and use of the Driver Records. There must be sufficient coverage to cover any losses, security breaches, privacy breaches, unauthorized distributions, or releases or uses of any data transferred to or accessed by Entity under or as a result of this Agreement. This includes response required under Tex. Bus. & Com. Code Chapter 521.
C. ensure that all required policies contain endorsements prohibiting cancellation except upon at least 30 days' advanced written notice to DPS.
D. deliver all copies of changes to insurance coverage (including extensions, renewals, cancellations, and revisions) at least ten calendar days prior to any expiration of a required policy. All renewal policies and corresponding certificates of insurance must meet all terms set forth in the Contract.

E. ensure that all provisions of the Contract concerning liability, duty, and standard of care, together with the indemnification provision, are underwritten by contractual liability coverage sufficient to include Entity's obligations under the Agreement.
F. obtain and maintain insurance policies that provide coverage for Entity's principals, officers, directors, shareholders, partners, owners, agents, employees, subcontractors, independent contractors, and any other representatives who may provide services under this Agreement.

3.0 Notice of Breach

If Entity experiences a breach of system security as defined by Texas Business & Commerce Code § 521.053 that includes data obtained under Texas Transportation Code § 730.007, Entity must notify DPS of the breach not later than 24 hours after the discovery of the breach.

4.0 Annual Report to DPS of Resell and Re-disclosure

Entity must annually provide to DPS a report of all third parties to which the personal information was sold or disclosed under this section and the purpose of the resell or re-disclosure.

5.0 Prohibition on Resell or Re-disclosure for Marketing Vehicle Warranties

Entity may not resell or re-disclose Driver Records for the purpose of marketing extended vehicle warranties.