FOLLOW ALL PROCEDURES ON BACK OF THIS FORM

Contract # 240076
Number Assigned by Purchasing Dept.

CONTRACT REVIEW

BOARD MEETING DATE:

WHEN BOARD APPROVAL IS REQUIRED DO NOT PLACE ITEM ON AGENDA UNTIL REVIEW IS COMPLETED

☐ Must Have Board Approval over $100,000.00

Date Submitted: 10/11/23

Name of Contract Initiator: Randall Crawford Telephone #: 904-336-0002

School/Dept Submitting Contract: Transportation Cost Center # 9011

Vendor Name: FLHSMV

Contract Title: Data Exchange MOU

Contract Type: New ☒ Renewal ☐ Amendment ☐ Extension ☐ Previous Year Contract #

Contract Term: 3 years 11/2026 Renewal Option(s): NO

Contract Cost: Ø

☐ **BUDGETED FUNDS – SEND CONTRACT PACKAGE DIRECTLY TO PURCHASING DEPT**

Funding Source: Budget Line # _____

Funding Source: Budget Line # _____

☒ **NO COST MASTER (COUNTY WIDE) CONTRACT - SEND CONTRACT PACKAGE DIRECTLY TO PURCHASING DEPT**

☐ **INTERNAL ACCOUNT - IF FUNDED FROM SCHOOL IA FUNDS – SEND CONTRACT PACKAGE DIRECTLY TO SBAO**

REQUIRED DOCUMENTS FOR CONTRACT REVIEW PACKAGE (*when applicable*):

✓ Completed Contract Review Form

_____ SBAO Template Contract or other Contract (NOT SIGNED by District / School)

_____ SIGNED Addendum A (If not an SBAO Template Contract) - **When using the Addendum A, *this Statement MUST BE included in the body of the Contract:***
"The terms and conditions of Addendum A are hereby incorporated into this Agreement and the same shall govern and prevail over any conflicting terms and/or conditions herein stated."

_____ Certificate of Insurance (COI) for General Liability & Workers' Compensation that meet these requirements:
COI must list the School Board of Clay County, Florida as an Additional Insured and Certificate Holder. Insurer must be rated as A- or better.
General Liability = $1,000,000 Each Occurrence & $2,000,000 General Aggregate.
Auto Liability = $1,000,000 Combined Single Limit ($5,000,000 for Charter Buses).
Workers' Compensation = $100,000 Minimum
[If exempt from Workers' Compensation Insurance, vendor/contractor must sign a Release and Hold Harmless Form. If not exempt, vendor/contractor must provide Workers' Compensation coverage].

_____ State of Florida Workers Comp Exemption (https://apps.fldfs.com/bocexempt/) (If Applicable)

_____ Release and Hold Harmless (If Applicable)

RECEIVED 10/11/23 SBAO

****AREA BELOW FOR DISTRICT PERSONNEL ONLY ****

CONTRACT REVIEWED BY:	COMMENTS BELOW BY REVIEWING DEPARTMENT
Purchasing Department BFS Review Date 10/11/23	No Cost Fill in Section D. on page 19 + page 27 by Board
School Board Attorney Review Date AB 10/24/23	Page 2 + 3 School Board of Clay County, SBCC Signed By Board, Complete Data Access Application, Certification Statement ① School Board of Clay County, Florida, Add this Throughout
Other Dept. as Necessary Review Date	② Complete Pg. 19 ③ Complete Pg. 27 ④ Good luck – There are a huge # of compliance rules
PENDING STATUS: ☐YES ☐NO	IF YES, HIGHLIGHTED COMMENTS ABOVE MUST BE CORRECTED BY INITIATOR
FINAL STATUS	DATE:

⑤ Take to Board

☑ APPROVED 10-25-23

FLORIDA DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES

DATA EXCHANGE MEMORANDUM OF UNDERSTANDING

This Memorandum of Understanding (MOU) is made and entered into by and between

The School Board of Clay County, Florida, hereafter referred to as the Requesting Party, and the Florida Department of Highway Safety and Motor Vehicles, hereafter referred to as the Providing Agency, collectively referred to as the Parties.

I. Purpose

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 Personal Information that identifies individuals. Based upon the nature of this information, the Providing Agency is subject to the various disclosure prohibitions and restrictions contained in 18 U.S.C. §2721, the Driver's Privacy Protection Act (hereafter "DPPA"), sections 119.0712(2), 316.066, 324.242, and 501.171, Florida Statutes, and other statutory provisions.

The Requesting Party is a Government Entity or Private Entity operating under the laws and authority of the state of Florida and/or operating under federal laws and is requesting Personal Information and declares that it is qualified to obtain Personal Information under the exception number(s), listed in Attachment I, authorized by DPPA.

This MOU is entered into for the purpose of establishing the conditions and limitations under which the Providing Agency agrees to provide electronic access to Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and/or Insurance

Record Information to the Requesting Party.

The types of data requested and the applicable statutory fees if applicable, are agreed to by both parties as indicated in Attachment II.

The Requesting Party is receiving a ☐ 9-digit, a ☐ 4-digit, or ☑ no social security number, pursuant to Chapter 119, Florida Statutes, or other applicable laws.

II. Definitions

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

A. Batch/File Transfer Protocol (FTP)/Secure File Transfer Protocol (SFTP) - An electronic transfer of data in a secure environment.

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

C. Consumer Complaint Point-of-Contact - A person appointed by the Requesting Party to assist the Providing Agency with complaints from consumers regarding misuse of Personal Information protected under DPPA.

D. Control Record - A record containing fictitious information that is included in data made available by the Providing Agency and is used to identify inappropriate disclosure or misuse of data.

E. Crash Insurance Information - Insurance information, such as insurance company name, policy type, policy status, insurance creation and expiration date, including insurance policy number, provided to the Requesting Party pursuant to section 324.242, Florida Statutes, on vehicles involved in a crash.

F. Crash Report Information - Information derived from crash reports submitted by the investigating law enforcement agency to the Providing Agency and entered into a computerized database pursuant to section 316.066, Florida Statutes, which includes

Personal Information and the employment street address, and the home and telephone numbers of the Parties involved in the crash.

G. Downstream Entity - Any individual, association, organization, or corporate entity who receives Driver License Information, Crash Report Information, Crash Insurance Information, and/or Insurance Record Information from a Third Party End User in accordance with DPPA and section 119.0712(2), Florida Statutes.

H. Driver License Information – Driver license and identification card data collected and maintained by the Providing Agency. This data includes Personal Information .

I. Driver's Privacy Protection Act (DPPA) - The Federal Act (see, 18 United States Code § 2721, et seq.) that prohibits release and use of Personal Information except as otherwise specifically permitted within the Act.

J. Government Entity - Any federal, state, county, county officer, or city government, including any court or law enforcement agency.

K. Highly Restricted Personal Information – Information that includes, but is not limited to, medical or disability information and social security number.

L. Insurance Record Information - Insurance information, such as insurance company name, policy type, policy status, insurance creation and expiration date, but excluding insurance policy number, provided to the Requesting Party, pursuant to section 324.242, Florida Statutes.

M. Motor Vehicle Information - Title and registration data collected and maintained by the Providing Agency for vehicles and vessels. This information includes Personal Information.

N. Parties - The Providing Agency and the Requesting Party.

O. Personal Information - As described in section 119.0712(2)(b), Florida Statutes and 18 U.S.C. S.2725, information which includes, but is not limited to, the subject's driver

identification number, name, address, (but not including the 5–digit zip code), date of birth, height, race, gender and medical or disability information.

P. Private Entity - Any entity that is not a unit of government, including, but not limited to, a corporation, partnership, limited liability company, nonprofit organization or other legal entity or a natural person.

Q. Providing Agency - The Department of Highway Safety and Motor Vehicles.

R. Requesting Party - Any entity type that is expressly authorized by section 119.0712(2), Florida Statutes and DPPA to receive Personal Information and/or Highly Restricted Personal Information that requests information contained in a driver license or motor vehicle record from the Providing Agency through remote electronic access.

S. Requesting Party Number - A unique number assigned to the Requesting Party by the Providing Agency that identifies the type of records authorized for release and the associated statutory fees for such records.

T. Technical Contact - A person appointed by the Requesting Party to oversee the maintenance/operation of setting up of Web Service and Batch/FTP/SFTP processes.

U. Third Party End User - Any individual, association, organization, or corporate entity who receives Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and Insurance Record Information from the Requesting Party in accordance with DPPA and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.

V. 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.

III. Legal Authority; Restrictions on the Dissemination of Information Provided by the Providing Agency

A. The Providing Agency maintains computer databases containing information pertaining to driver's licenses and motor vehicles pursuant to Chapters 316, 317, 319, 320, 322, 328, and section 324.242, Florida Statutes. The Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, Insurance Record Information and vessel data contained in the Providing Agency's databases is defined as public record pursuant to Chapter 119, Florida Statutes and, as such, are subject to public disclosure, unless otherwise exempted from disclosure or made confidential by law.

B. As the custodian of the state's Driver License Information, Motor Vehicle Information Crash Report Information, Crash Insurance Information, and Insurance Record Information, , the Providing Agency is responsible for providing access only to records and information permitted to be disclosed by law.

C. Under this MOU, the Requesting Party will be provided, via remote electronic means, certain Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and Insurance Record Information, including Personal Information authorized to be released pursuant to DPPA and sections 119.0712(2), 316.066, or 324.242, Florida Statutes,

D. Highly Restricted Personal Information shall only be released in accordance with DPPA and Florida law.

E. The Providing Party only may provide information derived from crash reports to the Requesting Party pursuant to section 316.066(2), Florida Statutes. Sixty days after the date a crash report is filed, the Providing Agency may provide Crash Report Information to entities eligible to access the crash report pursuant to section 316.066(2)(b), Florida Statutes, and in accordance with any of the permissible uses listed in 18 U.S.C. s. 2721(b) and pursuant to the resale and redisclosure requirements in 18 U.S.C. s. 2721(c).

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

IV. Statement of Work

A. The Providing Agency agrees to:

1. Provide the Requesting Party with the technical specifications, and Requesting Party Number if applicable, required to access data in accordance with this MOU and the access method being requested.

2. Allow the Requesting Party to electronically access Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and Insurance Record Information as authorized under this MOU, DPPA, and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.

3. Collect all fees for providing the electronically requested data, pursuant to applicable Florida Statutes, rules and policies, including sections 320.05 and 322.20, Florida Statutes. The fee shall include all direct and indirect costs of providing remote electronic access, according to section 119.07(2)(c), Florida Statutes.

4. Collect all fees due for electronic requests through the Automated Clearing House account of the banking institution which has been designated by the Treasurer of the State of Florida for such purposes.

5. Terminate the access of the Requesting Party for non-payment of required fees. The Providing Agency shall not be responsible for the failure, refusal, or inability of the Requesting Party to make the required payments, or interest on late payments for periods of delay attributable to the action or inaction of the Requesting Party.

6. Notify the Requesting Party at least thirty (30) business days prior to changing any fee schedules, when it is reasonable and necessary to do so, as determined by the Providing Agency. All fees are established by Florida law. Any changes in fees shall be effective on the effective date of the corresponding law change. The Requesting Party may continue with this MOU, as modified, or it may terminate the MOU in accordance with Section XI., subject to the payment of all fees incurred prior to termination.

7. Perform all obligations to provide access under this MOU contingent upon an annual

appropriation by the Legislature.

8. Provide electronic access to Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and Insurance Record Information, pursuant to roles and times established other than scheduled maintenance or periods of uncontrollable disruptions. Scheduled maintenance normally occurs Sunday mornings between the hours of 6:00 A.M. and 10:00 A.M., Eastern Time.

9. Provide a contact person for assistance with the implementation of this MOU.

B. The Requesting Party agrees to:

1. Access or utilize all information provided by the Providing Agency pursuant to this MOU in strict compliance with DPPA and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.

2. Maintain the confidential and exempt status of all information provided by the Providing Agency pursuant to this MOU as required by DPPA and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.

3. Ensure that any Third Party End Users and Downstream Users accessing or utilizing information obtained by the Requesting Party by, through, or as a result of this MOU shall do so strictly in compliance with DPPA and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.

4. Ensure that any Third Party End Users and Downstream Users accessing or utilizing information obtained by the Requesting Party by, through, or as a result of this MOU maintains the confidential and exempt status of such information as required by DPPA and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.

5. Ensure that Highly Restricted Personal Information, including that accessed by any Third Party End Users and Downstream Users by, through, or as a result of this MOU, only may be released as authorized by DPPA and Florida law.

6. Request access to Crash Insurance Information, including Vehicle Identification Number, if authorized pursuant to this MOU only for vehicles actually involved in a crash or for vehicles of persons involved in a crash. Access to Crash Insurance Information will be provided by the Providing Agency only upon the submission by the Requesting Party of the date of a specific crash, the associated crash report number, and evidence that the Requesting Party or a Third Party End User is the attorney of the person involved in a specific crash or a representative of the insurer of a person involved in a specific crash.

7. Use information provided pursuant to this MOU only for the expressed purposes as described in Attachment I of this MOU.

8. Not misuse its Requesting Party Number to obtain information pursuant to this MOU for any use which violates this MOU and the immediate termination of this MOU by the Providing Agency upon the discovery of any misuse by the Requesting Party of its Requesting Party Number.

9. Self-report to the Providing Agency all violations of the MOU within five (5) business days of discovery of such violation(s). The report shall include a description, the time period, the number of records impacted, the harm caused, and all steps taken as of the date of the report to remedy or mitigate any injury caused by the violation.

10. Accept responsibility for interfacing with any and all Third Party End Users. The Providing Agency will not interact directly with any Third Party End Users. Requesting Party shall not give Third Party End Users the name, e-mail address, or telephone number of any Providing Agency employee without the express written consent of the Providing Agency. In addition, the Requesting Party agrees to have controls in place to ensure Third Party End Users comply with all requirements of this MOU.

11. Have controls in place to ensure Third Party End Users who redisclose FLHSMV data to Downstream Entities are subject to the terms and conditions of this MOU and that such Downstream Entities comply with this MOU, DPPA, and sections 119.0712(2), 316.066, and 324.242, Florida Statutes

12. Establish procedures to ensure that its employees and agents, including any contractors carrying out work on behalf of the Requesting Party or Third Party End Users and/or Downstream Entities, comply with Section V., Safeguarding Information, and provide a copy of the procedures to the Providing Agency within ten (10) business days of a request.

13. 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.

14. Use the information received from the Providing Agency only for the purposes authorized by this MOU, DPPA, and sections 119.0712(2), 316.066, and 324.242, Florida Statutes. The Requesting Party shall not:

    a. Redisclose the information received from the Providing Agency for bulk distribution for surveys, marketing or solicitations.

    b. Share or provide any information to another unauthorized entity, agency or person.

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

16. Indemnify the Providing Agency and its employees from any and all damages arising from the Requesting Party's negligent or wrongful use of information provided by the Providing Agency, to the extent allowed by law. This provision is not applicable to federal governmental entities.

17. For federal governmental entities: The Requesting Party agrees to promptly consider and adjudicate any and all claims that may arise out of this MOU resulting from the actions of the Requesting Party, duly authorized representatives, agents, or contractors of the Requesting Party, and to pay for any damage or injury as may be required by federal law. Such adjudication will be pursued under the Federal Tort Claims Act, 28 U.S.C. § 2671 et seq., the Federal Employees Compensation Act, 5 U.S.C. § 8101 et seq., or such other federal legal authority as may be pertinent.

18. Update user access/permissions upon reassignment of users within five (5) business days.

19. Immediately inactivate user access/permissions following separation, negligent, improper, or unauthorized use or dissemination of any information.

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

21. Pay all costs associated with electronic access of the Providing Agency's Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and Insurance Record Information. The Requesting Party shall:

    a. Maintain an account with a banking institution as required by the Providing Agency.

    b. Complete and sign the appropriate document(s) to allow the Providing Agency's designated banking institution to debit the Requesting Party's designated account.

    c. Pay all fees due the Providing Agency by way of the Automated Clearing House account of the Providing Agency's designated banking institution. Collection of transaction fees from eligible and authorized Third Party End Users is the responsibility of the Requesting Party.

22. Notify the Providing Agency within five (5) business days of any changes to the name, address, telephone number or email address of the Requesting Party, its Point-of-Contact for Consumer Complaints, and/or its Technical 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. Immediately notify the Providing Agency of any change of FTP/SFTP for the receipt of data

under this MOU. Failure to update this information as required may adversely affect the timely receipt of information from the Providing Agency.

24. 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 understands that it is obligated to comply with all applicable provisions of law.

25. Timely submit Internal Control and Data Security Audits required by Section VII., A. and the statements required in Section VII., B. and C.

26. A Requesting Party who has not previously received records from the Providing Agency shall utilize Web Services currently offered by the Providing Agency rather than batch/FTP/SFTP processes. Also, any Requesting Party using the FTP/SFTP processes agrees to transition to Web Services, where available, within six months (6) months of the Providing Agency's request.

27. Cooperate and ensure that its subcontractors, if any, cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing pursuant to section 20.055, Florida Statutes.

28. If the Requesting Party, a Third Party End User, or Downstream Entity that receives data from the Requesting Party has a public facing website that allows an individual to obtain Driver License Information or Motor Vehicle Information, the following minimum requirements must be in place prior to the transmission of data:

    a. Safeguards to ensure information obtained through the website is only disclosed to individuals authorized to receive it under 18 U.S.C. §2721(b). This includes internal controls to prevent or detect instances in which an individual attempts to purchase a record other than their own or to verify that the requestor meets a DPPA exemption.

    b. If the Requesting Party intends to allow an individual to purchase their own transcript from the Requesting Party's website utilizing the DPPA permissible use provided by 18 U.S.C. §2721(b)(13), a process to verify that the payment instrument used to

authorize the purchase is in the same name as the transcript being requested.

c. Safeguards to ensure that information is provided through the website only for the expressed purposes as described in Attachment I of this MOU.

d. Use of Transport Layer Security version 1.2 or later for encryption of data in transit and in session state.

e. Safeguards to ensure that the website is periodically scanned by a qualified external vendor for system vulnerabilities and all identified vulnerabilities are promptly remedied.

f. Safeguards to ensure that all systems that process Driver License Information or Motor Vehicle Information adhere to a formalized patch management process.

g. If the Requesting Party allows Third Party End Users or Downstream Entities to have a public facing website, the Requesting Party shall have controls in place to ensure the Third Party End User or Downstream Entity meets these requirements.

V. Safeguarding Information

A. 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 Chapter 119, Florida Statutes, sections 316.066 and 324.242, Florida Statutes, and DPPA. Information obtained under this MOU shall only be disclosed to persons to whom disclosure is authorized under Florida law and 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 agrees to comply with the provisions of section 501.171, Florida Statutes.

B. Any person who knowingly violates section 119.0712(2), Florida Statutes or section 316.066, Florida Statutes, may be subject to criminal punishment and civil liability, as provided in sections 119.10 or 316.066, 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.

C. In an effort to ensure information is only used in accordance with Chapter 119, Florida Statutes, and DPPA, the Providing Agency may include Control Records in the data provided in an effort to identify misuse of the data.

D. The Requesting Party 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 and any other state or State Agency due to non-compliance with DPPA, data breaches, or any state laws relating to the protection of driver privacy. The Requesting Party shall also notify the Providing Agency if any state or State Agency declines to enter into an agreement/contract with the Requesting Party to provide DPPA protected data.

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

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

4. Any instance where the owner, officer, or control person of the Requesting Party owned a majority interest in, or acted as a control person of, an entity that was found guilty or liable by a court of competent jurisdiction for misuse of data under DPPA or under any law of any state relating to the protection of driver privacy.

5. A breach of security as defined by section 501.171, Florida Statutes.

E. 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 business purpose, personal use, and the dissemination, sharing, copying or passing of this or any unauthorized information to unauthorized persons.

2. The Requesting Party will not be liable to the Providing Agency for any Driver License Information or Motor Vehicle Information lost, damaged, or destroyed as a result of the electronic exchange of data pursuant to this MOU, unless resulting from a negligent or wrongful act or omission of the Requesting Party.

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 shall develop security requirements and standards consistent with section 282.318, Florida Statutes, Florida Administrative Code Rule 60GG-2 (Formerly 74-2, FAC), and the Providing Agency's security policies; and employ adequate security measures to protect Providing Agency's information, applications, data, resources, and services. The applicable Providing Agency security policies are set forth in Attachment III.

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 with access to the information exchanged under the terms of this MOU will be instructed about, and acknowledge in writing their understanding of, the confidential nature of the information. These written acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency not later than ten (10) business days after a written request from the Providing Agency to review the written acknowledgments.

7. All personnel with access to the information will be instructed about and acknowledge in writing their understanding of the civil and criminal sanctions specified in state and federal law for unauthorized use of the data. These written acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency not later than ten (10) business days after a written request from the Providing Agency to review the written acknowledgments.

8. All access to the information must be monitored on an ongoing basis by the Requesting Party. In addition, the Requesting Party 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. B, below.

9. All data 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 and Requesting Party, on behalf of the respective Parties, attest and ensure that the confidentiality of the information exchanged will be maintained.

VI. Third Party End Users

Any agreement by the Requesting Party to provide Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, or Insurance Record Information to a Third Party End User and any agreement by a Third Party End User to provide Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, or Insurance Record Information to a Downstream Entity shall:

A. Be in writing.

B. Include and incorporate this MOU by reference without any change to this MOU.

C. Require the Third Party End User and any Downstream Entity to comply with DPPA and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.

D. Require the Third Party End User and any Downstream Entity to acknowledge in writing that, by receipt of Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, or Insurance Record Information, such Third Party End User and Downstream Entity are subject to and must comply with DPPA, sections

119.0712(2), 316.066, and 324.242, Florida Statutes.

E. Require the Requesting Party, Third Party End User, and any Downstream Entity to provide a copy of such agreement to the Providing Agency within ten (10) business days after a request by the Providing Agency for a copy of such agreement.

The failure of a Requesting Party, Third Party End User, and Downstream Entity to timely provide a copy of such agreement to the Providing Agency when requested by the Providing Agency shall be cause for the immediate termination of this MOU by the Providing Agency.

VII. Compliance and Control Measures

A. Internal Control and Data Security Audit - This MOU is contingent upon the Requesting Party having appropriate internal controls in place at all times to ensure that the information provided or received pursuant to this MOU is protected from unauthorized access, distribution, use, modification, or disclosure. The Requesting Party must submit to the Providing Agency an Internal Control and Data Security Audit from a currently licensed Certified Public Accountant (CPA), on or before the first anniversary of the execution date of this MOU or within one hundred twenty (120) days from receipt of a written request from the Providing Agency. Government agencies may submit the Internal Control and Data Security Audit from their Agency's Internal Auditor or Inspector General. The audit report shall be sent to the Providing Agency in the manner prescribed in Section XII, for Notices.

1. The audit report shall:

    a. Indicate whether the internal controls governing the use and dissemination of personal data have been evaluated based on the requirements of this MOU (see item 2 below).

    b. Indicate whether those internal controls included data security policies/procedures in place for personnel to follow and data security procedures/policies in place to protect personal data.

c. Indicate whether those data security procedures/policies have been approved by a Risk Management IT Security Professional, with credentials such as, but not limited to: CISA, CISSP, CISM, or CRISC.

d. Indicate whether any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence.

e. Include an opinion on whether those internal controls are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure.

2. The audit must be based on the requirements of this MOU, Florida Administrative Code Rule 60GG-2, and the Providing Agency's External Information Security Policy (attachment III). Engagements that do not consider these specific criteria or do not render an independent auditor's opinion or conclusion will not meet the requirements for the Internal Control and Data Security Audit. The Parties agree that a SOC 2 Report, consulting service engagement, or other audit report type will not satisfy the requirements for the Internal Control and Data Security Audit if the SOC 2 Report, consulting service engagement, or other audit report does not specifically address each of the elements listed in Section VII., A., 1. a., b., c., d., and e.

3. The Parties agree that an audit report which includes an audit period entirely outside the term of this MOU does not satisfy the requirements for the Internal Control and Data Security Audit.

4. The Requesting Party is responsible for clearly specifying the above audit requirements to the CPA, or government agency auditor, before audit work commences.

B. Annual Certification Statement - The Requesting Party shall submit to the Providing Agency an annual statement, utilizing Attachment IV, indicating that the Requesting Party has evaluated and certifies that it has adequate controls in place to protect the personal data from unauthorized access, distribution, use, modification, or disclosure, and is in full compliance with the requirements of this MOU and applicable laws. The Requesting Party shall submit this statement to the Providing Agency annually, not later than 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 and submitted to the Providing Agency, submission of the Internal Control and Data Security Audit may satisfy the requirement for submission of an Annual Certification Statement.) Failure to timely submit the annual certification statement may result in an immediate termination of this MOU. The annual certification statement shall be sent to the Providing Agency in the manner prescribed in Section XII, for Notices.

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

C. Misuse of Personal Information – The Requesting Party must notify the Providing Agency in writing of any incident where it is suspected or confirmed that Personal Information has been compromised as a result of unauthorized access, distribution, use, modification, or disclosure, by any means, within five (5) business days of such discovery. The statement must be provided on the Requesting Party'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 compromised; the name or names of personnel responsible; whether disciplinary action or termination was rendered; and whether or not the persons whose Personal Information was compromised were notified. The statement shall also indicate the steps taken, or to be taken, by the Requesting Party to ensure that misuse of data does not continue or recur. This statement shall be sent to the Providing Agency in the manner prescribed in Section XII, for Notices. (NOTE: If an incident involving breach of Personal Information did occur and the Requesting Party did not notify the owner(s) of the compromised records, the Requesting Party must indicate why notice was not provided.)

In addition, the Requesting Party 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.

D. Consumer Complaints – The Requesting Party shall provide a point-of-contact for consumer complaints. In the event the Providing Agency receives a consumer complaint regarding misuse of DPPA protected information, the Requesting Party shall review and investigate the complaint. The Requesting Party shall provide its findings to the Providing Agency not later than fifteen (15) business days from the date the Requesting Party receives notice of such a complaint from the Providing Agency.

Consumer Complaint Point-of-Contact Information:

Name: Randall Crawford

Email: randall.crawford@myoneclay.net

Phone Number: 904-336-0003

E. Control Records - In the event a Control Record inserted into data received by the Requesting Party is used in a manner that does not comply with DPPA or state law and upon the written request of the Providing Agency to the Requesting Party, the Requesting Party shall conduct an investigation of any Third Party End Users who obtained the record from the Requesting Party. As part of this provision, the Requesting Party shall also retain the authority to require Third Party End Users to investigate the Downstream Entities' handling and distribution of data subject to protection pursuant to DPPA and state law and to provide the results of the investigation to the Requesting Party. The Requesting Party shall provide the results of the investigation(s), together with all associated documents and information collected by the Requesting Party, Third Party Users and Downstream Entities, to the Providing Agency not later than fifteen (15) business days after receipt by the Requesting Party of the written request from the Providing Agency. When the Providing Agency requests the results of such an investigation, the results of the investigation shall be sent to the Providing Agency in the manner prescribed in Section XII., for Notices.

VIII. Liquidated Damages

Unless the Requesting Party is a state agency, the Providing Agency reserves the right to impose liquidated damages upon the Requesting Party. The imposition of liquidated damages by the Providing Agency is separate from and unrelated to any other applicable criminal or civil penalties authorized by law for violations of DPPA and sections 119.0712, 316.066, or 324.242, Florida Statutes.

Failure by the Requesting Party to meet the established requirements of this MOU may result in the Providing Agency finding the Requesting Party 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 information received pursuant to this MOU due to non-compliance with DPPA, sections 119.0712(2), 316.066, 324.242, 501.171, Florida Statutes, or any other state laws designed to protect the privacy of a driver's Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, or Insurance Record Information, the Providing Agency may impose upon the Requesting Party liquidated damages of up to $25.00 per record for each record involved in such breach or misuse.

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

1. The Requesting Party's history with complying with DPPA, sections 119.0712(2), 316.066, 324.242, and 501.171, Florida Statutes, or any other state laws designed to protect a driver's privacy;

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

3. Whether the Requesting Party violated this MOU over an extended period of time;

4. Whether the Requesting Party'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 had controls and procedures that were implemented and reasonably designed to prevent or detect violations of this MOU; and,

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

In lieu of paying liquidated damages to the Providing Agency upon assessment of such damages by the Providing Agency, the Requesting Party may elect to temporarily suspend this MOU, contingent upon the Requesting Party submitting a written statement that the Requesting Party will not obtain information from the Providing Agency through remote electronic means until such time as the liquidated damages assessed by the Providing Agency are paid by the Requesting Party in full. Such statement shall be signed by the Requesting Party's authorized representative and shall be submitted to the Providing Agency in the manner prescribed in Section XII, for Notices not later than five days after receipt of notice by the Requesting Agency that liquidated damages have been assessed.

The Requesting Party agrees that the Providing Agency may refuse to enter a subsequent or replacement MOU with the Requesting Agency to allow the Requesting Party to access information available pursuant to this MOU through remote electronic means until the Requesting Party has paid all outstanding liquidated damages in full. The Requesting Party agrees that this subsection A shall survive the termination of this MOU.

B. Corrective Action Plan (CAP)

1. If the Providing Agency determines that the Requesting Party is out of compliance with any of the provisions of this MOU, including, without limitation thereto, submission of an Internal Control and Data Security Audit that does not meet the requirements set forth in Section VII., and requires the Requesting Party to submit a CAP, the Providing Agency may require the Requesting Party to submit a Corrective Action Plan (CAP) within a specified timeframe. The CAP shall provide an opportunity for the Requesting Party 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 of the occurrence in writing. The Providing Agency shall provide the Requesting Party with a timeframe for corrections to be made.

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

4. The Requesting Party shall implement the CAP only after the Providing Agency's approval of the CAP.

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

6. If the Requesting Party does not meet the standards established in the CAP within the agreed upon timeframe, the Requesting Party 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 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 three (3) 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 for failure of the Requesting Party 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), 316.066, 324.242 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, or any of its majority owners, officers or control persons 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 Information. This MOU may be terminated in the event any agreement/contract

between the Requesting Party and any other state or State Agency is terminated due to non-compliance with DPPA or data breaches, or any state laws designed to protect driver privacy. The Requesting Party will have ten (10) 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's Business Point-of-Contact listed on the signature page.

XIII. Additional Database Access/Subsequent MOU's

A. The Parties understand and acknowledge that this MOU entitles the Requesting Party to receive specific information included within the scope and subject to the requirements of this MOU. Should the Requesting Party wish to obtain access to other Personal Information not provided hereunder, the Requesting Party 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 Information will contain the same clauses as are contained herein regarding audits, report submission, and the submission of Certification statements.

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

XIV. Public Records Requirements

A. 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.

B. If the Requesting Party 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:

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

2. 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.

3. 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 term of this MOU and following completion of the MOU if the Requesting Party does not transfer the records to the Providing Agency.

4. Upon termination or expiration of the MOU, the Requesting Party agrees they shall cease disclosure or distribution of all data provided by the Providing Agency. In addition, the Requesting Party agrees that all data provided by the Providing Agency remains subject to the provisions contained in DPPA and sections 119.0712 and 501.171, Florida Statutes. The Parties agree that all provisions herein concerning the protection of data provided by the Providing Agency to the Requesting Party shall survive the expiration or termination of this MOU, that the Providing Agency reserves the right to enforce the provisions of this MOU after the MOU's expiration or termination, including obtaining injunctive relief.

IF THE REQUESTING PARTY HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE REQUESTING PARTY'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS MOU, 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 PAGE INTENTIONALLY LEFT BLANK

IN WITNESS HEREOF, the Parties hereto, have executed this MOU by their duly authorized officials on the date(s) indicated below.

REQUESTING PARTY:

The School Board of Clay County, Florida

Requesting Party Name

Clay

Street Address

Suite

Grn Cv Sprgs FL

City State Zip Code

BY:

Signature of Authorized Official

Ashley Gilhousen

Printed/Typed Name

SBCC Board Chair

Title

Date

randall.crawford@myoneclay.net

Official Requesting Party Email Address

904-336-0003

Phone Number

BUSINESS POINT-OF-CONTACT:

Randall Crawford

Printed/Typed Name

randall.crawford@myoneclay.net

Official Requesting Party Email Address

904-336-0003 /

Phone Number / Fax Number

TECHNICAL POINT-OF-CONTACT:

Printed/Typed Name

Official Requesting Party Email Address

/

Phone Number / Fax Number

PROVIDING AGENCY:

Florida Department of Highway Safety and Motor Vehicles

Providing Agencey Name

2900 Apalachee Parkway

Street Address

Suite

Tallahassee, Florida 32399

City State Zip Code

BY:

Signature of Authorized Official

Printed/Typed Name

Chief, Bureau of Purchasing and Contracts

Title

Date

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, address and, medical or disability information. Personal information does not include information related to driving violations and driver status. 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.

In lieu of completing this form, a request for information may be made in letter form (on company/agency letterhead, if appropriate) stating the type of information being requested, the DPPA exemption(s) under which the request is being made, a detailed description of the how the information will be used, and a statement that the information will not be used or redisclosed except as provided in DPPA. If the information is provided on letterhead it must include a statement that the information provided is true and correct, signed by the authorized official under penalty of perjury, and notarized.

I am a representative of an organization requesting personal information for one or more records as described below. I declare that my organization is qualified to obtain personal information under exemption number(s) 9, 14, as listed beginning on page 4 of this form.

Pursuant to Section 316.066, F.S., Crash Report Information is confidential and exempt. 60 days after the date a crash report is filed, Crash Report Information may be provided which includes personal information to entities who are eligible to receive it under Section 316.066 (2), F.S., or in accordance with the Driver Privacy Protection Act. Crash Report Information cannot be used for commercial solicitation of crash victims or knowingly disclosed to any third party for purposes of such solicitation.

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. For access to Crash Report Information, please provide justification of your organization's eligibility under Section 316.066, F.S. below (attach additional page, if necessary):

DPPA Exemption Claimed:	Description of How Requesting Party Qualifies for Exemption:	Description of how Data will be used:
9 ,14		School Board of Clay County, Florida Transportation Department will be using this to request MVR for potential bus driver applicants before employment is offered. SBCC will also be using this to track white fleet operators who we have to keep track of any potential license issues for point tracking purposes. We will need to pull a weekly report of MVR's in order to properly track this.

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.

_____	SBCC Board Chair
Signature of Authorized Official	Title
Ashley Gilhousen	The School Board of Clay County, Florida
Printed Name	Name of Agency/Entity
_____	
Date	

STATE OF Florida

COUNTY OF Clay

Sworn to (or affirmed) and subscribed before me this_____day of_____, 20___, by

_____.

Personally Known ____ OR Produced Identification ____

Type of Identification Produced_____

Bonnie O'Nora	_____
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.

DATA ACCESS SPECIFICATIONS – Attachment II

Requesting Party: The School Board of Clay County, Florida

Jobs and Processes Selected

Mode of Access	Type of Data Requested	Statutory Fees (subject to change by the Legislature)	
Batch (FTP)	☐ DL Data (Driver License Information)	☐ $0.01/record, per s. 322.20, F.S.	☐ No Charge
	☐ MV Data (Motor Vehicle Information)	☐ $0.01/record, per s. 320.05, F.S.	☐ No Charge
	☐ DL Status (DSS600/605) (Driver License Information)	☐ $0.01, $0.50/record, per s. 320.05, F.S.; $2.00/record not found, per s. 322.20, F.S.	☐ No Charge
Program/Job Name			
IP Address(es)			
Web Services			
Driver Transcript Web Service (Each service accesses Driver License Information)	☑ DL Transcript (3 Year) (old DTR060)	☐ $8.00; $2.00/record not found, per s. 322.20, F.S.	☐ No Charge
	☑ DL Transcript (7 Year or Complete) (old DTR060)	☐ $10.00; $2.00/record not found, per s. 322.20, F.S.	☐ No Charge
	☐ Bulk Lookback (old DMS485)	☐ $0.01/record or $2.00/record not found, per s. 322.20, F.S.	☐ No Charge
Public Access Web Service	☐ DL Status (Driver License Information)	☐ $0.50/ record, per s. 320.05, F.S.	☐ No Charge
	☐ MV Record (Motor Vehicle Information)	☐ $0.50/ record, per s. 320.05, F.S.	☐ No Charge
	☐ Insurance Record Information	☐ $0.50/ record, per s. 320.05, F.S.	☐ No Charge
	☐ Parking Permit Record Information	☐ $0.50/ record, per s. 320.05, F.S.	☐ No Charge

DATA ACCESS SPECIFICATIONS – Attachment II

Mode of Access		Type of Data Requested		Statutory Fees (subject to change by the Legislature)		
Penny Vendor DL Web service	☐	DL update file of issuance/ purge records (old DFO292) (Driver License Information	☐	$0.01/record, per s. 322.20, F. S.	☐	No Charge
DL Status Verification	☐	Driver License Status	☐	$0.01, $0.50/record, per s. 320.05, F.S.; $2.00/record not found, per s. 322.20, F.S.	☐	No Charge
Residency Verification Web service	☐				☐	No Charge
Other Web Services	☐				☐	No Charge
Crash Report Information	☐				☐	No Charge

FLHSMV
FLORIDA HIGHWAY SAFETY AND MOTOR VEHICLES

Dave Kerner
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

Data Access Application

Prior to executing the Memorandum of Understanding (MOU) for Driver License and/or Motor Vehicle Data Exchange, the Requesting Party is required to complete this application. Please use additional pages as necessary.

1. In the last ten (10) years, has any agreement/contract between the Requesting Party and/or any other State/State Agency been terminated due to non-compliance with DPPA, data breaches, or any state laws relating to the protection of driver privacy? Yes ○ No ◉ If yes, please explain and supply certified copies of the pertinent documents:

2. In the last ten (10) years, has any State/State Agency declined to enter into an agreement/contract with the Requesting Party to provide DPPA protected data? Yes ○ No ◉ If yes, please explain:

3. Is there any pending litigation against the Requesting Party alleging violations of DPPA or any state law relating to the protection of driver privacy? Yes ○ No ◉ If yes, please explain and provide a certified copy of the pertinent court documents:

4. In the last ten (10) years, has there been any instance where the Requesting Party has been 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? Yes ○ No ◉ If yes, please explain and provide certified copies of the pertinent documents:

5. In the last ten (10) years, has there been any instance where an owner, officer, or control person[1] of the Requesting Party who owned a majority interest in, or acted as a control person of, an entity that was 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? Yes ○ No ◉ If yes, please explain and provide certified copies of the pertinent documents:

6. In the last ten (10) years, has there been any breach of security as defined by Section 501.171, Florida Statutes? Yes ○ No ◉ If yes, provide details of each breach and discuss all safeguards implemented as a result of the breach of security:

7. How you will ensure that all personnel with access to the information exchanged under the terms of the MOU are instructed of, and acknowledge their understanding of, the confidential nature of the information?

Individual training on the confidential nature of the information.
Acknowledgement of terms and understanding will be signed and kept on file with Human Resources

8. Does your company or agency have a public facing website that allows an individual to purchase driver license/motor vehicle information? Yes ○ No ◉

If yes, please provide the URL: _____

In addition, please indicate whether your agency has the following minimum requirements listed below in place:

A. Safeguards to ensure information obtained through the website is only disclosed to individuals authorized to receive it under 18 U.S.C. §2721(c). This includes internal controls to prevent or detect instances in which an impostor attempts to purchase a record other than their own and/or to verify that the requestor meets a DPPA exemption. ◉ Yes ○ No ○ N/A

Please describe safeguards:

Records are only accessed through secured network by approved transportation staff.

[1] Control Person, for these purposes, means the power, directly or indirectly, to direct the management or policies of a company, whether through the ownership of securities, by contract, or otherwise. Any person that (i) is a director, general partner, or officer exercising executive responsibility (or having similar status or functions); (ii) directly or indirectly has the right to vote 25% or more of a class of a voting security or has the power to sell or direct the sale of 25% or more of a class of voting securities; or (iii) in the case of a partnership, has the right to receive upon dissolution, or has contributed, 25% or more of the capital, is presumed to control that company.

B. Do you intend to allow individuals to purchase their own transcript from your public facing website, utilizing DPPA exemption number 13? Yes ○ No ◉ N/A ○

C. If the answer to the previous question is yes, do you have a process in place to verify that the payment instrument used to authorize the purchase is in the same name as the transcript being requested? Yes ○ No ○ N/A ◉

Please explain the process:

D. Do you only provide information through the website for the expressed purposes as described in Attachment I of this MOU? Yes ○ No ○ N/A ◉

E. Does the website utilize Transport Layer Security version 1.2 or later for encryption of data in transit and in session state? Yes ○ No ○ N/A ◉

Please explain:

F. Is the website periodically scanned by a qualified external vendor for system vulnerabilities? Yes ○ No ○ N/A ◉

G. If the answer to the previous question is yes, are identified vulnerabilities promptly remediated? Yes ○ No ○ N/A ◉

Please explain:

9. Do all systems that process driver license / motor vehicle information adhere to a formalized patch management process? Yes ◉ No ○

Please explain:

Devices that access DL and MVI on the network are patched using WSUS and PDQ. Deploy weekly and monthly or immediately for critical updates

In addition, the following documents are required:

a. A copy of your business license.
b. A copy of your State of Florida corporation licensure or certification.
c. If providing services on behalf of a government entity, provide the supporting documentation to show or prove you are entitled to the DPPA exemption claimed. For example, a letter from each entity confirming the type of service being provided and/or an agreement with an entity authorizing you to conduct services.

Under penalty of perjury, I affirm that the information provided in this document is true and correct.

_____
Signature of Authorized Official

Ashely Gilhousen
Printed/Typed Name

SBCC Board Chair
Title

_____
Date

School Board of Clay Co, FL
NAME OF AGENCY/ENTITY

STATE OF Florida
COUNTY OF Clay

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

Personally Known ☐ OR Produced Identification ☐
Type of Identification Produced _____

Bonnie O'Nora
NOTARY PUBLIC (print name)

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

FLHSMV
FLORIDA HIGHWAY SAFETY AND MOTOR VEHICLES

Dave Kerner
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

CERTIFICATION STATEMENT

Under penalty of perjury I have read the requirements contained in the Memorandum of Understanding, Florida Administrative Code, Rule Chapter 60GG-2 (Formerly 74-2, FAC), and the Department of Highway Safety and Motor Vehicles External Information Security Policy and declare that the following is true:

The Requesting Party, School Board of Clay County, Florida hereby certifies that the Requesting Party has appropriate internal controls in place to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure. This includes policies/procedures in place for both personnel to follow and data security procedures/policies to protect personal data. The data security procedures/policies have been approved by a Risk Management IT Security Professional.

STATE OF Clay
COUNTY OF Clay

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

Personally Known __☑__ OR Produced Identification __☐__
Type of Identification Produced_____

Bonnie O'Nora
NOTARY PUBLIC (print name)

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

_____
Signature

Ashley Gilhousen
Printed Name

SBCC Board Chair
Title

_____
Date

School Board of Clay County, Florida
NAME OF AGENCY

(Rev. 01/23)

External Information Security
Policy Manual

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 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 section 282.318, F.S., in the footer, added effective issue date	12/7/2017
2.1	Scott Morgan	Reviewed all policies. Revised to align with Rule 60GG-2, F.A.C., State of Florida Cybersecurity Standards.	8/3/2020
3.0	Scott Morgan Crill Merryday Bonny Allen	Reviewed all policies and revised policies. Added an additional policy specifically addressing patch management requirements for external entities. Provided guidance on applicability of policies to specific entities. Removed 30-day training grace period. #B-02, 2.0, #3 – added a specific time frame as per compliance with Florida Commission on Accreditation (CFA) Standard 26.04M (Mandatory), for Access Control.	11/2/2022

* Note: This document version coincides with the separate IT Security Policy Manual for Internal Department employees.

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 60GG-2, Information Technology Security.

#A-02: Data Security	Review Date: 05/20/2022	Issue Date: 12/01/08	Revised Date: 05/22/2022

#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, wherever it may reside, 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 with an executed Memorandum of Understanding (MOU) which is held by the Department.

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 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 which include Department data 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 External Entity granted access to use of these resources.

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 and transmitted.

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. Additional requirements based on specific use cases may be outlined in the MOU between the Department and the External Entity.

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. Logs shall be maintained in a manner that provides timely reviews of access to confidential and sensitive data and will be made available on request to the Department for validation and compliance purposes.

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 FLHSMV requirements, which are based on 60GG-2, F.A.C., 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.
  - Customer data including personally identifying information which is protected under the DPPA.

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.

For Confidential Department Data Shared Outside of Departmental Systems:

- Tax Collectors or their authorized vendors, as well as any External Entity must have access controls in place to permit only authorized users from obtaining access to confidential data.
- Access to confidential customer information requires extensive web and system logging of all access. Logs will be securely retained for a minimum of one year and be made available on-demand to authorized Department personnel when requested for compliance attestation, fraud investigations, and other authorized usage.
- Tax Collectors or their authorized vendors and other External Entities must submit an audit which meets the requirements of the MOU that certifies that appropriate controls are in place to protect confidential data.

9.0 Governance and Implementation of Statutory Responsibilities for Department Systems and Data

The Department is responsible for the computer systems that implement its statutory responsibilities for various Chapters in Florida Statutes. In addition, protection of personal and confidential data is a primary duty and responsibility of the Department. To ensure that the statutory responsibilities of the Department are carried out appropriately, the following policies govern computer systems with access to Department web services and data, but outside the control of the Department.

- Non-Department Web sites, mobile applications, web services, or computer systems which utilize Department data to conduct transactions are prohibited without written consent from the Department.

- As required to protect customer information, public facing websites, mobile applications, web services, and any system accessible through a public interface which utilizes confidential data shared by the Department with authorized external entities must utilize Department approved system access controls to protect confidential information.

- Changes to customer addresses through any public facing service as described above must be updated only through approved FLHSMV Department systems.

#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 user identification (userID) 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).
    - Shall not be anything that can be easily guessed or associated to the account owner such as: username, social security number, nickname, relative's names, pet's names, birth date, sports team, etc.
    - Shall not be dictionary words or acronyms, as they can be easily guessed.
    - Based on role, privilege assigned, or risk factor, multi-factor authentication shall be assigned as deemed necessary to further strengthen / protect privileged accounts and Department data.
    - 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 or shared with anyone. Passwords must be treated as confidential information and shall be safeguarded. User credentials (UserID and passwords) are to ONLY be used by the person to which they are assigned.
4. Passwords and usernames 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.
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 shall 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. Note: At no time shall a user call TAC requesting a password change for another user. TAC has been instructed to lock both accounts immediately when encountering this type of call, as it is a violation of this policy.

#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 store 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 resource 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 FLHSMV website)
2. Users shall not under any circumstances use another user's account logon or credentials. This includes network logon accounts and accounts used in agency systems (ORION, FRVIS, etc.). A user shall never call the Technical Assistance Center (TAC) to have another user's account unlocked.
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 removed and/or disabled immediately, no later than within three (3) business days, 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.
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 systems 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. 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 also enforce a least privilege access for any access to Department data or systems. .
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	Review Date: 05/14/2022	Issue Date: 12/01/08	Revised Date: 05/16/2022

#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 a requirement for accessing Department's information resources and data.

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 the Information and Cyber Security Awareness for External Entities online training course in iLearn prior to receiving account credentials. Additionally, external entities must complete the Information Security Training in iLearn on an annual basis within 90 days of assignment. Failure to complete the training may result in termination of account access.
3. All accounts must be uniquely identifiable using the assigned username. 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 and timely removal of access to Department resources and data.
    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	Review Date: 05/15/2022	Issue Date: 12/01/08	Revised Date: 05/15/2022

#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 when requested.
    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 testing for the application and or system accessing Department data. For example, testing of authentication, authorization, and accounting functions, or any other activity designed to validate the security architecture, including external and internal penetration testing.
   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, and must comply with all relevant Department MOU's.
   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)	Review Date: 05/16/2022	Issue Date: 12/01/08	Revised Date: 05/16/2022

#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, malware detection, ransomware, anomalous activity, and 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. Quickly reporting known or suspected security 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. All known or suspected incidents must be reported immediately to the Department's ISM using the email address: ISM@flhsmv.gov.
2. All suspected incidents of ransomware or other malware type activity must be reported immediately to the Florida Digital Service's statewide portal. All state, local, and county governments must comply with this requirement.

3. 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, including Department data.
   - Ransomware, malware, or related anomalous activity, once known OR suspected.
   - Unauthorized disclosure, modification, misuse, or disposal of sensitive, critical, or business-controlled data and information.
   - Suspected or known unauthorized internal or external access activity, including, but not limited to, sharing of user credentials and accounts which 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

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 assists in identification and remediation of new security vulnerabilities or emerging threats. This early identification assists 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 and relevant MOUs.
   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

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 feature sets. No connectivity 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 or firewall features.

3. All External Entities' network connections must meet the requirements of the Florida Information Resource Security Policies and Standards (Rule 60GG-2). Blanket access is prohibited, and the principle of least privilege shall apply at all times. Interconnectivity is limited to services, devices, and equipment needed.

4. Through system monitoring, alerting, or due to a reported incident, the Department's ISA and ESM teams reserve the right to immediately terminate and drop connectivity from the External Entities' environment to the Department's network. The Department takes the security of the HSMV network and the state MFN2 network seriously. All decisions for termination of access will be made with a risk-based decision in consultation between the Department's ISM and CIO.

   <u>External Entity Agreements:</u>
   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.

#B-24: Malware/Virus Protection	Review Date: 05/19/2022	Issue Date: 12/01/08	Revised Date: 05/19/2022

#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, ransomware, 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, ransomware, 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, processing, or accessing Department data, must utilize a modern and supported anti-virus protection system. The Department's ISM will maintain a list of any non-approved protection vendors, typically which are known or suspected to have security issues. 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 and data 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 and data must utilize a antivirus 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 ransomware exploit those 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 External Entities network until it is verified as free of viruses and malware and coordinated incident response with the Department's ISM.

#B-23: Patch and Vulnerability Management	Review Date: 05/21/2022	Issue Date: 05/21/2022	Revised Date: 05/21/2022

#B-23: Patch and Vulnerability Management

1.0 Purpose

To ensure that External Entities who are connected to Department systems or have access to Department data have a documented patching process for servers, workstations, network infrastructure, and devices within the External Entities environment. Timely application of vendor-issued critical security updates and patches are necessary to protect systems that connect to, store, or process Department information resources and data from malicious attacks and vulnerabilities which may impact function. All computing devices connected to the network including servers, workstations, firewalls, network switches and routers, tablets, mobile devices, and cellular devices routinely require patching for functional and secure operations.

2.0 Policy

External Entities who connect to, store, or process Department data must have a documented process for patching servers, workstations, network infrastructure and all computing devices within their environment, as any vulnerable system has the potential to affect the Department's network if connected through a DHSMV firewall or interface. Vulnerable systems in an External Entity environment not directly connected to the Department's network can also affect systems that store, or process Department data and interfaces shared with the External Entity.

1. External Entities who connect to Department systems, or store or process Department data shall follow a documented and regimented process for mitigation of critical security patches and remediation of vulnerabilities.

2. The documented process for patching and vulnerability remediation shall follow a patch management approach as outlined in NIST Special Publication 800-40r4 "Guide to Enterprise Patch Management Patching Planning" which can be found at the following URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

3. Documentation outlining conformance with this policy will be provided when requested to confirm compliance with Department policy and the MOU executed between the Department and the External Entity.

.

4. Non-compliance by an External Entity for this policy may include termination of access to Department systems, data, and resources if not remediated to reduce and mitigate critical vulnerabilities which may affect the confidentiality, integrity, and availability of Department information resources.

Definitions	Review Date: 05/21/22	Issue Date: 8/18/17	Revised Date: 05/21/22

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.