RESOLUTION NO. 20-2734

A RESOLUTION OF THE TOWN COMMISSION OF THE TOWN OF SURFSIDE, FLORIDA, APPROVING A MEMORANDUM OF UNDERSTANDING (MOU) BETWEEN THE TOWN OF SURFSIDE, THE FLORIDA DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES, AND THE PINELLAS COUNTY SHERIFF'S OFFICE FOR ACCESS TO THE BIOMETRIC FACIAL ANALYSIS SYSTEM; PROVIDING FOR AUTHORIZATION; PROVIDING FOR IMPLEMENATION; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, the Town of Surfside ("Town") Police Department desires to access the Pinellas County Sheriff's Office ("PCSO") Biometric Facial Analysis System, which would provide the Town's Police Department access to driver's license and motor vehicle information for the purpose of biometric comparison; and

WHEREAS, in order to access the Biometric Facial Analysis System, the Florida Department of Highway Safety and Motor Vehicles ("FLHSMV") requires that all municipalities enter into an agreement declaring that they are qualified to obtain and protect personal information and highly restricted personal information on the FLHSMV database; and

WHEREAS, the Town and PCSO desire to enter into an Memorandum of Understanding, in substantially the form attached hereto as Exhibit "A" ("MOU"), to allow the Town's Police Department to access the PCSO Biometric Facial Analysis System; and

WHEREAS, the Town Commission finds that this Resolution is in the best interest and welfare of the Town and law enforcement.

NOW, THEREFORE, BE IT RESOLVED BY THE TOWN COMMISSION OF THE TOWN OF SURFSIDE, FLORIDA, AS FOLLOWS:

Section 1. Recitals Adopted. Each of the above-stated recitals are hereby adopted, confirmed and incorporated herein.

Section 2. **Approval of MOU.** The Town Commission hereby approves the MOU, in substantially the form attached hereto as Exhibit "A."

Section 3. **Authorization.** The Town Manager is hereby authorized to execute the MOU, subject to final approval by the Town Manager and Town Attorney as to form, content, and legal sufficiency.

Section 4. **Implementation.** The Town Manager and Town Officials are hereby authorized to take any and all action necessary to implement the purposes of the MOU and this Resolution.

Section 5. **Effective Date.** This Resolution shall be effective immediately upon adoption.

PASSED AND ADOPTED this 19th day of November, 2020.

Motion By: Commissioner Kesl
Second By: Commissioner Velasquez

FINAL VOTE ON ADOPTION:

Commissioner Charles Kesl	Yes
Commissioner Eliana R. Salzhauer	Yes
Commissioner Nelly Velasquez	Yes
Vice Mayor Tina Paul	Yes
Mayor Charles W. Burkett	Yes

Charles W. Burkett, Mayor

ATTEST:

Sandra McCready, MMC
Town Clerk

APPROVED AS TO FORM AND LEGALITY FOR THE USE AND BENEFIT OF THE TOWN OF SURFSIDE ONLY:

Weiss Serota Helfman Cole & Bierman, P.L.
Town Attorney

FLHSMV

Contract Number HSMV-_____

MEMORANDUM OF UNDERSTANDING
FOR ACCESS TO BIOMETRIC FACIAL ANALYSIS SYSTEM

This Memorandum of Understanding (MOU) is made and entered into by and between _____, hereinafter referred to as the Requesting Party or Third Party End User, as defined herein, executing this MOU, and the Florida Department of Highway Safety and Motor Vehicles, hereinafter referred to as the Providing Agency, collectively referred to as the Parties.

I. The Parties

The Providing Agency is a government entity whose primary duties include issuance of motor vehicle and driver licenses, registration and titling of motor vehicles, and enforcement of all laws governing traffic, travel, and public safety upon Florida's public highways.

In carrying out its statutorily mandated duties and responsibilities, the Providing Agency collects and maintains Driver License Information that identifies individuals. Based upon the nature of this information, the Providing Agency is subject to the disclosure prohibitions contained in 18 U.S.C. §2721, the Driver's Privacy Protection Act (hereinafter "DPPA"), Sections 119.0712(2), 322.142, and 501.171, Florida Statutes, and other statutory provisions.

The Requesting Party is a law enforcement agency operating under the laws and authority of the state of Florida and/or operating under Federal law, and is requesting Driver License Information including access to digital images of full-face Driver License Photographs from the Providing Agency for purposes of biometric comparison, and by signature hereon, declares that it is qualified to obtain both personal information and highly restricted personal information under the exception number(s), listed in Attachment I, authorized by DPPA and Sections 119.0712(2) and 322.142, Florida Statutes.

The Third Party End User is a law enforcement agency operating under the laws and authority of the state of Florida and/or operating under Federal law, and is requesting Driver License Information including access to digital images of full-face Driver License Photographs through the Requesting Party for purposes of biometric comparison, and by signature hereon, declares that it is qualified to obtain both personal information and highly restricted personal information under the exception number(s), listed in Attachment I, authorized by DPPA and Sections 119.0712(2) and 322.142, Florida Statutes.

II. Purpose

This MOU is entered into for the purposes of establishing the conditions and limitations under which the Providing Agency agrees to provide or otherwise make available electronic access to its Biometric Facial Analysis System to the Requesting Party or Third Party End User.

Any Driver License Information and Driver License Photographs provided under the authority of this MOU shall be for the purposes of biometric comparison and not as positive comparison of any individual. Such information, including photographs, shall be considered an investigative lead to be manually analyzed, evaluated and compared against a Probe Photograph, as defined below, by the Requesting Party or Third Party End User.

III. Definitions

For the purposes of this MOU, the below-listed terms shall have the following meanings:

A. **Biometric Facial Analysis System** – The Providing Agency's system, provided through its selected vendor, consisting of all the equipment, software, accessories, and similar items required for the automatic processing of digital images that contain the faces of individuals for purposes of comparison, authentication/verification of those individuals.

B. **Business Point-of-Contact** - A person appointed by the Requesting Party or Third Party End User to assist the Providing Agency with the administration of the MOU.

C. **Driver License Information** – Driver license and identification card data and information collected and maintained by the Providing Agency. This data and information includes personal information, and highly restricted personal information, as defined in items G and I below.

D. **Driver License Photograph** – Digital image(s) of an individual collected and maintained by the Providing Agency pursuant to Chapter 322, Florida Statutes. The photograph can only be provided pursuant to Section 322.142, Florida Statutes.

E. **Driver Privacy Protection Act (DPPA)** - The Federal Act (see, 18 United States Code § 2721, et seq.) that prohibits release and use of personal information, and highly restricted personal information, except as otherwise specifically permitted within the Act.

F. **Law Enforcement Agency** - An agency whose primary responsibility is the prevention and detection of crime and the enforcement of the penal, criminal, traffic, or highway laws of the state or country; and is also a Criminal Justice Agency subject to and in good standing under the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy; and is either a state, county, or city government agency that employs sworn law enforcement officers, as defined in Section, 943.10(1), Florida Statutes, or is a federal agency that employs full-time officers with authority to make arrests and carry firearms while on duty.

G. **Highly Restricted Personal Information** - Includes, but is not limited to, Driver License Photographs, medical or disability information or social security number.

H. **Parties** - The entities executing and intending to be legally bound under the terms and conditions of this MOU.

I. **Personal Information** - As described in Section 119.0712(2)(b), Florida Statutes, and 18 U.S.C. S.2725, Information found in the motor vehicle or driver record which includes, but is not limited to, the subject's driver comparison number, name, address, (but not the 5 – digit zip code), date of birth, height, and medical or disability information.

J. **Personal Identifiable Information** – Information about an individual provided by the Biometric Facial Analysis System, which may include, but is not limited to, the Driver License Photograph, customer number, name, address (city, state, and zip only), gender, date of birth, height, driver license number, driver license issue date, and race. Personal Identifiable Information includes information that is defined as Personal Information and Highly Restricted Personal Information under DPPA.

K. **Probe Photograph** – The photograph provided by a law enforcement agency that is being submitted for comparison with Driver License Photographs in the Providing Agency's Biometric Facial Analysis System.

L. **Providing Agency** - The Department of Highway Safety and Motor Vehicles. The Providing Agency is responsible for granting access to driver license and/or motor vehicle data and information to the Requesting Party and Third Party End User, as applicable.

M. **Quarterly Quality Control Review Report** – Report completed each quarter by the Business Point-of-Contact to monitor compliance with this agreement, containing the information required in Section VII., Compliance and Control Measures, subsection A.

N. **Requesting Party** - Any Law Enforcement Agency that is expressly authorized by Sections 119.0712(2) and 322.142, Florida Statutes, and DPPA to request and receive Driver License Information including Driver License Photographs contained in a driver license record for purposes of biometric comparison through an electronic interface with the Providing Agency.

O. **Technical Contact** - A person appointed by the Requesting Party to oversee the setup, maintenance, and operation of the Biometric Facial Recognition System interface with the Providing Agency.

P. **Third Party End User** - Any Law Enforcement Agency that is expressly authorized by Sections 119.0712(2) and 322.142, Florida Statutes, and DPPA to request and receive Driver License Information including Driver License Photographs contained in driver license records for purposes of biometric comparison through an interface with the Requesting Party, and has entered into a Memorandum of Understanding with the Providing Agency authorizing such access.

Q. **Web Service** - A service where the Requesting Party writes a call program to communicate with the Web Service of the Providing Agency to receive authorized motor vehicle and driver license data and information.

IV. Legal Authority

The Providing Agency maintains computer databases containing information pertaining to driver's licenses and motor vehicles pursuant to Chapters 317, 319, 320, 322, 328, and Section 324.242(2), Florida Statutes. The driver license, motor vehicle, and vessel data contained in the Providing Agency's databases is defined as public record pursuant to Chapter 119, Florida Statutes; and as such, is subject to public disclosure unless otherwise exempted by law.

As the custodian of the state's driver and vehicle records, the Providing Agency is required to provide access to records permitted to be disclosed by law.

Under this MOU, the Requesting Party will be provided, via remote electronic means, information pertaining to driver licenses, including Personal Identifiable Information authorized to be released pursuant to Sections 119.0712(2) and 322.142, Florida Statutes, and DPPA.

This MOU is governed by the laws of the State of Florida and jurisdiction of any dispute arising from this MOU shall be in Leon County, Florida.

V. Statement of Work

A. The Providing Agency agrees to:

1. Provide the Requesting Party with the technical specifications, and any additional information required to access data and information in accordance with one of the following allowed access methods:

   a. Access via the Biometric Facial Analysis System's Application Program Interface (API) using the Requesting Party's User Interface (UI)

   b. Access via the Biometric Facial Analysis System's User Interface (UI)

2. Allow the Requesting Party to electronically access data and information as authorized under this MOU.

3. Perform all obligations to provide access under this MOU contingent upon an annual appropriation by the Legislature.

4. Provide electronic access to Personal Identifiable Information pursuant to roles and times established other than scheduled maintenance or other uncontrollable disruptions. Scheduled maintenance normally occurs Sunday mornings between the hours of 6:00 A.M. and 10:00 A.M.

5. Provide a contact person for assistance with the implementation of services to be provided under this MOU.

B. The Requesting Party and/or Third Party End User agrees to:

1. Utilize information obtained pursuant to this MOU, only as authorized by law for the purposes prescribed by law, and as further described in this MOU.

2. Search and compare Probe Photographs to Personal Identifiable Information for biometric comparison utilizing one of the allowed access methods identified in Section V, Statement of Work, subsection A.1., above. This search and comparison may only be conducted when:

   A. The Requesting Party or Third Party End User has reasonable suspicion that the person in the Probe Photograph being searched is the suspect, person of interest, witness or victim of a crime, and can associate the probe photograph with an investigative case number; or,

   B. To intervene in life-threatening emergencies; or,

   C. To locate missing persons where the probe photograph can be associated with an investigative case number; or,

   D. To assist with the comparison of and/or determine the identity of individuals that are unable to communicate their identity; or

   E. To prevent or investigate the crime of terrorism as defined in 18 U.S. Code § 2332b or

Section 775.30, Florida Statutes, where the probe photograph can be associated with an investigative case number.

3. Not use Personal Identifiable Information for biometric comparison solely to track or identify individuals engaging in political, religious, or other protected free speech.

4. Maintain the confidential and exempt status of any and all information provided by the Providing Agency in compliance with this MOU and Sections 119.0712(2) and 322.142, Florida Statutes, and DPPA.

5. Retain information obtained from the Providing Agency only if necessary for law enforcement purposes. If retained, information shall be safeguarded in compliance with Section VI. Safeguarding Information, subsection C.

6. Ensure that its employees and agents comply with Section VI. Safeguarding Information.

7. Prior to allowing access to the Biometric Facial Analysis System by a Third Party End User, confirm with the Providing Agency that the Third Party End User has a valid MOU with the Providing Agency.

8. Self-report to the Providing Agency all violations of this MOU within thirty (30) days of discovery of such violation(s). The report shall include a description of the violation, the time period of the violation, the number of records impacted, and all steps taken as of the date of the report to remedy or mitigate any injury caused by the violation. If the report cannot be completed within thirty (30) days, the Requesting Party or Third Party End User agrees to notify the Providing Agency of the violation no later than the end of the thirtieth day by providing a written summary of the incident, and submit the full report as soon as possible upon its completion.

9. If the Providing Agency determines the Third Party End User has violated the provisions of Sections 119.0712 or 322.142, Florida Statutes, DPPA or this MOU, the Requesting Party agrees to terminate the Third Party End User's access to all Personal Identifiable Information upon a written request from the Providing Agency.

10. The Requesting Party accepts responsibility for interfacing with any and all Third Party End Users. It is the sole responsibility of the Requesting Party to provide the interface which will allow Third Party End Users to access Personal Identifiable Information through the Requesting Party's system.

11. Establish procedures and controls to ensure that its employees and agents comply with Section VI. Safeguarding Information. At a minimum, these controls must include a process for granting user access, logging use of the system by user, and periodically reviewing use of the system, including reviewing the submission of Probe Photographs that do not have an associated investigative case number.

12. Not assign, sub-contract, or otherwise transfer its rights, duties, or obligations under this MOU without the express written consent and approval of the Providing Agency.

13. Use the information received from the Providing Agency only for the purposes authorized by this MOU. The Requesting Party or Third Party End User shall not share or provide any

information to another unauthorized entity, agency, or person.

14. Protect and maintain the confidentiality and security of the data and information received from or through the Providing Agency in accordance with this MOU and applicable state and federal laws.

15. Requesting Party agrees to indemnify the Providing Agency and its employees and agents from any and all damages arising from the Requesting Party's negligent, improper, or unauthorized access, use, or dissemination of information provided by the Providing Agency, to the extent allowed by law.

16. Third Party End User agrees to indemnify the Providing Agency and Requesting Party, and its employees and agents from any and all damages arising from the Third Party End User's negligent, improper, or unauthorized access, use, or dissemination of information provided by the Providing Agency, to the extent allowed by law.

17. For Federal Agencies Only: If any injury, or loss of or damage to any real or personal property of any person, is caused by the Requesting Party or a Third Party End User, its liability, if any, shall be determined in accordance with applicable law, including applicable provisions of the Federal Tort Claims Act, 28 U.S.C. § 2671 et seq. The liability of the Requesting Party or Third Party End User under this paragraph is subject to the availability of appropriation for such payment, and nothing contained herein may be considered as a guarantee that Congress will at a later date appropriate funds sufficient to meet any deficiencies.

18. The Requesting Party shall update it's user's access/permissions upon reassignment of users within five (5) business days of the reassignment or within five (5) business days of notification from the Third-Party End User.

19. The Requesting Party shall immediately inactivate its user's access/permissions, following separation, or negligent, improper, or unauthorized use or dissemination of any information or immediately after notification from the Third-Party End User.

20. For all records containing Personal Identifiable Information and released to a Requesting Party or Third Party End User, maintain records identifying each person or entity that receives such information, and the permitted purpose for which it will be used, for a period of not less than five (5) years. The Requesting Party shall provide these records or otherwise make these records available for inspection within five (5) business days of a request by the Providing Agency.

21. Pay all costs associated with electronic access to the Providing Agency's Biometric Facial Analysis System or to information or data contained therein.

22. Notify the Providing Agency within ten (10) calendar days of any changes to the name, address, telephone number and/or email address of the Requesting Party or Third Party End User or its Business Point-of-Contact. The information shall be e-mailed to DataListingUnit@flhsmv.gov. Failure to update this information as required may adversely affect the timely receipt of information from the Providing Agency.

23. Understand that this MOU is subject to any restrictions, limitations, or conditions enacted by

the Florida Legislature, which may affect any or all terms of this MOU. The Requesting Party or Third Party End User understands that they are obligated to comply with all applicable provisions of law.

24. Timely submit information required in Section VII. Compliance and Control Measures.

VI. Safeguarding Information

The Parties shall access, disseminate, use and maintain all information received under this MOU in a manner that ensures its confidentiality and proper utilization in accordance with Chapters 119 and 322, Florida Statutes, and DPPA. Information obtained under this MOU shall only be disclosed to persons to whom disclosure is authorized under Florida law and applicable federal laws. Any disclosure of information shall be in accordance with 18 U.S.C. §2721(c). In the event of a security breach, the Requesting Party or Third Party End User agrees to comply with the provisions of Section 501.171, Florida Statutes.

Any person who knowingly violates any of the provisions of this section may be subject to criminal punishment and civil liability, as provided in Sections 119.10 and 775.083, Florida Statutes. In addition, any person who knowingly discloses any information in violation of DPPA may be subject to criminal sanctions, including fines, and civil liability.

A. **The Requesting Party and Third Party End User shall notify the Providing Agency of any of the following within five (5) business days:**

1. Termination of any agreement/contract between the Requesting Party or Third Party End User and any other State/State Agency due to non-compliance with DPPA, data breaches, or any state laws relating to the protection of driver privacy.

2. Any pending litigation alleging DPPA violations or under any state law relating to the protection of driver privacy.

3. Any instance where the Requesting Party or Third Party End User is found guilty or liable by a court of competent jurisdiction for misuse of data under DPPA or under any state law relating to the protection of driver privacy.

4. A breach of security as defined by Section 501.171, Florida Statutes.

B. **The Parties mutually agree to the following:**

1. Information exchanged will not be used for any purposes not specifically authorized by this MOU and its attachments. Unauthorized use includes, but is not limited to, queries not related to a legitimate law enforcement purpose, personal use, and the dissemination, sharing, copying or passing of this or any unauthorized information to unauthorized persons.

2. The Requesting Party and Third Party End User shall not indemnify and shall not be liable to the Providing Agency for any driver license or motor vehicle information lost, damaged, or destroyed as a result of the electronic exchange of data and information pursuant to this MOU, except as otherwise provided in Section 768.28, Florida Statutes.

3. Information obtained from the Providing Agency will be stored in a location that is physically and logically secure from access by unauthorized persons.

4. The Requesting Party and Third Party End User shall develop security requirements and standards consistent with Section 282.318, Florida Statutes, Rule Chapter 60GG-2 (previously 74-2), Florida Administrative Code, and the Providing Agency's security policies; and employ adequate security measures to protect Providing Agency's information, applications, data, information resources, and services. The applicable Providing Agency security policies are set forth in Attachment II.

5. Access to the information received from the Providing Agency will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information.

6. All personnel, including personnel of Third Party End Users, with access to the information exchanged under the terms of this MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information prior to accessing the information. These acknowledgements must be maintained by the Requesting Party or Third Party End User and be provided to the Providing Agency within ten (10) business days of a request.

7. All personnel, including personnel of Third Party End Users, with access to the information exchanged under the terms of this MOU will be instructed of, and acknowledge their understanding of the civil and criminal sanctions specified in state and federal law for unauthorized use of the data and information. These acknowledgements must be maintained in a current status by the Requesting Party or Third Party End User and provided to the Providing Agency within ten (10) business days of a request.

8. Access by its users to the information exchanged under the terms of this MOU must be monitored on an ongoing basis by the Requesting Party and Third Party End User. In addition, the Requesting Party and Third Party End User must complete an Annual Certification Statement to ensure proper and authorized use and dissemination of information and provide it to the Providing Agency pursuant to Section VII. C. below.

9. All data and information received from the Providing Agency shall be encrypted during transmission to Third Party End Users using Transport Layer Security (TLS) version 1.2 or higher encryption protocols. Alternate encryption protocols are acceptable only upon prior written approval by the Providing Agency.

10. By signing the MOU, the representatives of the Providing Agency, the Third Party End User and Requesting Party, on behalf of the respective Parties, attest and ensure that the confidentiality of the information exchanged will be maintained.

VII. Compliance and Control Measures

A. **Quarterly Quality Control Review Report** - Must be completed by the Requesting Party, utilizing Attachment III, Quarterly Quality Control Review Report, within 10 days after the end of each quarter and maintained for two years. This review must include the following elements:

   a. A comparison of the users by agency report with the agency user list;

   b. A listing of any new or inactivated users since the last quarterly quality control review; and

c. Documentation verifying that usage has been internally monitored to ensure proper, authorized use and dissemination.

B. **Internal Control and Data Security Audit** - This MOU is contingent upon the Requesting Party and Third Party End User having appropriate internal controls in place to ensure that data and other information being provided/received pursuant to this MOU is protected from unauthorized access, distribution, use, modification, or disclosure. At a minimum, these controls should include a process for granting user access, logging use of the system by user, and periodically reviewing use of the system, including reviewing the submission of Probe Photographs that do not have an associated investigative case number. The Requesting Party must submit an Internal Control and Data Security Audit on or before the first anniversary of the execution date of this MOU, or within one hundred twenty (120) days from receipt of a request from the Providing Agency, whichever occurs first. The Requesting Party may submit the Internal Control and Data Security Audit from their county or agency internal auditor or Inspector General, or from an independent Certified Public Accountant. The audit shall indicate compliance with all terms of the MOU and that the internal controls governing the use and dissemination of personal data and information, including Personal Identifiable Information, have been evaluated in light of the requirements of this MOU, including the completion of quarterly quality control reports, and applicable laws and are adequate to protect the personal data and information from unauthorized access, distribution, use, modification, or disclosure. This includes both policies/procedures in place for personnel to follow and data security procedures/policies in place to protect Personal Identifiable Information. The audit shall certify that the data security procedures/policies have been approved by an IT security professional. The audit shall also certify that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence. The audit must have an original signature of the Requesting Party's agency head or his or her designee, who is designated by Letter of Delegation to execute contracts/agreements on their behalf. The audit shall be sent via Certified U.S. Mail to the Providing Agency as set forth in Section XII, Notices.

C. **Annual Certification Statement** - The Requesting Party and Third Party End User shall each submit to the Providing Agency an annual statement indicating that the respective party has evaluated and certifies that it has adequate controls in place to protect the Personal Identifiable Information from unauthorized access, distribution, use, modification, or disclosure, and is in full compliance with the requirements of this MOU and applicable laws. This statement shall be submitted annually, within fifteen (15) business days after the anniversary of the execution date of this MOU. (NOTE: During any year in which an Internal Control and Data Security Audit is conducted, submission of the Internal Control and Data Security Audit may satisfy the requirement to submit an Annual Certification Statement.) Failure to timely submit the certification statement may result in an immediate termination of this MOU.

In addition, prior to expiration of this MOU, if the Requesting Party or Third Party End User intends to enter into a new MOU, a certification statement attesting that appropriate controls remained in place during the final year of the MOU and are currently in place shall be required to be submitted to the Providing Agency prior to issuance of a new MOU.

D. **Misuse of Personal Identifiable Information** – The Requesting Party or the Third Party End User must notify the Providing Agency in writing of any incident where it is suspected or confirmed that Personal Identifiable Information has been misused by its users as a result of unauthorized access, distribution, use, modification, or disclosure, by any means, within thirty (30) days of such discovery..

The statement must be provided on the Requesting Party's or Third Party End User's letterhead and include each of the following: a brief summary of the incident; the outcome of the review; the date of the occurrence(s); the number of records misused; the name or names of personnel responsible; whether disciplinary action or termination was rendered; and whether or not the person(s) whose Personal Identifiable Information, was misused, were notified. The statement shall also indicate the steps taken, or to be taken, by the Requesting Party or Third Party End User to ensure that misuse of data and information does not continue or recur. If the outcome of the review cannot be provided timely due to an on-going investigation, the Requesting Party or Third Party End User shall notify the Providing Agency of the incident, provide a summary of what occurred, and submit the detailed statement upon completion. This statement shall be mailed to the Providing Agency Bureau Chief of Records at the address indicated in Section XII, Notices. (NOTE: If an incident involving breach of Personal Identifiable Information did occur, and the Requesting Party or Third Party End User did not notify the owner(s) of the misused records, the Requesting Party or Third Party End User must indicate why notice was not provided.)

In addition, the Requesting Party and all Third Party End Users shall comply with the applicable provisions of Section 501.171, Florida Statutes, regarding data security and security breaches, and shall strictly comply and be solely responsible for adhering to the provisions regarding notice provided therein.

VIII. Liquidated Damages

Unless the Requesting Party or Third Party End User is a State of Florida Law Enforcement Agency, the Providing Agency reserves the right to impose liquidated damages upon the Requesting Party or Third Party End User.

Failure by the Requesting Party or Third Party End User to meet the established requirements of this MOU may result in the Providing Agency finding the Requesting Party or Third Party End User to be out of compliance, and, all remedies provided in this MOU and under law, shall become available to the Providing Agency.

A. General Liquidated Damages

In the case of a breach or misuse of data and information due to non-compliance with DPPA, Sections 119.0712(2), 322.142 or 501.171, Florida Statutes, or any other state laws designed to protect a driver's privacy and motor vehicle information, the Providing Agency may impose upon the Requesting Party or Third Party End User liquidated damages of up to $1,000.00 for each breach or incident of misuse.

In imposing liquidated damages, the Providing Agency will consider various circumstances including, but not limited to:

1. The Requesting Party's or Third Party End User's history with complying with DPPA, Sections 119.0712(2), 322.142 or 501.171, Florida Statutes, this MOU or any other state laws designed to protect a driver's privacy;

2. Whether the Requesting Party or Third Party End User self-reported violations of this MOU to the Providing Agency prior to discovery by the Providing Agency;

3. Whether the Requesting Party or Third Party End User violated this MOU over an extended

period of time;

4. Whether the Requesting Party's or Third Party End User's violation of this MOU directly or indirectly resulted in injury, and the nature and extent of the injury;

5. The number of records involved or impacted by the violation of this MOU;

6. Whether, at the time of the violation, the Requesting Party or Third Party End User had controls and procedures that were implemented and reasonably designed to prevent or detect violations of this MOU; and,

7. Whether the Requesting Party or Third Party End User voluntarily made restitution or otherwise remedied or mitigated the harm caused by the violation of this MOU.

In lieu of paying liquidated damages upon assessment, the Requesting Party or Third Party End User may elect to terminate the MOU contingent upon its submission of a written statement agreeing not to obtain data and information from the Providing Agency through remote electronic means until such time as the liquidated damages are paid in full. Such statement shall be signed by the Requesting Party's or Third Party End User's authorized representative and shall be submitted to the Providing Agency within five days of receipt of notices that damages are being assessed.

B. **Corrective Action Plan (CAP)**

1. If the Providing Agency determines that the Requesting Party or Third Party End User is out of compliance with any of the provisions of this MOU and requires the Requesting Party or Third Party End User to submit a CAP, the Providing Agency may require the Requesting Party or Third Party End User to submit the CAP within a specified timeframe. The CAP shall provide an opportunity for the Requesting Party or Third Party End User to resolve deficiencies without the Providing Agency invoking more serious remedies, up to and including MOU termination.

2. In the event the Providing Agency identifies a violation of this MOU, or other non-compliance with this MOU, the Providing Agency shall notify the Requesting Party or Third Party End User of the occurrence in writing. The Providing Agency shall provide the Requesting Party or Third Party End User with a timeframe for corrections to be made.

3. The Requesting Party or Third Party End User shall respond by providing a CAP to the Providing Agency within the timeframe specified by the Providing Agency.

4. The Requesting Party or Third Party End User shall implement the CAP only after the Providing Agency's approval.

5. The Providing Agency may require changes or a complete rewrite of the CAP and provide a specific deadline.

6. If the Requesting Party or Third Party End User does not meet the standards established in the CAP within the agreed upon timeframe, the Requesting Party or Third Party End User shall be in violation of the provisions of this MOU and shall be subject to liquidated damages and other remedies including termination of the MOU.

7. Except where otherwise specified, liquidated damages of $25.00 per day may be imposed on

the Requesting Party or Third Party End User for each calendar day that the approved CAP is not implemented to the satisfaction of the Providing Agency.

IX. Agreement Term

This MOU shall take effect upon the date of last signature by the Parties and shall remain in effect for six (6) years from this date unless terminated or cancelled in accordance with Section XI, Termination and Suspension. Once executed, this MOU supersedes all previous agreements between the parties regarding the same subject matter.

X. Amendments

This MOU incorporates all negotiations, interpretations, and understandings between the Parties regarding the same subject matter and serves as the full and final expression of their agreement. This MOU may be amended by written agreement executed by and between both Parties. Any change, alteration, deletion, or addition to the terms set forth in this MOU, including to any of its attachments, must be by written agreement executed by the Parties in the same manner as this MOU was initially executed. If there are any conflicts in the amendments to this MOU, the last-executed amendment shall prevail. All provisions not in conflict with the amendment(s) shall remain in effect and are to be performed as specified in this MOU.

XI. Termination and Suspension

A. This MOU may be unilaterally terminated for cause by either party upon finding that the terms and conditions contained herein have been breached by the other party. Written notice of termination shall be provided to the breaching party; however, prior-written notice is not required, and notice may be provided upon cessation of work under the agreement by the non-breaching party.

B. In addition, this MOU is subject to unilateral suspension or termination by the Providing Agency without notice to the Requesting Party or Third Party End User, as applicable, for failure of the Requesting Party or Third Party End User to comply with any of the requirements of this MOU, or with any applicable state or federal laws, rules, or regulations, including, but not limited to, DPPA, Sections 119.0712(2), 322.142 or 501.171, Florida Statutes, or any laws designed to protect driver privacy.

C. This MOU may also be cancelled by either party, without penalty, upon thirty (30) business days advanced written notice to the other party. All obligations of either party under the MOU will remain in full force and effect during the thirty (30) business day notice period.

D. This MOU may be terminated by the Providing Agency if the Requesting Party, the Third Party End User, or any of its executive leadership, are found by a court of competent jurisdiction to have violated any provision of any state or federal law governing the privacy and disclosure of Personal Identifiable Information. The Requesting Party and Third Party End User must report such finding within five (5) business days and will have ten (10) business days from any action described above to provide mitigating information to the Providing Agency. If submitted timely, the Providing Agency will take the mitigation into account when determining whether termination of the MOU is warranted.

XII. Notices

Any notices required to be provided under this MOU shall be sent via Certified U.S. Mail and

email to the following individuals:

For the Providing Agency:

Chief, Bureau of Records
2900 Apalachee Parkway
Tallahassee, Florida 32399
Tel: (850) 617-2702
Fax: (850) 617-5168
E-mail: DataListingUnit@flhsmv.gov

For the Requesting Party:

Requesting Party Business Point-of-Contact listed on the signature page.

For the Third Party End User:

Third Party End User Business Point-of-Contact listed on the signature page.

XIII. Additional Database Access/Subsequent MOU's

The Parties understand and acknowledge that this MOU entitles the Requesting Party or Third Party End User to specific information included within the scope of this MOU. Should the Requesting Party or Third Party End User wish to obtain access to other Personal Identifiable Information not provided hereunder, the Requesting Party or Third Party End User will be required to execute a subsequent MOU with the Providing Agency specific to the additional information requested. All MOU's granting access to Personal Identifiable Information will contain the same clauses as are contained herein regarding audits, report submission, and the submission of Certification statements.

The Providing Agency is mindful of the costs that would be incurred if the Requesting Party or Third Party End User was required to undergo multiple audits and to submit separate certifications, audits, and reports for each executed MOU. Accordingly, should the Requesting Party or Third Party End User execute any subsequent MOU's with the Providing Agency for access to Personal Identifiable Information, while the instant MOU remains in effect, the Requesting Party or Third Party End User may submit a written request, subject to Providing Agency approval, to submit one of each of the following covering all executed MOU's: Certification; Audit; and/or to have conducted one comprehensive audit addressing internal controls for all executed MOU's. The Providing Agency shall have the sole discretion to approve or deny such request in whole or in part or to subsequently rescind an approved request based upon the Requesting Party's or Third Party End User's compliance with this MOU and/or any negative audit findings.

XIV. Public Records Requirements

The parties to this MOU recognize and acknowledge that any agency having custody of records made or received in connection with the transaction of official business remains responsible for responding to public records requests for those records in accordance with applicable law (specifically, Chapter 119, Florida Statutes) and that public records that are exempt or confidential from public records disclosure requirements will not be disclosed except as authorized by law.

If the Requesting Party, or Third Party End User is a "contractor" as defined in Section

119.0701(1)(a), Florida Statutes, the Requesting Party agrees to comply with the following requirements of Florida's public records laws:

A. Keep and maintain public records required by the Providing Agency to perform the service.

B. Upon request from the Providing Agency's custodian of public records, provide the Providing Agency with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes, or as otherwise provided by law.

C. Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the contract term and following completion of the contract if the Requesting Party does not transfer the records to the Providing Agency.

D. Upon termination or expiration of the MOU, the Requesting Party and/or Third Party End User agrees they shall cease disclosure or distribution of all data and information provided by the Providing Agency. In addition, the Requesting Party agrees that all data and information provided by the Providing Agency remains subject to the provisions contained in DPPA and Sections 119.0712, 322.142, and 501.171, Florida Statutes.

IF THE REQUESTING PARTY AND/OR THIRD PARTY END USER HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE REQUESTING PARTY'S OR THIRD PARTY END USER'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (850) 617-3101, OGCFiling@flhsmv.gov, OFFICE OF GENERAL COUNSEL, 2900 APALACHEE PARKWAY, and STE. A432, TALLAHASSEE, FL 32399-0504.

REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK

Signature Page for Third Party End User

THIRD PARTY END USER:

Third Party End User Agency Name

Street Address

Suite

City State Zip Code

BY:

Signature of Authorized Official

Printed/Typed Name

Title

Date

Official Third Party End User Email Address

Phone Number

BUSINESS POINT-OF-CONTACT:

Printed/Typed Name.

Official Third Party End User Email Address

Phone Number Fax Number

TECHNICAL POINT-OF-CONTACT:

Printed/Typed Name

Official Third Party End User Email

Phone Number Fax Number

REQUESTING PARTY UTILIZED:

Pinellas County Sheriff's Office

Printed/Typed Name

PROVIDING AGENCY:

Florida Department of Highway Safety and Motor Vehicles
Providing Agency Name

2900 Apalachee Parkway
Street Address

Suite

Tallahassee, Florida 32399
City State Zip Code

BY:

Signature of Authorized Official

Printed/Typed Name

Title

Date

Official Providing Agency Email Address

Phone Number

ATTACHMENT I

FLORIDA DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES Request For Exempt Personal Information In A Motor Vehicle/Driver License Record

The Driver's Privacy Protection Act, 18 United States Code sections 2721("DPPA") makes personal information contained in motor vehicle or driver license records confidential and exempt from disclosure. Personal information in a motor vehicle or driver license record includes, but is not limited to, an individual's social security number, driver license or identification number, name, driver license photograph, date of birth, height, race, gender, address and, medical or disability information. Personal information from these records may only be released to individuals or organizations that qualify under one of the exemptions provided in DPPA, which are listed on the back of this form.

I am a representative of a Requesting Party or Third-Party End User requesting personal information for one or more records as described below. I declare that my agency is qualified to obtain personal information under exemption number(s) _____, as listed on page 3 of this form.

I understand that I shall not use or redisclose this personal information except as provided in DPPA and that any use or redisclosure in violation of these statutes may subject me to criminal sanctions and civil liability.

Complete the following for each DPPA exemption being claimed. (attached additional page, if necessary):

DPPA Exemption Claimed:	Description of How Requesting Party Qualifies for Exemption:	Description of how Data will be used:

Obtaining personal information under false pretenses is a state and federal crime. Under penalties of perjury, I declare that I have read the foregoing Request For Exempt Personal Information in A Motor Vehicle/Driver License Record and that the facts stated in it are true and correct.

_____ _____
Signature of Authorized Official

_____
Title

_____
Printed Name

_____
Name of Agency/Entity

_____
Date

STATE OF FLORIDA
COUNTY OF_____

Sworn to (or affirmed) and subscribed before me this _____ day of _____, 20___, by _____.

Personally Known _____ OR Produced Identification _____
Type of Identification Produced_____

_____
NOTARY PUBLIC (print name)

_____
NOTARY PUBLIC (sign name)
My Commission Expires: _____

Pursuant to section 119.0712(2), F. S., personal information in motor vehicle and driver license records can be released for the following purposes, as outlined in 18 United States Code, section 2721.

Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. 1231 et seq.), the Clean Air Act (42 U.S.C. 7401 et seq.), and chapters 301, 305, and 321-331 of title 49, and, subject to subsection (a)(2), may be disclosed as follows.

1. For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.

2. For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.

3. For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only -
(a) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and
(b) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.

4. For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

5. For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.

6. For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.

7. For use in providing notice to the owners of towed or impounded vehicles.

8. For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.

9. For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.

10. For use in connection with the operation of private toll transportation facilities.

11. For any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains.

12. For bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.

13. For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.

14. For any other use specifically authorized under the law of the State that holds the record if such use is related to the operation of a motor vehicle or public safety.

BIOMETRIC FACIAL ANALYSIS SYSTEM

QUARTERLY QUALITY CONTROL REVIEW REPORT

Pursuant to your Memorandum of Understanding (MOU), the Business Point of Contact (POC) must complete and keep a copy of this form along with the items listed below for six years:

- Maintain a list of all users who have access to the Biometric Facial Analysis System.
  - Update any user information, document the reason for the change in access, and the date the change is made.
  - Verification that user access/permissions, including Third Party End Users, is immediately inactivated following separation or negligent, improper, or unauthorized use or dissemination of any information.

- Maintain documentation verifying that usage has been internally monitored to ensure proper, authorized use and dissemination. This includes verification that each inquiry has an associated investigative case number, if required by the MOU.
  - **Please note:** DHSMV highly recommends the agency audit users as frequently as possible to ensure misuse is not occurring.

- Each quarter, complete the report below and ensure all actions are documented.

Quarter:	Year:
Total active users in the system:	
Users inactivated during quarter:	
Users audited during quarter:	
Total number of cases of misuse found:	
Total cases of misuse reported pursuant to *Section VII. Compliance and Control Measures, Part C.* of the MOU:	

_____ _____

POC Signature Date

_____

POC Name Printed