MEMORANDUM OF UNDERSTANDING
FOR ACCESS TO BIOMETRIC FACIAL ANALYSIS SYSTEM

This Memorandum of Understanding (MOU) is made and entered into by and between the City of North Port, 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:

City of North Port
Third Party End User Agency Name

4970 City Hall Boulevard
Street Address

Suite

North Port FL 34286
City State Zip Code

BY:

Signature of Authorized Official

Todd R. Garrison
Printed/Typed Name

Chief of Police
Title

09/09/2020
Date

tgarrison@northportpd.com
Official Third Party End User Email Address

941-429-7306
Phone Number

BUSINESS POINT-OF-CONTACT:

Michael Baute
Printed/Typed Name

mbaute@northportpd.com
Official Third Party End User Email Address

941-429-7412 / 941-429-7389
Phone Number Fax Number

TECHNICAL POINT-OF-CONTACT:

Commander John McDowel
Printed/Typed Name

jmcdowell@northportpd.con
Official Third Party End User Email

941-429-7357 / 941-429-7.89
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) 1_____, 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:
1	The CIty of North Port Police Department is a law enforcement agency in the state of Florida.	The North Port Police have a MOU with the Pinellas County Sheriff's Office for the FACES software run/hosted by PCSO. The North Port access DHSMV drivers license photographs via the FACES software for facial comparisons. This software is ONLY used for criminal investigations and is user access is audited monthly to ensure proper use.

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.

_____ Chief of Police

Signature of Authorized Official | Title

Todd R. Garrison | North Port Police Department

Printed Name | Name of Agency/Entity

09/09/2020

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.

Department of Highway Safety and Motor Vehicles

Prepared By:
Office of Enterprise Security Management

External Information Security Policy

Revision History

Version	Author	Release Notes	Issue Date
1.2*	Joe Cipriani	Baseline document	9/30/2015
1.21	Tom Trunda	Add definitions and clarifications	03/17/2016
2.0	Scott Morgan and Carl Ford (HSMV) in conjunction with the Tax Collector InfoSec Coalition - Terry Skinner, Kirk Sexton, Dan Andrews and the Honorable Ken Burton Jr., Tax Collector, Manatee County	Revised to align with Department policies in congruence with requirements for External Entities. Added scope for further clarification and applicability. Revised to align with Rule 74-2, F.A.C., Information Technology Security	08/18/2017
2.0	Scott Morgan	Removed draft watermark, formatting check; added statutory reference for F.S., 282.318 in the footer, added effective issue date	12/7/2017

* Note: The document version coincides with the IT Security Policy Manual.

External Information Security Policy

Scope:

This policy applies to all agents, vendors, contractors and consultants (External Entities) who use and/or have access to Department information resources. External Entities who use and/or have access to Department information resources shall adhere to the policies outlined herein. The authority for these policies derives from Florida Statutes 282.318, Security of Data and Information Technology Resources and Florida Administrative Code Chapter 74-2, Information Technology Security.

#A-02: Data Security	Review Date: 08/18/17	Issue Date: 12/01/08	Revised Date: 08/18/17

#A-02: Data Security

1.0 Purpose
To ensure that data is protected in all forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This includes any system or process which accesses the State of Florida telecommunications network, or Department information resources, and trusted partners including, but not limited to AAMVA, FDLE and CJIS networks and data.

2.0 Policy
Other than data defined as public**,** which may be accessible to public access inquiries (as well as authenticated users), all data and system resources are only accessible on a need-to-know basis to specifically identified, authenticated, and authorized entities.

3.0 Data Usage
All users who access Department data must do so only in conformance with this policy. Only uniquely identified, authenticated, and authorized users are allowed access to the Department data, excluding public access inquiries. Access control mechanisms must be utilized to ensure that users can access only that data to which they have been granted explicit access rights.

Information resources are strategic assets vital to the business performance of the Department. These strategic assets must be protected commensurate with their tangible value, legal and regulatory requirements, and their critical role in the Department's ability to conduct its mission. Ownership and management of these information resources reside with the Department, and not to any individual or group of individuals.

4.0 Data Storage or Transmission
All users who are responsible for the secure storage or transmission of the Department's data must do so only in conformance with this policy. Where confidentiality, privacy or sensitivity requires, stored or transmitted data must be secured via Department-approved encryption technology. This does not supersede provisions of the Public Records Act that states, "computer records are public records," but serves to protect data while stored.

5.0 Data Disposal
Access control mechanisms must be utilized to ensure that, during the disposal process, users can access only data to which they have been granted explicit access rights. External Entities shall follow an established process approved by the Department for the disposal of data to include the disposal of confidential data in accordance with The Florida Public Records Act and Federal Standards.

6.0 Management Responsibilities
Network operations and systems administration personnel shall ensure that adequate logs and audit trails are maintained. Logs and audit trails must at a minimum record access to data, records, and activation of industry recognized security mechanism for protection of confidential and sensitive data.

7.0 Data Classification

The Department is responsible for classification of data. External Entities are required to abide by data classification requirements as outlined by the Department. Data classification shall be done in accordance with Federal Information Processing Standards (FIPS) Publication 199 and is necessary to enable the allocation of resources for the protection of data assets, as well as determining the potential loss or damage from the corruption, loss, or disclosure of data. To ensure the security and integrity of all data, any data asset is Public, Sensitive or Confidential and should be labeled accordingly.

All data falls into one of the following categories:

- Public:
  Information or data that is not classified as sensitive or confidential. Information that, if disclosed outside the State or agency, would not harm the State or Department, its employees, customers, or business partners. This data may be made generally available without specific data custodian approval.

- Sensitive**:**
  Information not approved for general circulation outside the State or Department where its loss would inconvenience the State/Department or management but disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include internal memos, minutes of meetings, and internal project reports. Security at this level is controlled but normal.

- Confidential**:**
  - Data that, by its nature, is exempt from disclosure under the requirements of Chapter 119, F.S.
  - Data whose loss, corruption, or unauthorized disclosure would be a violation of federal or State laws/regulations. Information of a proprietary nature. Procedures, operational work routines, project plans, designs, or specifications that define the way in which the organization operates.
  - Data whose loss, corruption, or unauthorized disclosure would tend to impair business functions or result in any business, financial, or legal loss.
  - Data that involves issues of personal credibility, reputation, or other issues of privacy.
  - Highly sensitive internal documents that could seriously damage the State or Department if such information were lost or made public. Information usually has very restricted distribution and must be protected at all times.

8.0 Web Services and Data Exchanges

The Department has created online web-based services and data exchanges which may be utilized by Tax Collectors and authorized Vendors who meet various technical standards, requirements, and statutory authority. The specific standards, requirements, and conditions for use of the aforementioned web services and data exchanges are outlined in the individual Memorandum of Understanding (MOU) for each service offered. The terms and conditions of the MOU shall govern the applicable use, timeframe, and requirements of each web service and data exchange.

#A-04: Passwords	Review Date: 08/18/17	Issue Date: 12/01/08	Revised Date: 08/18/17

#A-04: Passwords

1.0 Purpose

To ensure the processes for password creation, distribution, changing, safeguarding, termination, and recovery adequately protect information resources.

2.0 Policy and Standards

Passwords are unique strings of characters that personnel or information resources provide in conjunction with a logon ID to gain access to an information resource. Passwords, which are the first line of defense for the protection of the Departments information resources, shall be treated as confidential information and must not be divulged.

1. All user accounts used to access the Department information resources shall have passwords of sufficient strength and complexity, and be implemented based on system requirements and constraints, and in accordance with the following rules to ensure strong passwords are established:
   - Shall be routinely changed at an interval not greater than 90 days.
   - Shall be different than the last 10 passwords.
   - Shall adhere to a minimum length of 8 characters.
   - Shall be a combination of alpha (upper and lower case), numeric, and special characters (unless a particular system does not allow, passwords shall consist of at least 3 of the above 4 categories).
   - Should not be anything that can be easily guessed or associated to the account owner such as: user name, social security number, nickname, relative's names, pet's names, birth date, sports team, etc.
   - Should not be dictionary words or acronyms.
   - Newly created or reset passwords must be randomly generated. Use of a default or standard new/reset password is prohibited.
2. Stored passwords shall be encrypted.
3. Passwords shall not be divulged to anyone. Passwords must be treated as confidential information and shall be safeguarded.
4. Passwords and user names shall not be shared with anyone to include co-workers or contractors. Passwords must be treated as confidential information. Credentials (UserID and passwords) are for exclusive use only by the user to which they are assigned.
5. All users are responsible for the work performed under their credentials (User Id and password). Allowing other users to use your computer while you are logged on is strictly prohibited. Approved exceptions are:
   - Initial System Configuration
   - System Support
   - Troubleshooting Activities

6. If the security of a password is in doubt, the password must be changed immediately.
7. Administrators shall not circumvent this policy solely for ease of use.
8. Users shall not circumvent password entry with auto logon, application remembering, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Department's ISM. For an exception to be approved, there must be a procedure to change the password.
9. Computing devices shall not be left unattended without enabling a password-protected screensaver that is activated after 15 minutes of inactivity, or logging off the device.
10. User accounts must be locked after 5 unsuccessful login attempts.
11. Passwords must not be transmitted via e-mail or other forms of electronic communication.
12. Passwords must be encrypted during transmission and storage using appropriate encryption technology.
13. Passwords should not be written down and stored at your workstation in your office.
14. Passwords stored on physical media must be protected by an encryption technology outlined in Policy #B-01 Acceptable Encryption.
15. Initial use passwords that have been assigned must expire at the time of first use in a manner that requires the password owner to supply a new password, provided that this functionality is available within that particular product or facility.
16. For all password resets, the identity of the person requesting the password reset must be verified.

#B-01: Acceptable Encryption	Review Date: 08/18/17	Issue Date: 12/01/08	Revised Date: 08/18/17

#B-01: Acceptable Encryption

1.0 Overview
To establish policy that directs the use of encryption to provide adequate protection of data where required. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is obtained for the dissemination and use of encryption technologies outside of the United States.

2.0 Purpose
To ensure the confidentiality, integrity and availability of data is maintained for Department data and information resources.

3.0 Scope
In the event encryption is required for the transmittal of confidential information, the encryption methodology shall be coordinated with the Department's ISM for the management of secure escrow and storage of encryption keys.

4.0 Policy
Encryption is the primary means for providing confidentiality for information that can be stored or transmitted, either physically or logically. When possible, confidential information should not be transmitted via email. If confidential information must be sent via email, it shall be encrypted. Information resources that stores or transmits sensitive or confidential data must have the capability to encrypt information.

Proven, standard algorithms must be used as the basis for encryption technologies. Encryption key lengths must be at least 128 bits. The Department key length requirements will be reviewed periodically and upgraded as technology, legislation, or business needs requires.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by and approved by the Department's ISM. It should be noted that the U.S. Government restricts the export of encryption technologies. Potential users of the Department information resources in countries outside the United States should make themselves aware of the encryption technology laws of those countries.

#B-02: Access Control

1.0 Purpose

To protect the Department's information resources from threats of unauthorized access, disclosure, modifications, or destruction.

2.0 Policy

1. Each user accessing a Department information resource shall be assigned a unique personal identifier, commonly referred to as either a user account, Logon ID, user identification, or User ID. Exceptions: public systems where such access is authorized or for situations where risk analysis by the Department demonstrates such use to be applicable and appropriate. (Example: DL check on the DHSMV website)
2. Users shall not under any circumstances use another user's account logon or credentials.
3. User access rights shall be established based on approved written requests. The user identification shall be traceable to the user for the lifetime of the records or reports in which they appear.
4. A user's access shall be promptly disabled and/or removed from systems which access Department information resources, when access is no longer required. Examples include, but are not limited to, termination, transfer, or removal of the duties that require access. Notification of changes in the status of users with established Department credentials is the responsibility of the authorizing External Entity to report such changes to the Department.
5. Each user shall agree in writing to use the access only for the purpose intended.
6. An automatic workstation time-out shall occur no later than 15 minutes after inactivity. A password shall be required to unlock the user account. User accounts shall be locked after 5 unsuccessful attempts.
   Exception: In the interest of officer safety, devices that are part of a law enforcement vehicle or are used to conduct dispatch functions and are within a physically secure location are exempt from this requirement. However, these devices shall be logged off or locked if they are left unattended.
7. External Entities must monitor the access rights of those whom they have authorized.
8. Established controls must ensure that Department information resources are accessed only by users authorized to do so.
9. Access to accounts with elevated access rights shall follow the principle of least-privilege, and should be restricted to systems personnel only; usage of these accounts shall be logged and subject to audit.
10. Administrative access shall incorporate Separation of Duties to ensure no individual has the ability to control an entire process.
11. Access rights to Department information resources by systems personnel shall be based on specific job requirements. Responsibility for production processing must be separated from

system development, testing and maintenance. Systems or development personnel should only access production data to resolve emergencies.

12. All development and testing shall be performed on test data and not utilize the Department's production data. Test systems shall be kept physically or logically separate from production systems. However, in some instances there is a need to access the Department's production data in a test environment, which requires an exception from the Department's CIO and ISM. The production environment shall not be adversely affected and data shall not be altered. Security controls that provide restricted access and auditing shall not be disabled or removed. Confidential or exempt data shall not be used in any test system.
13. The Department utilizes the principle of least privilege for access control to information resources. All External Entities shall be limited to the access required to do their assigned tasks.
14. Support personnel utilizing remote access to Department information resources for the purpose of providing technical support shall use RDP (Remote Desktop Protocol) or Windows Remote Assistance, or a remote access product approved by the Department's ISM. The following requirements must be met:
    - Remote connectivity must be done in a secure fashion.
    - Remote access must be granted by the end-user or system administrator before a remote session can be initiated.
    - Remote session must be monitored at all times for the duration of the session.
    - Remote session must be terminated immediately upon completion of authorized tasks.

#B-03: Account Management for User Accounts

1.0 Purpose

To ensure that user accounts which access Department information resources are created, maintained, monitored, and removed in a manner that protects Department information resources and user access privileges.

2.0 Background

Computer user accounts are the means used to grant access to the Department's information resources. These accounts provide accountability, a key to the Department's computer security program for information resource usage. Creating, controlling, and monitoring all computer user accounts is extremely important for the Department's information resources.

3.0 Policy

1. All accounts created must have an associated request and approval that is appropriate for the Department's information resource or service.
2. External Entities must complete Information Security Training on the Department's PartnerNet Portal within 30 days of receiving their account or risk having access terminated.
3. All accounts must be uniquely identifiable using the assigned user name. User accounts and the associated passwords constitute a user's credentials and shall never be shared.
4. All default passwords for accounts must comply with password policy # A-04.
5. All accounts must have a password expiration that complies with password policy # A-04.
6. The appropriate system administrator or other designated staff should disable accounts of individuals on extended leave. Extended leave is defined as greater than 60 days.
7. External Entity user accounts established by the Department that have not been accessed within 30 days are subject to being disabled.
    a. External Entities' System Administrators are responsible for modifying the accounts of individuals that change duties or are separated from their relationship with the External Entity upon notification of change or separation.
    b. Must have a documented process to modify a user account to accommodate situations such as name changes, account changes, and permission changes.
    c. Must have a documented process for periodically reviewing existing accounts for validity.
    d. Department information resources utilized by External Entities are subject to independent audit review of user account management.
    e. Must provide a list of accounts for the systems they administer when requested by authorized Department management.
    f. Must cooperate with authorized Department management investigating security incidents.

#B-06: Application Service Provider

1.0 Purpose

To define minimum security requirements for an Application Service Provider (ASP) to the Department. This policy applies to ASPs that are either being considered for use by the Department or its agent, or have already been selected for use.

2.0 Policy and Standards

1. General Security:

    a. The Department reserves the right to audit the infrastructure utilized by the ASP to ensure compliance with this policy. Non-intrusive network audits (basic port scans, etc.) may be performed.
    b. The ASP must provide a proposed architecture document that includes a full network diagram of the Department Application Environment (initially provided to ASP by the Department), illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart that details where Department data resides, the applications that manipulate it, and the security thereof.
    c. The ASP must be able to immediately disable all or part of the functionality of the application should a security issue be identified.
    d. Exceptions to this policy require prior approval by the Department's ISM and CIO who will evaluate requests on a case-by-case basis.
    e. The ASP must certify compliance to these requirements in writing annually.
    f. The ASP must identify their ISM and provide the Department and authorizing External Entity with contact information.

Physical Security:

a. The ASP's application infrastructure (hosts, network equipment, etc.) must be located in a physically secure facility and in a locked environment.

b. The ASP must disclose who amongst their personnel will have access to the environment hosting the application for the authorizing External Entity.

c. The Department requires that the ASP disclose their ASP background check procedures and results prior to the Department's ISM approval.

3. Network Security:

    a. The network hosting the application must be logically or physically separated from any other network or customer that the ASP may have. This means the authorizing External Entity's application environment must use logically or physically separated hosts and infrastructure.

    b. Data flow between the authorizing External Entity and the ASP:

        - If the Department or the authorizing External Entity will be connecting to the ASP via a private circuit, then that circuit must terminate on the authorizing External Entity's infrastructure, and the operation of that circuit will adhere to this policy.

- If the data between the authorizing External Entity and the ASP traverses a public network such as the Internet, the ASP must deploy appropriate firewall technology, and the traffic between the authorizing External Entity and the ASP must be protected and authenticated by cryptographic technology.

4. Host Security:
   a. The ASP must disclose how and to what extent the hosts or servers (Unix, Windows, etc.) comprising its application infrastructure have been hardened against potential threats and attack vectors. The ASP shall provide any hardening documentation it has for the Department or authorizing External Entity's application infrastructure as well.
   b. The ASP must provide a methodology and plan for ensuring systems are patched or updated according to industry best practices and guidelines. Patches include, but are not limited to, host OS, web server, database, and any other system or application.
   c. The ASP must disclose its processes for monitoring the confidentiality, integrity and availability of those hosts.
   d. The ASP must provide to the Department information on its password policy for the application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.
   e. The ASP must provide information on account creation, maintenance, and termination processes, for service, system, and user accounts. This should include information as to how an account is created, how account information is communicated to the user, and how accounts are terminated when no longer needed.
5. Web Security:
   a. The ASP will disclose the use of various web architecture and programming languages, including, but not limited to Java, JavaScript, ActiveX, PHP, Python, C, Perl, VBScript, etc.
   b. The ASP will describe the process for performing security quality assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, or any other activity designed to validate the security architecture.
   c. The ASP will disclose the methodology utilized for web code reviews, including CGI, Java, etc., for the explicit purposes of finding and remediating security vulnerabilities, the authorizing party who performed the review, results of the review, and what remediation activity has taken place.
6. Encryption:
   a. The Department's application data in the custody of the authorizing External Entity must be stored and transmitted using acceptable encryption technology as outlined in Policy #B-01, Acceptable Encryption.
   b. Connections to the ASP utilizing the Internet must be protected using any of the following encryption technologies: IPsec, TLS, SSH/SCP, PGP, or any other encryption technologies approved by the Department's ISM.

#B-10: Incident Handling (Security Incidents)

1.0 Purpose

To ensure that computer security incidents which impacts, or has the potential to impact the confidentiality, integrity, and availability of the Department's information resources are properly recorded, communicated and remediated. Security incidents include, but are not limited to: virus and malware detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of information resources.

2.0 Policy

Information security incidents are events involving the Department's information resources, systems, or data, whether suspected or proven, deliberate or inadvertent, that threatens the confidentiality, integrity, and availability, of the Department's information resources. The reporting of incidents enables the Department to review the security controls and procedures; establish additional, appropriate corrective measures, if required, and reduce the likelihood of recurrence.

1. The Department's ISM is responsible for the coordination of any security incident that occurs.

2. Whenever a security incident, such as a virus, Denial of Service, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed that impacts or has the potential to impact the Department's information resources, the Department's ISM must be notified immediately and the appropriate incident management procedures must be followed.

   Reportable Incidents:
   Reportable incidents include, but are not limited to, the following:
   - Physical loss, theft, or destruction of the Department's information resources.
   - Unauthorized disclosure, modification, misuse, or disposal of sensitive, critical, or business-controlled information.
   - Suspected or known unauthorized internal or external access activity, including, but not limited to, sharing of user credentials and accounts must be reported immediately.
   - Unauthorized activity or transmissions using Department information resources.
   - Internal/external intrusions/interference with Department networks (denial of service attacks, unauthorized activity on restricted systems, unauthorized modification or deletion of files, or unauthorized attempts to control information resources.
   - Editing of files when no changes in them should have occurred.
   - Appearance / disappearance of files, or significant /unexpected changes in file size.
   - Systems that display strange messages or that mislabel files and directories.
   - Data that has been altered or destroyed or access that is denied outside of normal business procedures.
   - Detection of unauthorized personnel in controlled information security areas.
   - Lost security tokens, smart cards, identification badges, or other devices used for identification and authentication shall be reported immediately.
   - Fraud, embezzlement, and other illegal activities.
   - Violation of any portion of the External Information Security Policy.

#B-20: Security Monitoring and Auditing	Review Date: 08/18/17	Issue Date: 12/01/08	Revised Date: 08/18/17

#B-20: Security Monitoring and Auditing

1.0 Purpose

To ensure that information resource security controls required to protect the Department's information resources are established, effective, and are not being bypassed. This policy defines the requirements and provides the authority for the Department's ISM, and Enterprise Security Management Team (ESM) to conduct audits and risk assessments to ensure integrity of information resources, to investigate incidents, to ensure conformance to security policies, or to monitor user/system activity where appropriate. This section applies to monitoring inbound and outbound traffic to/from External Entities, agents, and trusted partners' networks and environments. External Entities who access or utilize Department information resources are subject to independent audit review.

2.0 Background

Security monitoring allows the Department to detect and mitigate illicit or fraudulent activity as early as possible, therefore limiting the risk of exposure or compromise. Security monitoring can assist in identification and remediation of new security vulnerabilities or emerging threats. This early identification can assist in preventing, or limiting harm to Department information resources.

3.0 Policy

1. Security monitoring will be used as a method to confirm that security practices, controls, and policies are functional, adhered to, and are effective.

2. Monitoring consists of activities such as the periodic review of:
   a. Automated intrusion detection system logs
   b. Firewall logs
   c. User account logs
   d. Network scanning logs
   e. Application logs
   f. Data backup recovery logs
   g. Technical Assistance Center (TAC) logs

3. Audits may be conducted to:
   a. Ensure integrity, confidentiality and availability of the Department's information resources
   b. Investigate possible security incidents
   c. Ensure conformance to the Department's security policies
   d. Monitor user or system activity where appropriate

4. The Department shall use automated tools to provide real time notification of detected anomalies or vulnerability exploitation. These tools will be deployed to monitor network traffic and/or operating system security parameters.

5. The following files may be checked for signs of misuse, fraudulent activity, and vulnerability exploitation periodically, or as requested for investigative purposes:
   a. Automated intrusion detection system logs
   b. Firewall logs

c. User account logs
d. Network scanning logs
e. System error logs
f. Application logs
g. Data backup and recovery logs
h. Telephone activity – Call Detail Reports

6. The following audit review may be performed periodically or upon request by assigned technical staff:
   a. Password strength
   b. Unauthorized network devices
   c. Unauthorized personal web servers
   d. Unsecured sharing of devices
   e. Unauthorized modem use
   f. Operating system and software licenses
   g. Unauthorized wireless access points

7. When requested, and for the purpose of performing an audit, any access needed will be provided to members of ESM as designated by the Department's ISM. This access may include:

   a. User level and/or system level access to any computing or communications device
   b. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on the Department's information resources
   c. Access to work areas that access or process Department information resources
   d. Access to interactively monitor and log traffic on the Department's networks.

8. Any security issues discovered will be reported to the Department's ISM for follow-up review and possible improvement to security settings.

#B-23: Network Interconnectivity	Review Date: 08/18/17	Issue Date: 12/01/08	Revised Date: 08/18/17

#B-23: Network Interconnectivity

1.0 Purpose

To ensure that interconnection of External Entities' networks to the Department's networks does not compromise the security of the Department's information resources.

2.0 Policy

1. Access to the Department's networks via External Entities' networks shall be protected via firewall or firewall features. No network connection between the Department's network and an external network shall be permitted without the use of firewall features to the appropriate degree based on level of risk, as determined by ISA, in conjunction with the Department's ISM.

2. Access to devices (servers) within the confines of the Department's core network from External Entities' networks shall be limited to the minimum manageable set of users/connections, as determined by ISA in conjunction with the Department's ISM, via firewall features.

3. All External Entities' network connections must meet the requirements of the Florida Information Resource Security Policies and Standards (Rule 74-2). Blanket access is prohibited and the principle of least privilege shall apply. Interconnectivity is limited to services, devices, and equipment needed.

   External Entity Agreements:

   a. All External Entities that desire to connect their networks to the Department's network for the purpose of retrieving Motor Vehicle and Driver License information must complete and submit to the Department the agreement(s) governing External Entity connections.
   b. In addition to the agreement, the External Entity shall be required to submit the Entity's name, address, phone number, fax number, email address, a technical contact's name, phone number, fax number and email address. The Department may request and obtain additional information from the External Entity.
   c. The Department's External Entity connection agreements shall determine the responsibilities of the External Entity, including approval authority levels and all terms and conditions of the agreement.
   d. All External Entities shall implement a binding Memorandum of Understanding, or where applicable, a Management Control Agreement (ex. Entity that manages CJIS data or systems) to ensure appropriate security controls are established and maintained by their trusted partner and agents.

#B-24: Malware/Virus Protection	Review Date: 08/18/17	Issue Date: 12/01/08	Revised Date: 08/18/17

#B-24: Malware/Virus Protection

1.0 Purpose

To ensure the Department's information resources are protected from computer threats, including but not limited to viruses, worms, malware, and other threats of malicious software designed to compromise system confidentiality, integrity, and availability. As a part of the Department's information security program, information resources must receive adequate protection against viruses and malware. External Entities which access and or utilize the Department's information resources are required to adhere to this policy.

2.0 Policy

1. All computing devices (workstations, servers, laptops, tablets, etc.) whether connected to the Department's network or storing Department data, must utilize a Department approved virus protection system. The Department's ISM will maintain a list of approved protection vendors. Exceptions to this list will be considered for approval by the Department's ISM on a case-by-case basis.

2. The virus protection system must be enabled on workstations and servers at start-up, employ resident scanning, and never be disabled or bypassed for production usage. The settings for the virus protection system must not be altered in a manner that will reduce the effectiveness of the system.

3. External Entities which access and utilize the Department's information resources are required to update virus signature files immediately upon release.

4. The automatic update frequency of the virus protection system must not be altered to reduce the frequency of updates. Each computing device which accesses Department information resources must utilize a Department approved virus protection system and setup to detect and clean viruses that may infect file shares.

5. External Entities which access or utilize the Department's information resources shall ensure that email is scanned to ensure email and attachments are free from malware and viruses.

6. Each virus, malware, or system exploit that impacts, or potentially impacts the Department's information resources constitutes a security incident and must be reported to the Department's ISM as outlined in #B-10, Incident Handling. The computing device shall be removed from the network until it is verified as free of viruses and malware, and coordinated with the Department's ISM.

Definitions	Review Date: 08/18/17	Issue Date: 8/18/17	Revised Date: 08/18/17

Term	Definition
Access	To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.
Air-Gap	An air gap is a network security measure, also known as air gapping, employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks.
Agent	Entity operating on the Department's behalf, but who is not an official Department member.
Application Service Provider (ASP)	ASP's combine hosted software, hardware and networking technologies to offer a service-based application, as opposed to a Department -owned and operated application. In some cases, systems provided by ASP's reside and operate from within the Department's data center environment. Common ASP offerings include enterprise resource planning (ERP), collaboration and sales force automation tools, but are not limited to these things. For example: Cloud Provider or Software as a Service Provider.
Audit	To examine or verify appropriate use of computing devices and the interconnectivity with External Entities. A Security audit may include **an** independent formal review and examination of system records and activities to (a) determine the adequacy of system controls, (b) ensure compliance with established security policy and operational procedures, (c) detect breaches in security, and (d) recommend any indicated changes in any of the foregoing.
Authentication	The process that verifies the claimed identify or access eligibility of a station, originator, or individual as established by an identification process.
Authorization	A positive determination by the information resource owner or delegated custodian that a specific individual may access that information resource, or validation that a positively identified user has the need and the owner's permission to access the resource.
Business Function	The business need that a software application satisfies. Managed by an ASP that hosts an application on behalf of the Department.
Chief Information Officer (CIO)	Responsible for the management of the Department's information resources. The Director of Information Systems Administration serves as the Department's CIO.
Client	A system that requests and uses the service provided by a "server".
Computer security	Measures that implement and assure security in a computer system, particularly those that assure access control; usually understood to include functions, features and technical characteristics of computer hardware and software, especially operating systems.
CJIS	Criminal Justice Information Systems. For purposes of this policy, CJIS data and systems process, store, or transmit criminal justice information (CJI).
Computing Device	Workstations, servers, laptops, tablets, etc. either connected to the Department's network or which store or process the Department's data.
Confidential information	Information that is exempted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Florida Public Records Act.
Credentials	The combination of User ID, or Logon ID and password constitute credentials assigned to an entity.
Custodian	Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. The custodian is normally a provider of services.
Data	A representation of facts or concepts in an organized manner that may be stored, communicated, interpreted, or processed by people or automated means.
Database	A set of related files that is created and managed by a database management system
Denial of service	The prevention of authorized access to a system resource or the delaying of system operations and functions.
Department	The Department of Highway Safety and Motor Vehicles.

Term	Definition
E-mail or email	Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application.
Encryption	Encryption is the conversion of data into a form, which cannot be easily understood by unauthorized people.
Extranet	Connections between third parties that require access to connections non-public DHSMV resources, as defined in the Network Support Organization's extranet policy.
External Entities	Agents, vendors, contractors and consultants who use and/or have access to Department information resources.
Firewall	A firewall is a safeguard or type of gateway that is used to control access to information resources. A firewall can control access between separate networks, between network segments, or between a single computer and a network. It can be a PIX, a router with access control lists or similar security devices approved by the Network Support Organization.
Host	A computer in a network that provides direct support functions, such as database access, application programs, and programming languages.
Incident (or breach)	An event that results in loss, unauthorized disclosure, unauthorized acquisition, unauthorized use, unauthorized modification, or unauthorized destruction of information resources whether accidental or deliberate.
Information Resources (IR)	For purposes of this policy, information resources are defined as Department owned assets (hardware, systems, software, and data) which are strategic assets vital to the business performance of the Department.
Information Security Manager (ISM)	The person designated to administer the Department's information resource security program in accordance with section 282.318(2)(a)1, Florida Statutes, and the Department's internal and external point of contact for all information security matters.
Information Systems Administration (ISA)	Entity responsible for computers, networking and data management.
Technical Assistance Center (TAC)	The ISA Section that receives requests for assistance from customers using Department computer equipment or network.
ISA	Information Systems Administration (within DHSMV).
IT (or IR)	Information Technology (or Information Resources). IT is a term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived).
Local Area Network (LAN)	Two or more computers and associated devices that share a common communications line within a small geographic area (for example, within an office building), for the purposes of sharing applications, peripherals, data files, etc.
Members	Employees of DHSMV.
Network	A combination of data circuits and endpoints that are utilized to transmit and receive information.
Password	A protected word or string of characters which serves as authentication of a person's identity ("personal password"), or an account identity ("service or system account") which is used to grant or deny access to private or shared data.
Physical Security	The protection of building sites and equipment (and information and software contained therein) from theft, vandalism, natural and manmade disasters, and damages, whether accidental or intentional.
Production or Production System	A system used to process an organization's daily work. It implies a real-time operation and the most mission critical systems in the enterprise.
Proprietary Encryption	Encryption technology that has not been made public and/or has not withstood public scrutiny. The developer of the encryption technology could be a vendor, an individual, or the government.
Provider	Third party such as a contractor, vendor, or private organization providing products, services and/or support.

Term	Definition
Remote Desktop Protocol (RDP)	Connection protocol that presents the screen of a remote computing device on a user's computer screen. The user's computer does not have physical access to the external network. The user will be able to use the remote computer as if they were sitting at it.
Risk analysis	A process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and recommends how to allocate resources to countermeasures so as to minimize total exposure.
Security Monitoring	Security monitoring is a process that assists in proactive identification and remediation of security vulnerabilities and threats. This early identification can assist in preventing, or limiting harm to Department information resources.
Sensitive Information	Information that is confidential or exempt from disclosure by federal or state law; information that requires protection from unauthorized access by virtue of its legal exemption from the Public Records Act.
Server	A physical or virtual computer/device that provides information or services on a network.
State	The government of the State of Florida.
System Administrator	Person responsible for the effective operation and maintenance of IT, including implementation of standard procedures and controls.
Test System	A system that mimics the production environment for the testing of system and application changes yet does not interfere with the production environment.
User	An individual who accesses or utilizes the Department's information resources.
Virus	A computer virus is a type of malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code. Infected computer programs can include data files or the "boot" sector of the hard drive.
Wireless Access Point	A wireless receiver, typically 802.1x, which provides connectivity, commonly referred to as "Wi-Fi" from wireless network devices to a wired network.
Worm	A worm is a malicious program that can self-replicate and actively transmit itself over a network to infect other computers.

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