

PALM BEACH COUNTY
BOARD OF COUNTY COMMISSIONERS

AGENDA ITEM SUMMARY

Meeting Date: April 10, 2018

☒ Consent

☐

Regular

☐ Ordinance

☐

Public Hearing

Department: Risk Management

Submitted By: Risk Management

I. EXECUTIVE BRIEF

Motion and Title: Staff recommends motion to:


- A) **ratify** the signature of the Mayor on the Memorandum of Understanding For Driver's License and/or Motor Vehicle Record Data Exchange; and.
- B) **delegate** to the County Administrator, or designee, signature authority to execute any future renewals, addendums or other documents related to this Memorandum of Understanding.


Summary: The Memorandum of Understanding for Driver's License and/or Motor Vehicle Record Data Exchange with the Florida Department of Highway Safety and Motor Vehicles allows the County, through its Risk Management Department, to continue to ensure only authorized drivers with valid licenses are allowed to operate County vehicles. This is to ensure the safety of County employees and the general public. The record data exchange provides an automated file from the State to the County on a weekly basis. The file contains information on each authorized driver including notification of an invalid license, and the reason why a license has been suspended or revoked. A newly executed document is required by the State of Florida every three years as a condition of continuing the Driver's License and Motor Vehicle Record Data Exchange with the County under the provisions of the Driver's Privacy Protection Act, which protects the personal information contained within the files. Countywide (HH)

Background and Justification (or Policy Issues): Under the provisions of the County's Policy and Procedures Manual CW-O-004, the first version of which went into effect in 1991, the Risk Management Department is authorized to approve or disapprove an employee's privilege to drive a County owned vehicle. County drivers are not approved if they do not have a valid driver's license from the State of Florida. The electronic files received from the Department of Highway Safety and Motor Vehicles allow staff to ensure the validity of the licenses of all approved and newly hired drivers. Driver's licenses contain personal information that is protected under the Driver's Privacy Protection Act (DPPA) 18, USC 2721; however the State of Florida is authorized to provide the information to the County for the purpose of determining the eligibility of current employees and new hires to operate County vehicles. To that end, the State requires the execution of the attached Memorandum of Understanding every three years.

Attachments:

1. Executed Memorandum of Understanding For Driver's License and/or Motor Vehicle Record Data Exchange with Walkthrough Memoranda

Recommended By:  3/22/18
Department Director Date

Approved By:  3/28/18
Assistant County Administrator Date

II. FISCAL IMPACT ANALYSIS

A. Five Year Summary of Fiscal Impact

Fiscal Years	<u>2018</u>	<u>2019</u>	<u>2020</u>	<u>2021</u>	<u>2022</u>
Capital Expenditures					
Operating Costs					
External Revenues					
Program Income (County)					
In-Kind Match (County)					
Net Fiscal Impact	\$				

ADDITIONAL FTE

POSITIONS (Cumulative)	0	0	0	0	0
------------------------	---	---	---	---	---

Does this item include the use of federal funds? Yes No ☒ X

Is Item Included In Current Budget?	Yes	n/a	No
-------------------------------------	-----	-----	----

Budget Account	Exp No.:	Fund	Dept	Unit	Obj
	Rev No.:	Fund	Dept	Unit	Obj

B. Recommended Sources of Funds/Summary of Fiscal Impact:

* There is no fiscal impact associated with this item

C. Departmental Fiscal Review:

1: *B*

III. REVIEW COMMENTS

A. OFMB Fiscal and/or Contract Dev. and Control Comments:

Lisa Ponce 3/26/19
 OFMB
 3/26/19
 3/24 3/22

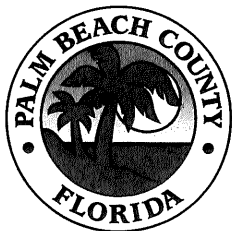
[Signature] 3/27/18
Contract Dev. and Control
3/27/18 *re*

B. Legal Sufficiency:


Assistant County Attorney

C. Other Department Review:

Department Director



Risk Management Department

100 Australian Avenue, Suite 200

West Palm Beach, FL 33406

(561) 233-5400

Fax: (561) 233-5420

www.pbcgov.com

**Palm Beach County
Board of County
Commissioners**

Melissa McKinlay, Mayor

Mack Bernard, Vice Mayor

Hal R. Valeche

Paulette Burdick

Dave Kerner

Steven L. Abrams

Mary Lou Berger

County Administrator

Verdenia C. Baker

MEMORANDUM

TO: Melissa McKinlay, Mayor *MM*
Board of County Commissioners

THRU: Verdenia C. Baker, County Administrator *VCB*
Board of County Commissioners

THRU: Nancy L. Bolton, Assistant County Administrator *NLB*
Board of County Commissioners

FROM: Scott Marting, Department Director *SM*
Risk Management Department

DATE: January 26, 2018

RE: Memorandum of Understanding between the Florida
Department of Highway Safety and Motor Vehicles and
Palm Beach County Board of County Commissioners.

Recently you signed the attached MOU as required by the State of Florida. Based on numerous conversations with the State, we believed the packet to be complete. However, the Florida Department of Highway Safety and Motor Vehicles notified Risk Management that an additional form was required from Palm Beach County upon their review of the MOU package. As such, we are submitting one additional document for signature.

In accordance with County PPM CW-O-051, this agreement will also be submitted as a "Receive and File" once the MOU has been fully executed.

If additional information is needed, please contact Jean Heald at (561) 233-5432.

Approved by:

[Signature]
Department Director

[Signature]
Assistant County Attorney

[Signature]
OFMB
[Signature]
Assistant County Administrator

Attachments:

1. The above listed MOU including the additional signature page

"An Equal Opportunity
Affirmative Action Employer"

printed on sustainable
and recycled paper



Risk Management Department
100 Australian Avenue, Suite 200
West Palm Beach, FL 33406
(561) 233-5400
Fax: (561) 233-5420
www.pbcgov.com



**Palm Beach County
Board of County
Commissioners**

Melissa McKinlay, Mayor
Mack Bernard, Vice Mayor
Hal R. Valeche
Paulette Burdick
Dave Kerner
Steven L. Abrams
Mary Lou Berger

County Administrator
Verdenia C. Baker

MEMORANDUM

TO: Melissa McKinlay, Mayor
Board of County Commissioners

THRU: Verdenia C. Baker, County Administrator
Board of County Commissioners

THRU: Nancy L. Bolton, Assistant County Administrator
Board of County Commissioners

FROM: Scott Marting, Department Director
Risk Management Department

DATE: January 5, 2018


RE: Memorandum of Understanding between the Florida
Department of Highway Safety and Motor Vehicles and Palm
Beach County Board of County Commissioners.

In December of 2014, Palm Beach County entered into a Memorandum of Understanding (MOU) with the Florida Department of Highway Safety and Motor Vehicles (DHSMV) that allows the County to submit authorized driver information to the State in order to confirm our employees continue to meet the requirements of County PPM CW-O-004, Vehicle Safety Program.

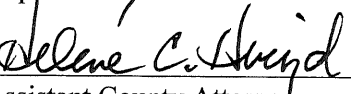
The renewal of that three-year MOU was overlooked due to staff turnover. To avoid an interruption in service, the attached MOU must be executed before the next meeting of the Board of County Commissioners. In accordance with County PPM CW-O-051, this MOU will be submitted for ratification at the next BCC meeting.

If additional information is needed, please contact Jean Heald at (561) 233-5432.

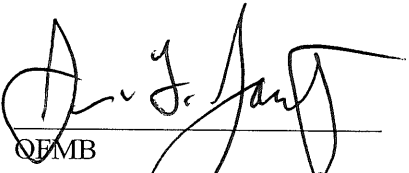
Approved by:



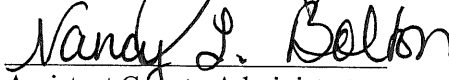
Department Director



Assistant County Attorney



OCMB



Assistant County Administrator

Attachment:

1. Memorandum of Understanding for Driver's License and/or Motor Vehicle Record Data Exchange



Florida Department of Highway Safety and Motor Vehicles

Contract / Agreement Review

DHSMV Contract No.:

HSMV-0478-18

Division:

Motorist Services

Date:

2/19/2018

Contractor Name:

Palm Beach County Board of County Commissioners

Contract Summary:

New MOU

Previous MOU HSMV-0383-15 terminated on 12/15/2017.

Total Cost / Revenue:

\$0.00

or No Cost

☐

Term:

3 years

Contract Manager:

Kayla white

Phone:

850.617.2805

☒ New Agreement

☐ New Contract (Procurement)

Procurement Method:

☐ ITB

☐ RFP

☐ ITN

☐ RFQ

☐ Single Source

☐ Informal Quote

☐ Exempt per _____, Florida Statutes

☐ Not Required

☐ Renewal

☐ Amendment

☐ Settlement Agreement

☐ New / Revised Template

Approvals	Comments
<div>Division Director(s)</div> <div>DocuSigned by: Signature: <u>Robert Kynoch</u> Date: <u>2/19/2018</u></div> <div>Signature: _____ Date: _____</div>	Data MOU
<div>Budget</div> <div>DocuSigned by: Signature: <u>Susan Lamy</u> Date: <u>2/28/2018</u></div> <div><input type="checkbox"/> If checked, budgetary review/approval is not required as funds are not expended under this Contract/Agreement.</div>	No costs or revenue impact
<div>Accounting</div> <div>DocuSigned by: Signature: <u>Sam</u> Date: <u>2/28/2018</u></div> <div><input type="checkbox"/> If checked, accounting review/approval is not required as funds are not received or obligated under this Contract/Agreement.</div>	n/a
<div>Information Services</div> <div>DocuSigned by: Signature: <u>Boyd Dickerson-Walden</u> Date: <u>3/1/2018</u></div> <div><input type="checkbox"/> If checked, ISA review/approval is not required as this Contract/Agreement does not impact information systems.</div>	no impact
<div>Legal</div> <div>DocuSigned by: Signature: <u>Jonathan P. Sanford</u> Date: <u>3/2/2018</u></div> <div><input type="checkbox"/> If checked, legal review/approval is not required as the document is a previously-approved boilerplate</div>	None.
<div>Purchasing & Contracts</div> <div>DocuSigned by: Signature: <u>[Signature]</u> Date: <u>3/2/2018</u></div>	.
<div>Administrative Services</div> <div>DocuSigned by: Signature: <u>Kelley Scott</u> Date: <u>3/4/2018</u></div>	3/4/18
<div>Deputy Executive Director</div> <div>Signature: _____ Date: _____</div> <div><input type="checkbox"/> If checked, review/approval by Deputy Executive Director is not required as the Contract/Agreement is either an approved template or does not fall under the Deputy Executive Director's areas of responsibility.</div>	
<div>Chief of Staff / Executive Director</div> <div>DocuSigned by: Signature: <u>Jamie Deload</u> Date: <u>3/4/2018</u></div>	C

Data Exchange
Memorandum of Understanding (MOU) – Item check list

Agency Name: Palm Beach County Board of County Commissioners

Documentation of current licensure or certification from resident state of corporation

- ☐ Copy of requestor’s business license
- ☐ Corporation status obtained from www.sunbiz.org.
- ☐ If vendor is acting on behalf of a government agency, a letter of authority is attached.
- ☒ This is a Government agency
- ☐ This is a Law enforcement agency.

Memorandum of Understanding

- ☒ Forms have been provided, reviewed, and approved.
 - ☒ Attachment 1 and/or letter provided in Lieu of
 - ☒ Attachment 2
 - ☒ Data Access Form
 - ☒ Certification Statement
 - ☒ Data Access Questionnaire
 - ☐ DPPA Violation Background Check Completed
 - ☐ Letter of delegation is required if signed by other than authorized official.

Debit Authorization Form

- ☐ Account/Routing number is provided.
- ☐ An appropriate signature is provided.
- ☐ Copy of form provided to Revenue.
- ☒ N/A

Reviewed By:

DocuSigned by:

Michael Sarvis

AEFB922945A74CE...

Date: 2/19/2018

Certificate Of Completion

Envelope Id: 432D2377303647829019114626845064

Status: Completed

Subject: Please DocuSign these documents:Palm Beach County Board of County Commissioners Data Ex MOU New

Source Envelope:

Document Pages: 27

Signatures: 10

Envelope Originator:

Certificate Pages: 4

Initials: 0

Kayla White

AutoNav: Enabled

PO Box 6669

Portland, OR 97228

Envelopeld Stamping: Enabled

kaylawhite@flhsmv.gov

IP Address: 207.156.9.1

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Record Tracking

Status: Original

Holder: Kayla White

Location: DocuSign

2/13/2018

kaylawhite@flhsmv.gov

Signer Events

Michael Sarvis
MichaelSarvis@flhsmv.gov
Florida Department of Highway Safety and Motor Vehicles
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Signature

DocuSigned by:

Michael Sarvis

AEFB922945A74CE...

Using IP Address: 207.156.9.1

Timestamp

Sent: 2/13/2018
Viewed: 2/19/2018
Signed: 2/19/2018

Robert Kynoch
RobertKynoch@flhsmv.gov
Director of Motorist Services
FL Dept HSMV
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

DocuSigned by:

Robert Kynoch

0A2EF6A47ABE486...

Using IP Address: 207.156.9.1

Sent: 2/19/2018
Viewed: 2/19/2018
Signed: 2/19/2018

Danielle Nesbeth
DanielleNesbeth@flhsmv.gov
HSMV
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Completed

Using IP Address: 207.156.9.1

Sent: 2/19/2018
Viewed: 2/23/2018
Signed: 2/23/2018

Susan Carey
SusanCarey@flhsmv.gov
Chief Financial Officer
FL Dept HSMV
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

DocuSigned by:

Susan Carey

7BD6B4036905431...

Using IP Address: 97.34.131.24

Signed using mobile

Sent: 2/23/2018
Resent: 2/28/2018
Viewed: 2/28/2018
Signed: 2/28/2018

Steve Burch
Steveburch@flhsmv.gov
Chief of Accounting
FL Dept HSMV
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:

DocuSigned by:

Steve Burch

C98ACEAF33244DF...

Using IP Address: 207.156.9.1

Sent: 2/28/2018
Viewed: 2/28/2018
Signed: 2/28/2018

Signer Events

Not Offered via DocuSign

Boyd Dickerson-Walden
Boyddickerson-walden@flhsmv.gov
Director of Informational Services
FL Dept HSMV
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Jonathan P. Sanford
JonathanSanford@flhsmv.gov
Chief Counsel
Florida Department of Highway Safety and Motor Vehicles
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Lisa Bassett
LisaBassett@flhsmv.gov
Chief
FL Dept HSMV
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Kelley Scott
KelleyScott@flhsmv.gov
Director of Administrative Services
Florida Department of Highway Safety and Motor Vehicles
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Jamie DeLoach
JamieDeLoach@flhsmv.gov
Chief of Staff NKB
Florida Department of Highway Safety and Motor Vehicles
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Becky Parramore
BeckyParramore@flhsmv.gov
Leasing Consultant
Florida Department of Highway Safety and Motor Vehicles
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Signature

DocuSigned by:
Boyd Dickerson-Walden
30156DFB955A473...

Using IP Address: 207.156.9.1

DocuSigned by:
Jonathan P. Sanford
ECF1225030E4490...

Using IP Address: 207.156.9.1

DocuSigned by:
Lisa Bassett
7E2E9F0980B2459...

Using IP Address: 207.156.9.1

DocuSigned by:
Kelley Scott
633CAC89C201454...

Using IP Address: 199.254.101.109

DocuSigned by:
Jamie DeLoach
991490B7AA52486...

Using IP Address: 174.227.139.173
Signed using mobile

Completed

Using IP Address: 207.156.9.1

Timestamp

Sent: 2/28/2018
Viewed: 3/1/2018
Signed: 3/1/2018

Sent: 3/1/2018
Viewed: 3/2/2018
Signed: 3/2/2018

Sent: 3/2/2018
Viewed: 3/2/2018
Signed: 3/2/2018

Sent: 3/2/2018
Viewed: 3/4/2018
Signed: 3/4/2018

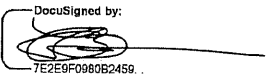
Sent: 3/4/2018
Viewed: 3/4/2018
Signed: 3/4/2018

Sent: 3/4/2018
Viewed: 3/5/2018
Signed: 3/5/2018

Signer Events

Lisa M. Bassett
LisaBassett@flhsmv.gov
Chief
FL Dept HSMV
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Signature



Using IP Address: 207.156.9.1

Timestamp

Sent: 3/5/2018
Viewed: 3/5/2018
Signed: 3/5/2018

In Person Signer Events

Signature

Timestamp

Editor Delivery Events

Status

Timestamp

Agent Delivery Events

Status

Timestamp

Intermediary Delivery Events

Status

Timestamp

Certified Delivery Events

Status

Timestamp

Carbon Copy Events

Status

Timestamp

Jonathan P. Sanford
JonathanSanford@flhsmv.gov
Chief Counsel
Florida Department of Highway Safety and Motor Vehicles
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

COPIED

Sent: 2/28/2018

Tiffany Allen
TiffanyAllen@flhsmv.gov
Paralegal
Florida Department of Highway Safety and Motor Vehicles
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

COPIED

Sent: 3/2/2018
Viewed: 3/2/2018

Data Listing Unit
DataListingUnit@flhsmv.gov
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

COPIED

Sent: 3/5/2018

Tiffany Allen
TiffanyAllen@flhsmv.gov
Paralegal
Florida Department of Highway Safety and Motor Vehicles
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

COPIED

Sent: 3/5/2018

Carbon Copy Events

Becky Parramore
BeckyParramore@flhsmv.gov
Leasing Consultant
Florida Department of Highway Safety and Motor Vehicles
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Status

COPIED

Timestamp

Sent: 3/5/2018

Melissa McKinlay
mmckinlay@pbcgov.org
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

COPIED

Sent: 3/5/2018

Jean Heald
jheald1@pbcgov.org
Security Level: Email, Account Authentication (None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

COPIED

Sent: 3/5/2018

Notary Events

Signature

Timestamp

Envelope Summary Events

Envelope Sent
Certified Delivered
Signing Complete
Completed

Status

Hashed/Encrypted
Security Checked
Security Checked
Security Checked

Timestamps

3/5/2018
3/5/2018
3/5/2018
3/5/2018

Payment Events

Status

Timestamps



MEMORANDUM OF UNDERSTANDING
FOR DRIVER'S LICENSE AND/OR MOTOR VEHICLE RECORD DATA EXCHANGE
Contract Number HSMV-0478-18

This Memorandum of Understanding (MOU) is made and entered into by and between
Palm Beach County Board of County Commissioners hereinafter referred to as
the Requesting Party, and the Florida Department of Highway Safety and Motor Vehicles, hereinafter 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 disclosure prohibitions contained in 18 U.S.C. §2721, the Driver's Privacy
Protection Act (hereinafter "DPPA"), Sections 119.0712(2) and 501.171, Florida Statutes, and other statutory
provisions

The Requesting Party is a government 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 and Motor Vehicle information to
the Requesting Party. The type of data requested and the statutory fees, if applicable, are agreed to by both
parties as indicated in Attachment II.

The Requesting Party is receiving a ☐ 9-digit ☐ 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 Inquiry - 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(2), Florida Statutes. Such inquiry is to be made on only vehicles involved in a crash. The Vehicle Identification Number (VIN) on which such inquiry is made must be involved in the crash for which a crash report number and the date of crash is provided to the Agency.
- F. Downstream Entity - Any individual, association, organization, or corporate entity who receives driver license and/or motor vehicle data from a Third Party End User in accordance with DPPA and Section 119.0712(2), Florida Statutes
- G. Driver License Information - Driver license and identification card data collected and maintained by the Providing Agency. This data includes personal information as defined in item N, below.
- H. Driver 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.
- I. Government Entity - Any federal, state, county, county officer, or city government, including any court or law enforcement agency.
- J. Highly Restricted Personal Information - Includes, but is not limited to, medical or disability information or social security number.
- K. Insurance Record - 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(2), Florida Statutes.
- L. Motor Vehicle Information - Title and registration data collected and maintained by the Providing Agency for vehicles. This information includes personal information as defined in item N, below.
- M. Parties - The Providing Agency and the Requesting Party.
- N. Personal Information - As described in Section 119.0712(2)(b), Florida Statutes and 18 U.S.C. S.2725, information found in the motor vehicle or driver record which includes, but is not limited to, the subject's driver identification number, name, address, (but not the 5 - digit zip code) and medical or disability information.
- O. 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.
- P. Providing Agency - The Department of Highway Safety and Motor Vehicles. The Providing Agency is responsible for granting access to driver license and/or motor vehicle data to the Requesting Party.
- Q. Registration Hold - A hold placed on the owner, vehicle or registration, intended to prevent extension or renewal of any motor vehicle registration.
- 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 record authorized for release and the associated statutory fees. Misuse of a Requesting Party Number to obtain information is strictly prohibited and shall be grounds for termination in accordance with Section X, Termination and Suspension.
- 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 and/or motor vehicle data from the Requesting Party in accordance with DPPA and Section 119.0712(2), 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

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

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

Under this MOU, the Requesting Party will be provided, via remote electronic means, information pertaining to driver licenses and vehicles, including personal information authorized to be released pursuant to Section 119.0712(2), Florida Statutes and DPPA. By executing this MOU, the Requesting Party agrees to maintain the confidential and exempt status of any and all information provided by the Providing Agency pursuant to this MOU and to ensure that any Third Party End Users accessing or utilizing said information shall do so in compliance with Section 119.0712(2), Florida Statutes and DPPA. Highly restricted personal information shall only be released in accordance with DPPA and Florida law. In addition, the Requesting Party agrees that insurance policy information shall only be utilized pursuant to Section 324.242(2), Florida Statutes.

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

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 the access method being requested.
 - 2. Allow the Requesting Party to electronically access data as authorized under this MOU.
 - 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 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 X., 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 and/or motor vehicle information pursuant to roles and times established other than scheduled maintenance or other uncontrollable disruptions. Scheduled maintenance normally occurs Sunday mornings between the hours of 6:00 A.M. and 10:00 A.M.
9. Provide a contact person for assistance with the implementation of this MOU.

B. The Requesting Party agrees to:

1. Use information only for the expressed purposes as described in Attachment I of this MOU.
2. 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.
3. 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, and/or telephone number of any Providing Agency employee without the express written consent of the Providing Agency.
4. Establish procedures to ensure that its employees and agents 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.
5. 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.
6. Use the information received from the Providing Agency only for the purposes authorized by this MOU. The Requesting Party shall not share or provide any information to another unauthorized entity, agency or person.
7. 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.
8. Defend, hold harmless and indemnify the Providing Agency and its employees or agents from

- any and all claims, actions, damages, or losses which may be brought or alleged against its employees or agents for the Requesting Party's negligent, improper, or unauthorized use or dissemination of information provided by the Providing Agency, to the extent allowed by law.
9. For Federal agencies: 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.
 10. Update user access/permissions upon reassignment of users within five (5) business days.
 11. Immediately inactivate user access/permissions following separation, or negligent, improper, or unauthorized use or dissemination of any information.
 12. 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 these records or otherwise make these records available for inspection within five (5) business days of a request by the Providing Agency.
 13. Pay all costs associated with electronic access of the Providing Agency's driver license and/or motor vehicle 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.
 14. Notify the Providing Agency within five (5) business days of any changes to the name, address, telephone number and/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.
 15. 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.
 16. 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 they are obligated to comply with all applicable provisions of law.
 17. Timely submit statements required in Section VI. Compliance and Control Measures, subsections B and C.
 18. 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.

V. Safeguarding Information

The Parties shall access, disseminate, use and maintain all information received under this MOU in a manner that ensures its confidentiality and proper utilization in accordance with Chapter 119, 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.

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

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.

The Requesting Party shall notify the Providing Agency of any of the following within five (5) business days:

- A. Termination of any agreement/contract between the Requesting Party and any other State/State Agency due to non-compliance with DPPA, data breaches, or any state laws relating to the protection of driver privacy. The Requesting Party shall also notify the Providing Agency if any State/State Agency declines to enter into an agreement/contract with the Requesting Party to provide DPPA protected data.
- B. Any pending litigation alleging DPPA violations or under any state law relating to the protection of driver privacy.
- C. 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 state law relating to the protection of driver privacy.
- D. 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 state law relating to the protection of driver privacy.
- E. A breach of security as defined by Section 501.171, Florida Statutes.

The Parties mutually agree to the following:

- A. 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.
- B. The Requesting Party shall not indemnify and shall not be liable to the Providing Agency for any driver license or motor vehicle information lost, damaged, or destroyed as a result of the electronic exchange of data pursuant to this MOU, except as otherwise provided in Section 768.28, Florida Statutes.
- C. Information obtained from the Providing Agency will be stored in a location that is physically and logically secure from access by unauthorized persons.
- D. The Requesting Party shall develop security requirements and standards consistent with Section 282.318, Florida Statutes, Florida Administrative Code Rule 74-2, and the Providing Data Exchange MOU (Rev. 05/2017)

- 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.
- E. 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.
- F. All personnel with access to the information exchanged under the terms of this MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency within ten (10) business days of a request.
- G. All personnel with access to the information will be instructed of, and acknowledge their understanding of the civil and criminal sanctions specified in state and Federal law for unauthorized use of the data. These acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency within ten (10) business days of a request.
- H. 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 VI. B below.
- I. 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.
- J. 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. **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 that data is being provided/received pursuant to this MOU to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure. The Requesting Party must submit an Internal Control and Data Security Audit from a currently licensed Certified Public Accountant, on or before the first anniversary of the execution date of this MOU or within one hundred twenty (120) days from receipt of a request from the Providing Agency. Government agencies may submit the Internal Control and Data Security Audit from their Agency's Internal Auditor or Inspector General. The audit shall indicate that the internal controls governing the use and dissemination of personal data have been evaluated in light of the requirements of this MOU, and applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. This includes both policies/procedures in place for personnel to follow and data security procedures/policies in place to protect personal data. The audit shall certify that the data security procedures/policies have been approved by a Risk Management IT Security Professional. The audit shall also certify that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence. The audit must have an original signature of the CPA and the Requesting Party's agency head, owner, officer, or control person designated by Letter of Delegation to execute contracts/agreements on their behalf. The audit shall be sent via Certified U.S. Mail to the Providing Agency as set forth in Section XI, Notices.
- B. **Annual Certification Statement** - The Requesting Party shall submit to the Providing Agency an annual statement 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 annually, within fifteen (15) business days after the anniversary of the execution date of this MOU. (NOTE: During any year in which an Internal Control and Data Security Audit is conducted, submission of the Internal Control and Data Security Audit may satisfy the requirement to submit an Annual Certification Statement.) Failure to timely submit the certification statement may result in an immediate termination of this MOU.

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

- 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 mailed to the Providing Agency Bureau Chief of Records at the address indicated in XI, Notices A., above. (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 within fifteen (15) business days from the date they were notified by the Providing Agency.

Consumer Complaint Point of Contact Information:

Name: Jean A. Heald

Email: jheald1@pbcbgov.org

Phone Number: 561-233-5432

- 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, 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 DPPA

protection and to provide the results of the investigation to the Requesting Party. The Requesting party shall provide the results of the investigation(s) and the documents and information collected therein to the Providing Agency within fifteen (15) business days.

VII. Liquidated Damages

The Providing Agency reserves the right to impose liquidated damages upon the Requesting Party.

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 data due to non-compliance with DPPA, Sections 119.0712(2) and 501.171, Florida Statutes, or any other state laws designed to protect a driver's privacy and motor vehicle information, the Providing Agency may impose upon the Requesting Party liquidated damages of up to \$25.00 per record.

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) 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.

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

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.

VIII. 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 X, Termination and Suspension. Once executed, this MOU supersedes all previous agreements between the parties regarding the same subject matter.

IX. 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.

X. 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) and 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/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 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.

XI. 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@fhsmv.gov

For the Requesting Party:

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

XII. Additional Database Access/Subsequent MOU's

The Parties understand and acknowledge that this MOU entitles the Requesting Party to specific information included within the scope 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.

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 execute 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 Providing Agency approval, to submit one of each of the following covering all executed MOU's: Certification; Audit; and/or to have conducted one comprehensive audit addressing internal controls for all executed MOU's. The Providing Agency shall have the sole discretion to approve or deny such request in whole or in part or to subsequently rescind an approved request based upon the Requesting Party's compliance with this MOU and/or any negative audit findings.

XIII. Public Records Requirements

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 contract term and following completion of the contract 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.

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 CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (850) 617-3101, OGCFiling@flhsmv.gov, OFFICE OF GENERAL COUNSEL, 2900 APALACHEE PARKWAY, and STE. A432, TALLAHASSEE, FL 32399-0504.

REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK

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

REQUESTING PARTY:

PALM BEACH COUNTY BOCC
Requesting Party Name

100 AUSTRALIAN AVE
Street Address

200
Suite

WEST PALM BEACH FL 33406
City State Zip Code

Approved as to Terms
and Conditions:
Risk Management

[Signature]
Department Director

BUSINESS POINT-OF-CONTACT:

Jean A. Heald
Printed/Typed Name

jheald1@pbccgov.org
Official Requesting Party Email Address

5612335432 561233-5420
Phone Number Fax Number

PROVIDING AGENCY:

Florida Department of Highway Safety
and Motor Vehicles
Providing Agency Name

2900 Apalachee Parkway
Street Address

Tallahassee, Florida 32399
City State Zip Code

BY:

[Signature]
Signature of Authorized Official

Melissa McKinlay
Printed/Typed Name

Mayor
Title

4/12/2018
Date

MMcKinlay@pbccgov.org
Official Requesting Party Email Address

561-355-2206
Phone Number

APPROVED AS TO FORM
AND LEGAL SUFFICIENCY

[Signature]
County Attorney

TECHNICAL POINT-OF-CONTACT:

Yunus Kazi

Printed/Typed Name

ykazi@pbccgov.org

Official Requesting Party Email Address

5613553409 5612427534
Phone Number Fax Number

BY:

DocuSigned by:

[Signature]
7E2E9F0980B2459
Signature of Authorized Official

Lisa M. Bassett

Printed/Typed Name

Chief Administrative Officer

Title

3/5/2018

Date

Lisabassett@flhsmv.gov

Official Providing Agency Email Address

850-617-3407

Phone Number

ATTACHMENT I

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

The Driver's Privacy Protection Act, 18 United States Code sections 2721 ("DPPA") makes personal information contained in motor vehicle or driver license records confidential and exempt from disclosure. Personal information in a motor vehicle or driver license record includes, but is not limited to, an individual's social security number, driver license or identification number, name, 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) 1, as listed on page 3 of this form.

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

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

DPPA Exemption Claimed	Description of How Requesting Party Qualifies for Exemption:	Description of how Data will be used:
1	As a Government Agency carrying out its functions	For determining eligibility of driver license of current and prospective new hires operating government vehicles. Status checks will be provided through program DSS600, Batch/FTP process.

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.

Melissa McKinlay
Signature of Authorized Official

Mayor
Title

Melissa McKinlay
Printed Name

Palm Beach County
Name of Agency/Entity

January 17, 2018
Date

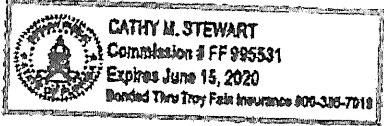
STATE OF Florida
COUNTY OF Palm Beach

Sworn to (or affirmed) and subscribed before me this 17th day of January, 2018, by
Melissa McKinlay

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

Cathy M. Stewart
NOTARY PUBLIC (print name)

Cathy M. Stewart
NOTARY PUBLIC (sign name)
My Commission Expires: June 15, 2020



APPROVED AS TO FORM
AND LEGAL SUFFICIENCY
Helene C. Lapid
County Attorney

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 343 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 --Jobs and Processes Selected

Mode of Access	Type of Data Requested	Statutory Fees (subject to change by the Legislature)
Batch/Email/CD*	DL data	\$0.01/record, per s 322.20, F. S.
	MV data	\$0.01/record, per s 320.05, F. S.
	DL Status	\$0.01, \$0.50, \$2.00/record, per s 320.05, F.S.
	X MV Status/MV Record	\$0.01, \$0.50, \$2.00/record, per s 320.05, F.S.
	DL Record Search with Transcript	\$0.01, \$8.00, \$10.00, \$2.00/record, per s 322.20, F.S.
	DL Transcript (3 year)	\$8.00/record, per s. 322.20, F.S.
	DL Transcript (7 Year or Complete)	\$10.00/record, per s. 322.20, F.S.
	IP Address(es) Please See Attachment	X No charge
Driver Transcript Web Service	DL Transcript (3 year)	\$8.00/record, per s. 322.20, F.S.
	DL Transcript (7 Year or Complete)	\$10.00/record, per s. 322.20, F.S.
Public Access Web Service	X DL Status	No charge
	MV Record	\$0.50/record, per s. 320.05, F.S.
	Insurance Record	\$0.50/record, per s. 320.05, F.S.
	Parking Permit Record	\$0.50/record, per s. 320.05, F.S.
		X No charge
Web Service/ Batch	Residency Verification	No charge

DATA ACCESS SPECIFICATIONS

ATTACHMENT II-jobs and Processes Selected

IP Address (es):

151.132.206.26
151.132.206.250
151.132.106.25
151.132.106.250
151.132.200.6

Terry L. Rhodes
Executive Director

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



Rick Scott
Governor

Pam Bondi
Attorney General

Jeff Atwater
Chief Financial Officer

Adam Putnam
Commissioner of Agriculture

Data Access Technical Specifications Questionnaire
Agency: Palm Beach County Board of County Commissioners

- I. Access Method or Condition. The Requesting Party shall attest to their respective statutory eligibility by completing the Florida Department of Highway Safety and Motor Vehicles Request for Exempt Personal Information in a Driver License/Motor Vehicle Record form.
- II. Access Specifications. Please provide a description of the specific data being requested, the statutory authority/DPPA exemption, and which method of receiving the data is being requested in the space below:

Description of specific data needed	Description of specific use of data, to include statutory and/or DPPA authority to receive data.
1. Drivers license eligibility check (Batch process)	For determining the eligibility of driver license of current and prospective new hires operating government vehicles. Status checks will be provided through the DSS600, Batch/FTP process.
2. Drivers license eligibility check (Web Access)	For validating Palm Tran's bus operator and Paratransit driver licenses via the Public Access webservice.

III. Method of receiving/accessing data:

Public Access / Web service: This service provides basic driver information and eligibility. It also provides motor vehicle information. This service is available to private agencies for \$0.50 per record search and is at no charge for governmental agencies.

Driver Transcript / Web Service: 3 year, 7 year and complete driver license transcripts are available through this service. This service is available to private, city and county agencies for \$8.00 for a 3 year transcript and \$10.00 for a 7 year or complete transcript per record. Transcripts are provided at no charge to law enforcement agency, federal and state agencies.

The requestor's software communicates with our software over the Internet; The API specification for the driver transcripts and public access web service can be found within the following URL: <https://betaservices.flhsmv.gov/transcripts/> and URL: <https://betaservices.flhsmv.gov/PublicAccess/>. Access is by a user id and a password. There is no web page, as such, for the user.

Batch/FTP: The requestor submits a file with multiple records that they want matched through a standard file transfer protocol (SFTP) from their server to one of ours. Our processes pulls the file, run a program or series of programs, and return matching records or records meeting established criteria by FTP for the requestor to pick up. Driver license transcripts, DL status check, motor vehicle records, can be provided in this process also. Note: the requesting party must transition to web services as they become available for these processes.

We have different kinds of FTP processes to suit your various needs. A few are listed below.

DMS485 - This program provides a driver transcript. This program reviews each record and returns transcripts for only those driver records who have had a sanction or a conviction added onto their record within the past 1, 3, 6, 12, 24 or 36 month (lookback) period. A transcript will NOT be returned on those drivers who do not meet the above criteria. Transcripts requested can be (\$8.00) 3 year, (\$10.00) 7 year or (\$10.00) complete; \$2.00 for record not found and \$0.01 for a DL# not meeting the criteria.

DSS600/605 - This does not provide a driver transcript but will provide pertinent information only on those drivers whose status is ineligible. You will receive such information as the type of sanction, reason, and effective date. A response will not be given on eligible drivers. License type is NOT provided in the output file. A fee of .50 for each inquiry whose status is ineligible and a fee of .01 for all drivers whose status is eligible. This service is free to all government agencies.

DTR060 - Driver license transcript programs/ Returns transcripts on all DL# provided, no criteria set. This service is available to private entities, city, county and governmental agencies for \$8.00 for a 3 year transcript and \$10.00 for a 7 year or complete transcript per record. Transcripts are at no charge to LEA, federal and state agencies.

DL/MV database - We also provide a Driver License and Motor Vehicle Database for \$0.01 per record, with weekly or monthly updates.

Payment process: Automatic debits to your bank account will be made whenever the services are utilized. Prior to setup for above services, a debit authorization form should be completed by you and your banking institution and returned to us. This will allow DHSMV to debit your account. Please note that there is no other method of payment when utilizing the above services for a charge.

Entity or Agency name:

Palm Beach Board of County Commissioners

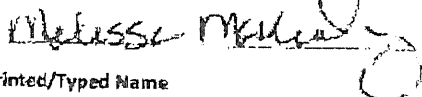
Entity or Agency Address:

301 N Olive Ave

City, State, Zip:

West Palm Beach, FL 33401

Signature of Authorized Official



Printed/Typed Name

Melissa McKinlay

Title

Mayor

Date

1/30/18

E-Mail Address

MMcKinlay@pbccgov.org

Phone Number

561-355-2206

Web Application Access

Contact information of the person and serves as liaison for DHSMV

Printed/typed Name

Yunus Kazi

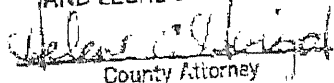
E-Mail Address

ykazi@pbccgov.org

Phone Number

561-335-3409

APPROVED AS TO FORM
AND LEGAL SUFFICIENCY


County Attorney

If you are not a governmental agency, please include the company's articles of incorporation or certificate with the Florida Division of Corporations along with FEIN number

FEIN Number

Terry L. Rhodes
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0600
www.flhsmv.gov



Rick Scott
Governor

Pam Bondi
Attorney General

Jeff Atwater
Chief Financial Officer

Adam Putnam
Commissioner of Agriculture

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 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:

(01/2017)

Page 2 of 3

5. In the last ten (10) years, has there been any instance where an owner, officer, or control person¹ 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?
Employees who handle confidential data are required to complete Ethics compliance and HIPAA training.
8. Please provide the URL to your company or agency's website that will be used to provide access to the data being requested: Discover.Ph.gov.org.

In addition, the following documents are required:

- A copy of your business license.
- A copy of your State of Florida corporation licensure or certification.
- 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.

Page 3 of 3

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.

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

Melissa McKinlay
Signature of Authorized Official

Melissa McKinlay
Printed/Typed Name

Mayor
Title

January 17, 2018
Date

Palm Beach County
NAME OF AGENCY/ENTITY

APPROVED AS TO FORM
AND LEGAL SUFFICIENCY
[Signature]
County Attorney

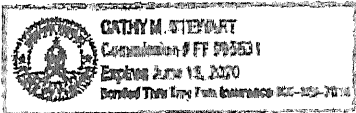
STATE OF Florida
COUNTY OF Palm Beach

Sworn to (or affirmed) and subscribed before me this 17th day of January, 2018, by
Melissa McKinlay

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

Cathy M. Stepiant
NOTARY PUBLIC (print name)

Cathy M. Stepiant
NOTARY PUBLIC (sign name)
My Commission Expires: June 15, 2020



Terry L. Rhodes
Executive Director

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



Rick Scott
Governor

Pam Bondi
Attorney General

Jeff Atwater
Chief Financial Officer

Adam Putnam
Commissioner of Agriculture

CERTIFICATION STATEMENT

Under penalty of perjury I have read the requirements contained in the Memorandum of Understanding, Florida Administrative Code 74-2, and the Department of Highway Safety and Motor Vehicles Vendor IT Security Policy and declare that the following is true:

The Requesting Party Palm Beach County Board Of County Commissioners hereby certifies that the Requesting Party has appropriate internal controls in place at all times 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 Florida
COUNTY OF Palm Beach

Sworn to (or affirmed) and subscribed before me this 17th day of June, 2018, by
Melissa McKinlay

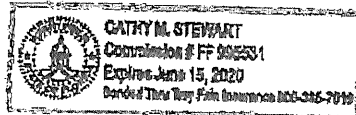
Personally Known ☒ OR Produced Identification ☐
Type of Identification Produced _____

Cathy M. Stewart
NOTARY PUBLIC (print name)

Cathy M. Stewart
NOTARY PUBLIC (sign name)
My Commission Expires: June 15, 2020

Melissa McKinlay
Signature

Melissa McKinlay
Printed Name



Mayor
Title

June 17, 2018
Date

Palm Beach County
NAME OF AGENCY

APPROVED AS TO FORM
AND LEGAL SUFFICIENCY

Debra C. Hargis
County Clerk

• Service • Integrity • Courtesy • Professionalism • Innovation • Excellence •
An Equal Opportunity Employer



**MEMORANDUM OF UNDERSTANDING
FOR DRIVER'S LICENSE AND/OR MOTOR VEHICLE RECORD DATA EXCHANGE
Contract Number HSMV-_____**

This Memorandum of Understanding (MOU) is made and entered into by and between Palm Beach County Board of County Commissioners hereinafter referred to as the Requesting Party, and the Florida Department of Highway Safety and Motor Vehicles, hereinafter 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 disclosure prohibitions contained in 18 U.S.C. §2721, the Driver's Privacy Protection Act (hereinafter "DPPA"), Sections 119.0712(2) and 501.171, Florida Statutes, and other statutory provisions.

The Requesting Party is a government 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 and Motor Vehicle information to the Requesting Party. The type of data requested and the statutory fees, if applicable, are agreed to by both parties as indicated in Attachment II.

The Requesting Party is receiving a ☐ 9-digit ☐ 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 Inquiry - 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(2), Florida Statutes. Such inquiry is to be made on only vehicles involved in a crash. The Vehicle Identification Number (VIN) on which such inquiry is made must be involved in the crash for which a crash report number and the date of crash is provided to the Agency.
- F. Downstream Entity - Any individual, association, organization, or corporate entity who receives driver license and/or motor vehicle data from a Third Party End User in accordance with DPPA and Section 119.0712(2), Florida Statutes.
- G. Driver License Information - Driver license and identification card data collected and maintained by the Providing Agency. This data includes personal information as defined in item N, below.
- H. Driver 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.
- I. Government Entity - Any federal, state, county, county officer, or city government, including any court or law enforcement agency.
- J. Highly Restricted Personal Information - Includes, but is not limited to, medical or disability information or social security number.
- K. Insurance Record - 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(2), Florida Statutes.
- L. Motor Vehicle Information - Title and registration data collected and maintained by the Providing Agency for vehicles. This information includes personal information as defined in item N, below.
- M. Parties - The Providing Agency and the Requesting Party.
- N. Personal Information - As described in Section 119.0712(2)(b), Florida Statutes and 18 U.S.C. S.2725, information found in the motor vehicle or driver record which includes, but is not limited to, the subject's driver identification number, name, address, (but not the 5 – digit zip code) and medical or disability information.
- O. 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.
- P. Providing Agency - The Department of Highway Safety and Motor Vehicles. The Providing Agency is responsible for granting access to driver license and/or motor vehicle data to the Requesting Party.
- Q. Registration Hold - A hold placed on the owner, vehicle or registration, intended to prevent extension or renewal of any motor vehicle registration.
- 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 record authorized for release and the associated statutory fees. Misuse of a Requesting Party Number to obtain information is strictly prohibited and shall be grounds for termination in accordance with Section X, Termination and Suspension.
- 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 and/or motor vehicle data from the Requesting Party in accordance with DPPA and Section 119.0712(2), 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

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

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

Under this MOU, the Requesting Party will be provided, via remote electronic means, information pertaining to driver licenses and vehicles, including personal information authorized to be released pursuant to Section 119.0712(2), Florida Statutes and DPPA. By executing this MOU, the Requesting Party agrees to maintain the confidential and exempt status of any and all information provided by the Providing Agency pursuant to this MOU and to ensure that any Third Party End Users accessing or utilizing said information shall do so in compliance with Section 119.0712(2), Florida Statutes and DPPA. Highly restricted personal information shall only be released in accordance with DPPA and Florida law. In addition, the Requesting Party agrees that insurance policy information shall only be utilized pursuant to Section 324.242(2), Florida Statutes.

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

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 the access method being requested.
2. Allow the Requesting Party to electronically access data as authorized under this MOU.
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 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 X., 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 and/or motor vehicle information pursuant to roles and times established other than scheduled maintenance or other uncontrollable disruptions. Scheduled maintenance normally occurs Sunday mornings between the hours of 6:00 A.M. and 10:00 A.M.
9. Provide a contact person for assistance with the implementation of this MOU.

B. The Requesting Party agrees to:

1. Use information only for the expressed purposes as described in Attachment I of this MOU.
2. 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.
3. 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, and/or telephone number of any Providing Agency employee without the express written consent of the Providing Agency.
4. Establish procedures to ensure that its employees and agents 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.
5. 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.
6. Use the information received from the Providing Agency only for the purposes authorized by this MOU. The Requesting Party shall not share or provide any information to another unauthorized entity, agency or person.
7. 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.
8. Defend, hold harmless and indemnify the Providing Agency and its employees or agents from

- any and all claims, actions, damages, or losses which may be brought or alleged against its employees or agents for the Requesting Party's negligent, improper, or unauthorized use or dissemination of information provided by the Providing Agency, to the extent allowed by law.
9. For Federal agencies: 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.
 10. Update user access/permissions upon reassignment of users within five (5) business days.
 11. Immediately inactivate user access/permissions following separation, or negligent, improper, or unauthorized use or dissemination of any information.
 12. 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 these records or otherwise make these records available for inspection within five (5) business days of a request by the Providing Agency.
 13. Pay all costs associated with electronic access of the Providing Agency's driver license and/or motor vehicle 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.
 14. Notify the Providing Agency within five (5) business days of any changes to the name, address, telephone number and/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.
 15. 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.
 16. 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 they are obligated to comply with all applicable provisions of law.
 17. Timely submit statements required in Section VI. Compliance and Control Measures, subsections B and C.
 18. 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.

V. Safeguarding Information

The Parties shall access, disseminate, use and maintain all information received under this MOU in a manner that ensures its confidentiality and proper utilization in accordance with Chapter 119, 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.

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

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.

The Requesting Party shall notify the Providing Agency of any of the following within five (5) business days:

- A. Termination of any agreement/contract between the Requesting Party and any other State/State Agency due to non-compliance with DPPA, data breaches, or any state laws relating to the protection of driver privacy. The Requesting Party shall also notify the Providing Agency if any State/State Agency declines to enter into an agreement/contract with the Requesting Party to provide DPPA protected data.
- B. Any pending litigation alleging DPPA violations or under any state law relating to the protection of driver privacy.
- C. 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 state law relating to the protection of driver privacy.
- D. 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 state law relating to the protection of driver privacy.
- E. A breach of security as defined by Section 501.171, Florida Statutes.

The Parties mutually agree to the following:

- A. 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.
- B. The Requesting Party shall not indemnify and shall not be liable to the Providing Agency for any driver license or motor vehicle information lost, damaged, or destroyed as a result of the electronic exchange of data pursuant to this MOU, except as otherwise provided in Section 768.28, Florida Statutes.
- C. Information obtained from the Providing Agency will be stored in a location that is physically and logically secure from access by unauthorized persons.
- D. The Requesting Party shall develop security requirements and standards consistent with Section 282.318, Florida Statutes, Florida Administrative Code Rule 74-2, and the Providing Data Exchange MOU (Rev. 05/2017)

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.

- E. 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.
- F. All personnel with access to the information exchanged under the terms of this MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency within ten (10) business days of a request.
- G. All personnel with access to the information will be instructed of, and acknowledge their understanding of the civil and criminal sanctions specified in state and Federal law for unauthorized use of the data. These acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency within ten (10) business days of a request.
- H. 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 VI. B below.
- I. 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.
- J. 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. 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 that data is being provided/received pursuant to this MOU to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure. The Requesting Party must submit an Internal Control and Data Security Audit from a currently licensed Certified Public Accountant, on or before the first anniversary of the execution date of this MOU or within one hundred twenty (120) days from receipt of a request from the Providing Agency. Government agencies may submit the Internal Control and Data Security Audit from their Agency's Internal Auditor or Inspector General. The audit shall indicate that the internal controls governing the use and dissemination of personal data have been evaluated in light of the requirements of this MOU, and applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. This includes both policies/procedures in place for personnel to follow and data security procedures/policies in place to protect personal data. The audit shall certify that the data security procedures/policies have been approved by a Risk Management IT Security Professional. The audit shall also certify that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence. The audit must have an original signature of the CPA and the Requesting Party's agency head, owner, officer, or control person designated by Letter of Delegation to execute contracts/agreements on their behalf. The audit shall be sent via Certified U.S. Mail to the Providing Agency as set forth in Section XI, Notices.

B. Annual Certification Statement - The Requesting Party shall submit to the Providing Agency an annual statement 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 annually, within fifteen (15) business days after the anniversary of the execution date of this MOU. (NOTE: During any year in which an Internal Control and Data Security Audit is conducted, submission of the Internal Control and Data Security Audit may satisfy the requirement to submit an Annual Certification Statement.) Failure to timely submit the certification statement may result in an immediate termination of this MOU.

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

- 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 mailed to the Providing Agency Bureau Chief of Records at the address indicated in XI, Notices A., above. (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 within fifteen (15) business days from the date they were notified by the Providing Agency.

Consumer Complaint Point of Contact Information:

Name: Jean A. Heald

Email: jheald1@pbcgov.org

Phone Number: 561-233-5432

- 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, 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 DPPA

protection and to provide the results of the investigation to the Requesting Party. The Requesting party shall provide the results of the investigation(s) and the documents and information collected therein to the Providing Agency within fifteen (15) business days.

VII. Liquidated Damages

The Providing Agency reserves the right to impose liquidated damages upon the Requesting Party.

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 data due to non-compliance with DPPA, Sections 119.0712(2) and 501.171, Florida Statutes, or any other state laws designed to protect a driver's privacy and motor vehicle information, the Providing Agency may impose upon the Requesting Party liquidated damages of up to \$25.00 per record.

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) 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.

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

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.

VIII. 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 X, Termination and Suspension. Once executed, this MOU supersedes all previous agreements between the parties regarding the same subject matter.

IX. 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.

X. 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) and 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/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 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.

XI. 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 Point-of-Contact listed on the signature page.

XII. Additional Database Access/Subsequent MOU's

The Parties understand and acknowledge that this MOU entitles the Requesting Party to specific information included within the scope 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.

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 execute 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 Providing Agency approval, to submit one of each of the following covering all executed MOU's: Certification; Audit; and/or to have conducted one comprehensive audit addressing internal controls for all executed MOU's. The Providing Agency shall have the sole discretion to approve or deny such request in whole or in part or to subsequently rescind an approved request based upon the Requesting Party's compliance with this MOU and/or any negative audit findings.

XIII. Public Records Requirements

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 contract term and following completion of the contract 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.

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 CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (850) 617-3101, OGCFiling@flhsmv.gov, OFFICE OF GENERAL COUNSEL, 2900 APALACHEE PARKWAY, and STE. A432, TALLAHASSEE, FL 32399-0504.

REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK

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

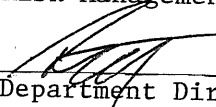
REQUESTING PARTY:

PAWM BEACH COUNTY BOCC
Requesting Party Name
C/O RISK MANAGEMENT
100 AUSTRALIAN AVE
Street Address

200
Suite

WEST PALM BEACH, FL 33406
City State Zip Code

Approved as to Terms
and Conditions:
Risk Management


Department Director

BUSINESS POINT-OF-CONTACT:

Jean A. Heald

Printed/Typed Name

jheald1@pbcgov.org

Official Requesting Party Email Address

5612335432 / 561233-5420

Phone Number Fax Number

PROVIDING AGENCY:

Florida Department of Highway Safety
and Motor Vehicles
Providing Agency Name

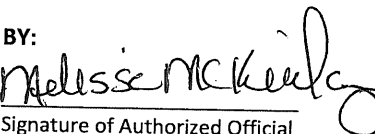
2900 Apalachee Parkway
Street Address

Suite

Tallahassee, Florida 32399

City State Zip Code

BY:


Signature of Authorized Official

Melissa McKinlay
Printed/Typed Name

Mayor
Title

1/17/2018
Date

Official Requesting Party Email Address

Phone Number

TECHNICAL POINT-OF-CONTACT:

Yunus Kazi

Printed/Typed Name

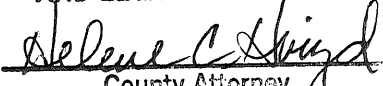
ykazi@pbcgov.org

Official Requesting Party Email Address

5613553409 / 5612427534

Phone Number Fax Number

APPROVED AS TO FORM
AND LEGAL SUFFICIENCY


County Attorney

BY:

Signature of Authorized Official

Printed/Typed Name

Title

Date

Official Providing Agency Email Address

Phone Number

ATTACHMENT I

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

The Driver's Privacy Protection Act, 18 United States Code sections 2721("DPPA") makes personal information contained in motor vehicle or driver license records confidential and exempt from disclosure. Personal information in a motor vehicle or driver license record includes, but is not limited to, an individual's social security number, driver license or identification number, name, 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)
1 _____, as listed on page 3 of this form.

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

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

DPPA Exemption Claimed	Description of How Requesting Party Qualifies for Exemption:	Description of how Data will be used:
1	As a Government Agency carrying out its functions	For determining eligibility of driver license of current and prospective new hires operating government vehicles. Status checks will be provided through program DSS600, Batch/FTP process.

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.

Melissa McKinlay
Signature of Authorized Official

Mayor
Title

Melissa McKinlay
Printed Name

Palm Beach County
Name of Agency/Entity

January 17, 2020
Date

STATE OF Florida
COUNTY OF Palm Beach

Sworn to (or affirmed) and subscribed before me this 17th day of January, 2018, by
Melissa McKinlay.

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

Cathy M. Stewart
NOTARY PUBLIC (print name)

Cathy M. Stewart
NOTARY PUBLIC (sign name)
My Commission Expires: June 15, 2020



APPROVED AS TO FORM
AND LEGAL SUFFICIENCY
Helene C. Guizd
County Attorney

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 –Jobs and Processes Selected

Mode of Access	Type of Data Requested		Statutory Fees (subject to change by the Legislature)	
Batch/Email/CD*		DL data		\$0.01/record, per S 322.20, F. S.
		MV data		\$0.01/record, per S 320.05, F.S.
		DL Status		\$0.01, \$0.50, \$2.00/record, per S 320.05, F.S.
	X	MV Status/MV Record		\$0.01, \$0.50, \$2.00/record, per S 320.05, F.S.
		DL Record Search with Transcript		\$0.01, \$8.00, \$10.00, \$2.00/record, per S 322.20, F.S.
		DL Transcript (3 year)		\$8.00/record, per s. 322.20, F.S.
		DL Transcript (7 Year or Complete)		\$10.00/record, per s. 322.20, F.S.
			X	No charge
		IP Address(es) <u>Please See Attachment</u>		
Driver Transcript Web Service				
		DL Transcript (3 year)		\$8.00/record, per s. 322.20, F.S.
		DL Transcript (7 Year or Complete)		\$10.00/record, per s. 322.20, F.S.
				No charge
Public Access Web Service	X	DL Status		\$0.50/record, per s. 320.05, F.S.
		MV Record		\$0.50/record, per s. 320.05, F.S.
		Insurance Record		\$0.50/record, per s. 320.05, F.S.
		Parking Permit Record		\$0.50/record, per s. 320.05, F.S.
			X	No charge
Web Service/ Batch		Residency Verification		No charge

DATA ACCESS SPECIFICATIONS

ATTACHMENT II-jobs and Processes Selected

IP Address (es):

151.132.206.26
151.132.206.250
151.132.106.25
151.132.106.250
151.132.200.6

Terry L. Rhodes
Executive Director

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



Rick Scott
Governor

Pam Bondi
Attorney General

Jeff Atwater
Chief Financial Officer

Adam Putnam
Commissioner of Agriculture

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 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:

(01/2017)

5. In the last ten (10) years, has there been any instance where an owner, officer, or control person¹ 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?
Employees who handle confidential data are required to complete Ethics compliance and HIPAA training.

8. Please provide the URL to your company or agency's website that will be used to provide access to the data being requested: Discover.Pbcgov.org.

In addition, the following documents are required:

- A copy of your business license.
- A copy of your State of Florida corporation licensure or certification.
- 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.

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.

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

Melissa McKinlay
Signature of Authorized Official

Melissa McKinlay
Printed/Typed Name

Mayor
Title

January 17, 2018
Date

Palm Beach County
NAME OF AGENCY/ENTITY

APPROVED AS TO FORM
AND LEGAL SUFFICIENCY
Debra C. Boyd
County Attorney

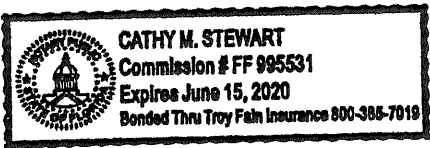
STATE OF Florida
COUNTY OF Palm Beach

Sworn to (or affirmed) and subscribed before me this 17th day of January, 20 18, by
Melissa McKinlay.

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

Cathy M. Stewart
NOTARY PUBLIC (print name)

Cathy M. Stewart
NOTARY PUBLIC (sign name)
My Commission Expires: June 15, 2020



Terry L. Rhodes
Executive Director



Rick Scott
Governor

Pam Bondi
Attorney General

Jeff Atwater
Chief Financial Officer

Adam Putnam
Commissioner of Agriculture

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 74-2, and the Department of Highway Safety and Motor Vehicles Vendor IT Security Policy and declare that the following is true:

The Requesting Party Palm Beach County Board Of County Commissioners hereby certifies that the Requesting Party has appropriate internal controls in place at all times 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 Florida
COUNTY OF Palm Beach

Sworn to (or affirmed) and subscribed before me this 17th day of January, 2018, by
Melissa McKinlay.

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

Cathy M. Stewart
NOTARY PUBLIC (print name)

Cathy M. Stewart
NOTARY PUBLIC (sign name)
My Commission Expires: June 15, 2020

Melissa McKinlay
Signature

Melissa McKinlay
Printed Name



Mayor
Title

January 17, 2018
Date

Palm Beach County
NAME OF AGENCY

APPROVED AS TO FORM
AND LEGAL SUFFICIENCY
Deleene C. Strickland
County Attorney

CHAPTER 74-2
INFORMATION TECHNOLOGY SECURITY

74-2.001	Purpose and Applicability; Definitions
74-2.002	Identify
74-2.003	Protect
74-2.004	Detect
74-2.005	Respond
74-2.006	Recover

74-2.001 Purpose and Applicability; Definitions

(1) Purpose and Applicability.

(a) Rules 74-2.001 through 74-2.006, F.A.C., will be known as the Florida Cybersecurity Standards (FCS).

(b) This rule establishes cybersecurity standards for information technology (IT) resources. These standards are documented in Rules 74-2.001 through 74-2.006, F.A.C. State Agencies must comply with these standards in the management and operation of state IT resources. This rule is modeled after the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014, and the Federal Information Security Management Act of 2002 (44 U.S.C. §3541, et seq.). For the convenience of the reader cross-references to these documents and Special Publications issued by the NIST are provided throughout the FCS as they may be helpful to agencies when drafting their security procedures. The Florida Cybersecurity Standards:

1. Establish minimum standards to be used by state agencies to secure IT resources. The FCS consist of five high-level functions: Identify, Protect, Detect, Respond, and Recover. These functions support lifecycle management of IT risk. The functions identify underlying key categories and subcategories for each function. Subcategories contain specific IT controls. The FCS is visually represented as follows:

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Category Unique Identifier subcategory references are detailed in Rules 74-2.002 – 74-2.006, F.A.C., and are used throughout the FCS as applicable.

2. Define minimum management, operational, and technical security controls to be used by state agencies to secure IT resources.

3. Allow authorizing officials to employ compensating security controls or deviate from minimum standards when the agency is unable to implement a security standard or the standard is not cost-effective due to the specific nature of a system or its environment. The agency shall document the reasons why the minimum standards cannot be satisfied and the compensating controls to be employed. After the agency analyzes the issue and related risk a compensating security control or deviation may be employed if the agency documents the analysis and risk steering workgroup accepts the associated risk. This documentation is exempt from Section 119.07(1), F.S., pursuant to Sections 282.318 (4)(d) and (4)(f), F.S., and, shall be securely submitted to AST upon acceptance.

(2) Each agency shall:

(a) Perform an assessment that documents the gaps between requirements of this rule and controls that are in place.

(b) Submit the assessment to AST with the agency's strategic and operational plan.

(c) Annually update the assessment to reflect progress toward compliance with this rule.

(3) Definitions.

(a) The following terms are defined:

1. Agency – shall have the same meaning as state agency, as provided in Section 282.0041, F.S., except that, per Section 282.318(2), F.S., the term also includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

2. Agency-owned (also agency-managed) – any device, service, or technology owned, leased, or managed by the agency for which an agency through ownership, configuration management, or contract has established the right to manage security configurations, including provisioning, access control, and data management.

3. Breach – see Section 282.0041(2), F.S.

4. Compensating security controls – a management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a required security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an IT resource.

5. Confidential information – records that, pursuant to Florida's public records laws or other controlling law, are exempt from public disclosure.

6. Critical infrastructure – the physical and cyber systems and assets so vital to Florida that their incapacity or destruction would have a debilitating effect on security, state economic security, state public health or safety, or any combination thereof.

7. Critical process – a process that is susceptible to fraud, cyberattack, unauthorized activity, or seriously impacting an agency's mission.

8. Customer – an entity in receipt of services or information rendered by a state agency. This term does not include state agencies with regard to information sharing activities.

9. Data-at-rest – stationary data which is stored physically in any digital form.

10. External partners – non-state agency entities doing business with a state agency, including other governmental entities, third parties, contractors, vendors, suppliers and partners. External partners does not include customers.

11. Information Security Manager (ISM) – the person appointed pursuant to Section 282.318(4)(a), F.S.

12. Information system owner – the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

13. Industry sector(s) – the following major program areas of state government: Health and Human Services, Education, Government Operations, Criminal and Civil Justice, Agriculture and Natural Resources, and Transportation and Economic Development.

14. Information technology resources (IT resources) – see Section 282.0041(13), F.S.

15. Legacy applications – programs or applications inherited from languages, platforms, and techniques earlier than current technology. These applications may be at or near the end of their useful life, but are still required to meet mission objectives or fulfill program area requirements.

16. Personal information – see Sections 501.171(1)(g)1. and 817.568, F.S.

17. Separation of Duties – an internal control concept of having more than one person required to complete a critical process. This is an internal control intended to prevent fraud, abuse, and errors.

18. Stakeholder – a person, group, organization, or state agency involved in or affected by a course of action related to state agency-owned IT resources.

19. User – a worker or non-worker who has been provided access to a system or data.

20. Workforce – employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency (see User; Worker).

21. Worker – a member of the workforce. A worker may or may not use IT resources. This includes employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency.

(b) With the exception of the terms identified in subparagraphs 1.-4., the NIST Glossary of Key Information Security Terms, Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce (May 2013), maintained at: <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>, is hereby incorporated by reference into this rule: <http://www.flrules.org/Gateway/reference.asp?No=Ref-06494>.

1. Risk assessment – see Section 282.0041(18), F.S.

2. Continuity Of Operations Plan (COOP) – disaster-preparedness plans created pursuant to Section 252.365(3), F.S.

3. Incident – see Section 282.0041(10), F.S.

4. Threat – see Section 282.0041(26), F.S.

Rulemaking Authority 282.318(5) FS. Law Implemented 282.318(3) FS. History--New 3-10-16.

74-2.002 Identify.

The identify function of the FCS is visually represented as such:

Function	Category	Subcategory
Identify (ID)	Asset Management (AM)	ID.AM-1: Inventory agency physical devices and systems
		ID.AM-2: Inventory agency software platforms and applications
		ID.AM-3: Map agency communication and data flows
		ID.AM-4: Catalog interdependent external information systems
		ID.AM-5: Prioritize IT resources based on classification, criticality, and business value
		ID.AM-6: Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders
	Business Environment (BE)	ID.BE-1: Identify and communicate the agency's role in the business mission/processes
		ID.BE-2: Identify and communicate the agency's place in critical infrastructure and its industry sector to workers
		ID.BE-3: Establish and communicate priorities for agency mission, objectives, and activities
		ID.BE-4: Identify dependencies and critical functions for delivery of critical services
		ID.BE-5: Implement resiliency requirements to support the delivery of critical services
	Governance (GV)	ID.GV-1: Establish an organizational information security policy
		ID.GV-2: Coordinate and align information security roles & responsibilities with internal roles and external partners
		ID.GV-3: Understand and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations
		ID.GV-4: Ensure that governance and risk management processes address cybersecurity risks
	Risk Assessment (RA)	ID.RA-1: Identify and document asset vulnerabilities
		ID.RA-2: Receive threat and vulnerability information from information sharing forums and sources
		ID.RA-3: Identify and document threats, both internal and external
		ID.RA-4: Identify potential business impacts and likelihoods
		ID.RA-5: Use threats, vulnerabilities, likelihoods, and impacts to determine risk

	Risk Management Strategy (RM)	ID.RA-6: Identify and prioritize risk responses
		ID.RM-1: Establish, manage, and ensure organizational stakeholders understand the approach to be employed via the risk management processes
		ID.RM-2: Determine and clearly express organizational risk tolerance
		ID.RM-3: Ensure that the organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

(1) Asset Management. Each agency shall ensure that IT resources are identified and managed. Identification and management shall be consistent with the IT resource's relative importance to business objectives and the organization's risk strategy. Specifically, each agency shall:

- (a) Ensure that physical devices and systems within the organization are inventoried and managed (ID.AM-1).
- (b) Ensure that software platforms and applications within the organization are inventoried and managed (ID.AM-2).
- (c) Ensure that organizational communication and data flows are mapped and systems are designed or configured to regulate information flow based on data classification (ID.AM-3). Each agency shall:
 - 1. Establish procedures that ensure only agency-owned or approved IT resources are connected to the agency internal network and resources.
 - 2. Design and document its information security architecture using a defense-in-breadth approach. Design and documentation shall be assessed and updated periodically based on an agency-defined, risk-driven frequency that considers potential threat vectors (i.e., paths or tools that a threat actor may use to attack a target).
 - 3. Consider diverse suppliers when designing the information security architecture.
- (d) Each agency shall ensure that interdependent external information systems are catalogued (ID.AM-4). Agencies shall:
 - 1. Verify or enforce required security controls on interconnected external IT resources in accordance with the information security policy or security plan.
 - 2. Implement service level agreements for non-agency provided technology services to ensure appropriate security controls are established and maintained.
 - 3. For non-interdependent external IT resources, execute information sharing or processing agreements with the entity receiving the shared information or hosting the external system in receipt of shared information.
 - 4. Restrict or prohibit portable storage devices either by policy or a technology that enforces security controls for such devices.
 - 5. Authorize and document inter-agency system connections.
 - 6. Require (e.g., contractually) external service providers adhere to agency security policies.
 - 7. Document agency oversight expectations, and periodically monitor provider compliance.
- (e) Each agency shall ensure that IT resources (hardware, devices and software) are categorized, prioritized, and documented based on their classification, criticality, and business value (ID.AM-5). Agencies shall:
 - 1. Perform a criticality analysis for each categorized IT resource and document the findings of the analysis conducted.
 - 2. Designate an authorizing official for each categorized IT resource and document the authorizing official's approval of the security categorization.
 - 3. Create a contingency plan for each categorized IT resource. The contingency plan shall be based on resource classification and identify related cybersecurity roles and responsibilities.
 - 4. Identify and maintain a reference list of exempt, and confidential and exempt agency information or software and the associated applicable state and federal statutes and rules.
- (f) Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (ID.AM-6). Each agency is responsible for:
 - 1. Informing workers that they are responsible for safeguarding their passwords and other authentication methods.
 - 2. Informing workers that they shall not share their agency accounts, passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.
 - 3. Informing workers that use, or oversee or manage workers that use, IT equipment that they shall immediately report suspected unauthorized activity, in accordance with agency-established incident reporting procedures.
 - 4. Informing users that they shall take precautions that are appropriate to protect IT resources in their possession from loss, theft, tampering, unauthorized access, and damage. Consideration will be given to the impact that may result if the IT resource is lost, and safety issues relevant to protections identified in this subsection.

5. Informing users of the extent that they will be held accountable for their activities.
6. Informing workers that they have no reasonable expectation of privacy with respect to agency-owned or agency-managed IT resources.
7. Ensuring that monitoring, network sniffing, and related security activities are only to be performed by workers who have been assigned security-related responsibilities either via their approved position descriptions or tasks assigned to them.
8. Appointing an Information Security Manager (ISM). Agency responsibilities related to ISMs include:
 - a. Notifying the Agency for State Technology (AST) of ISM appointments and reappointments.
 - b. Specifying ISM responsibilities in the ISM's position description.
 - c. Establishing an information security program that includes information security policies, procedures, standards, and guidelines; an information security awareness program; an information security risk management process, including the comprehensive risk assessment required by Section 282.318, F.S.; a Computer Security Incident Response Team; and a disaster recovery program that aligns with the agency's Continuity of Operations (COOP) Plan.
 - d. Each agency ISM shall be responsible for the information security program plan.
9. Performing background checks and ensuring that a background investigation is performed on all individuals hired as IT workers with access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate-impact or higher. See paragraph 74-2.002(4)(a), F.A.C. These positions often, if not always, have privileged access. As such, in addition to agency-required background screening, background checks conducted by agencies shall include a federal criminal history check that screens for felony convictions that concern or involve the following:
 - a. Computer related or IT crimes;
 - b. Identity theft crimes;
 - c. Financially-related crimes, such as: fraudulent practices, false pretenses and frauds, credit card crimes;
 - d. Forgery and counterfeiting;
 - e. Violations involving checks and drafts;
 - f. Misuse of medical or personnel records; and,
 - g. Theft.

Each agency shall establish appointment selection disqualifying criteria for individuals hired as IT workers that will have access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate-impact or higher.

(2) Business Environment. Each agency's cybersecurity roles, responsibilities, and IT risk management decisions shall align with the agency's mission, objectives, and activities. To accomplish this, agencies shall:

- (a) Identify and communicate the agency's role in the business mission of the state (ID.BE-1).
- (b) Identify and communicate the agency's place in critical infrastructure and its industry sector to inform internal stakeholders of IT strategy and direction (ID.BE-2).
- (c) Establish and communicate priorities for agency mission, objectives, and activities (ID.BE-3).
- (d) Identify system dependencies and critical functions for delivery of critical services (ID.BE-4).
- (e) Implement information resilience requirements to support the delivery of critical services (ID.BE-5).

(3) Governance. Each agency shall establish policies, procedures, and processes to manage and monitor the agency's regulatory, legal, risk, environmental, and operational IT requirements. Procedures shall address providing timely notification to management of cybersecurity risks. Agencies shall also:

- (a) Establish or adopt a comprehensive information security policy (ID.GV-1).
 - (b) Coordinate and align information security roles and responsibilities with internal roles and external partners (ID.GV-2).
 - (c) Document and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations (ID.GV-3).
 - (d) Ensure governance and risk management processes address cybersecurity risks (ID.GV-4).
- (4) Risk Assessment.

(a) Approach. Each agency shall identify and manage the cybersecurity risk to agency operations (including mission, functions, image, or reputation), agency assets, and individuals using the following approach, that derives from the NIST Risk Management Framework (RMF) which is hereby incorporated by reference and may be found at:

<http://csrc.nist.gov/groups/SMA/fisma/framework.html>. The Risk Assessment steps provided in the table below must be followed; however, agencies may identify and, based on the risk to be managed, consider other risk assessment security control requirements and frequency of activities necessary to manage the risk at issue.

Risk Assessments	
Categorize:	Categorize information systems and the information processed, stored, and transmitted by that system based on a security impact analysis.
Select:	Select baseline security for information systems based on the security categorization; tailoring and supplementing the security baseline as needed based on organization assessment of risk and local conditions.
Implement:	Implement the selected baseline security and document how the controls are deployed within information systems and environment of operation.
Assess:	Assess the baseline security using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for systems.
Authorize:	Authorize information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the state resulting from the operation of the information system and the decision that this risk is acceptable.
Monitor:	Monitor and assess selected baseline security in information systems on an ongoing basis including assessing control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of systems to appropriate agency officials.

Agencies are required to consider the following security objectives when assessing risk and determining what kind of assessment is required and when or how often an assessment is to occur: confidentiality, integrity and availability. When determining the potential impact to these security objectives agencies will use the following table, taken from the Federal Information Processing Standards (FIPS) Publication No. 199 (February 2004), which is hereby incorporated into this rule by reference and may be found at: <http://www.firules.org/Gateway/reference.asp?No=Ref-06498>.

Security Objectives:	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations,	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations,	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations,

	organizational assets, or individuals.	organizational assets, or individuals.	organizational assets, or individuals.
--	--	--	--

In accordance with Section 282.318(4)(c), F.S., each agency shall complete and submit to AST no later than July 31, 2017, and every three years thereafter, the Florida Enterprise Information Security Risk Assessment Survey (Form #AST-100), which is hereby incorporated by reference and maintained at: <https://www.flrules.org/Gateway/reference.asp?No=Ref-06533>. In completing the AST 100 form, agencies shall follow the six-step process ("Conducting the Risk Assessment") outlined in Section 3.2 of NIST Special Publication 800-30, utilizing the exemplary tables provided therein as applicable to address the particular agency's threat situation. NIST Special Publication 800-30, Guide for Conducting Risk Assessments, Revision 1 (September 2012) is hereby incorporated by reference and may be found at: <http://www.flrules.org/Gateway/reference.asp?No=Ref-06499>. When establishing risk management processes may be helpful for agencies to review NIST RFM Special Publications – they can be downloaded from the following website: <http://csrc.nist.gov/publications/PubSPs.html>. When assessing risk agencies shall estimate the magnitude of harm resulting from unauthorized access, unauthorized modification or destruction, or loss of availability of a resource. Estimates shall be documented as low-impact, moderate-impact, or high-impact relative to the security objectives of confidentiality, integrity, and availability.

(b) Other agency risk management activities that agencies shall perform:

1. Identify and document asset vulnerabilities (ID.RA-1), business processes and protection requirements. Establish procedures to analyze systems and applications to ensure security controls are effective and appropriate.
2. Receive and manage threat and vulnerability information from information sharing forums and sources that contain information relevant to the risks or threats (ID.RA-2).
3. Identify and document internal and external threats (ID.RA-3).
4. Identify potential business impacts and likelihoods (ID.RA-4).
5. Use threats, vulnerabilities, likelihoods, and impacts to determine risk (ID.RA-5).
6. Identify and prioritize risk responses, implement risk mitigation plans, and monitor and document plan implementation (ID.RA-6).

(5) Risk Management. Each agency shall ensure that the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Each agency shall:

(a) Establish risk management processes that are managed and agreed to by agency stakeholders and the agency head (ID.RM-1).

1. Establish a risk management team that ensures that risk management processes are authorized by agency stakeholders. The risk management team must include a member of the agency IT unit, and shall determine the appropriate meeting frequency and agency stakeholders.

(b) Identify and clearly document organizational risk tolerance based on the confidential and exempt nature of the data created, received, maintained, or transmitted by the agency; by the agency's role in critical infrastructure and sector specific analysis (ID.RM-2).

(c) Determine risk tolerance as necessary, based upon: their analysis of sector specific risks; the agency's industry sector; agency-specific risks (e.g., Health Information Portability Accountability Act of 1996 compliance for agencies that maintain this information); and the agency's role in the state's mission (ID.RM-3).

(d) Establish parameters for IT staff participation in procurement activities.

(e) Identify the IT issues IT staff must address during procurement activities (e.g., system hardening, logging, performance, service availability, incident notification, and recovery expectations).

(f) Implement appropriate security controls for software applications obtained, purchased, leased, or developed to minimize risks to the confidentiality, integrity, and availability of the application, its data, and other IT resources.

(g) Prior to introducing new IT resources or modifying current IT resources, perform an impact analysis. The purpose of this analysis is to assess the effects of the technology or modifications on the existing environment. Validate that IT resources conform to agency standard configurations prior to implementation into the production environment.

Rulemaking Authority 282.318(5) FS. Law Implemented 282.318(3) FS. History--New 3-16-16.

74-2.003 Protect.

The protect function of the FCS is visually represented as such:

Function	Category	Subcategory
Protect (PR)	Access Control (AC)	PR.AC-1: Manage identities and credentials for authorized devices and users
		PR.AC-2: Manage and protect physical access to assets
		PR.AC-3: Manage remote access
		PR.AC-4: Manage access permissions, incorporate the principles of least privilege and separation of duties
		PR.AC-5: Protect network integrity, incorporate network segregation where appropriate
	Awareness and Training (AT)	PR.AT-1: Inform and train all users
		PR.AT-2: Ensure that privileged users understand roles and responsibilities
		PR.AT-3: Ensure that third-party stakeholders understand roles and responsibilities
		PR.AT-4: Ensure that senior executives understand roles and responsibilities
		PR.AT-5: Ensure that physical and information security personnel understand roles & responsibilities
	Data Security (DS)	PR.DS-1: Protect data-at-rest
		PR.DS-2: Protect data-in-transit
		PR.DS-3: Formally manage assets managed throughout removal, transfers, and disposition
		PR.DS-4: Ensure that adequate capacity is maintained to support availability needs
		PR.DS-5: Implement data leak protection measures
		PR.DS-6: Use integrity checking mechanisms to verify software, firmware, and information integrity
		PR.DS-7: Logically or physically separate the development and testing environment(s) from the production environment
	Information Protection Processes and Procedures	PR.IP-1: Create and maintain a baseline configuration of information technology/industrial control systems
		PR.IP-2: Implement a System Development Life Cycle to manage systems
		PR.IP-3: Establish configuration change control processes
		PR.IP-4: Conduct, maintain, and periodically test backups of information
		PR.IP-5: Meet policy and regulatory requirements that are relevant to the physical operating environment for organizational assets
		PR.IP-6: Destroy data according to policy
		PR.IP-7: Continuously improve protection processes
		PR.IP-8: Share effectiveness of protection technologies with stakeholders that should or must receive this information
		PR.IP-9: Establish and manage response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery)
		PR.IP-10: Test response and recovery plans
		PR.IP-11: Include cybersecurity in human resources practices (e.g., deprovisioning, personnel screening)
		PR.IP-12: Develop and implement a vulnerability management plan
	Maintenance (MA)	PR.MA-1: Perform and log maintenance and repair of organizational assets in a timely manner, with approved and controlled tools
		PR.MA-2: Approve, log, and perform remote maintenance of agency assets in a manner that prevents unauthorized access
	Protective Technology (PT)	PR.PT-1: Determine, document, implement, and review audit/log records in accordance with policy
		PR.PT-2: Protect and restrict removable media usage according to policy

		PR.PT-3: Control access to systems and assets, incorporate the principle of least functionality
		PR.PT-4: Protect communications and control networks

(1) Access Control. Each agency shall ensure that access to IT resources is limited to authorized users, processes, or devices, and to authorized activities and transactions. Specifically:

(a) Each agency shall manage identities and credentials for authorized devices and users (PR.AC-1). Control measures shall, at a minimum:

1. Require that all agency-owned or approved computing devices, including mobile devices, use unique user authentication.
2. Require users to log off or lock their workstations prior to leaving the work area.
3. Require inactivity timeouts that terminate or secure sessions with a complex password.
4. Secure workstations with a password-protected screensaver, set at no more than 15 minutes.
5. Force users to change their passwords at least every 30-90 days, based on assessed risk of the system.
6. Address responsibilities of information stewards that include administering access to systems and data based on the documented authorizations and facilitate periodic review of access rights with information owners. Frequency of reviews shall be based on system categorization or assessed risk.
7. Establish access disablement and notification timeframes for worker separations. The agency will identify the appropriate person in the IT unit to receive notification. Notification timeframes shall consider risks associated with system access post-separation.
8. Ensure IT access is removed when the IT resource is no longer required.
9. Consider the use of multi-factor authentication (MFA) for any application that has a categorization of moderate or contains exempt, or confidential and exempt information. This excludes externally hosted systems designed to deliver services to customers, where MFA is not necessary or viable.
10. Require MFA for any application that has a categorization of high or is administered by remote connection to the internal network.
11. Require MFA for network access to privileged accounts.

(b) Each agency shall manage and protect physical access to assets (PR.AC-2). In doing so, agency security procedures or controls shall:

1. Address protection of IT resources from environmental hazards (e.g., temperature, humidity, air movement, dust, and faulty power) in accordance with manufacturers' specifications.
2. Implement procedures to manage physical access to IT facilities and/or equipment.
3. Identify physical controls that are appropriate for the size and criticality of the IT resources.
4. Specify physical access to central information resource facilities and/or equipment that is restricted to authorized personnel.
5. Detail visitor access protocols, including recordation procedures, and in locations housing systems categorized as moderate-impact or high-impact, require that visitors be supervised.
6. Address how the agency will protect network integrity by incorporating network segregation.

(c) Each agency shall manage remote access (PR.AC-3). In doing so, agencies shall:

1. Address how the agency will securely manage and document remote access.
2. Specify that only agency-managed, secure remote access methods may be used to remotely connect computing devices to the agency internal network.
3. For systems containing exempt, or confidential and exempt data, ensure written agreements and procedures are in place to ensure security for sharing, handling or storing confidential data with entities outside the agency.

(d) Each agency shall ensure that access permissions are managed, incorporating the principles of least privilege and separation of duties (PR.AC-4). In doing so, agencies shall:

1. Execute interconnection security agreements to authorize, document, and support continual management of inter-agency connected systems.
2. Manage access permissions by incorporating the principles of "least privilege" and "separation of duties."
3. Specify that all workers be granted access to agency IT resources based on the principles of "least privilege" and "need to know determination."
4. Specify that system administrators restrict and tightly control the use of system development utility programs that may be capable of overriding system and application controls.

(e) Each agency shall ensure that network integrity is protected, incorporating network segregation where appropriate (PR.AC-5).

(2) Awareness and Training. Agencies shall provide all their workers cybersecurity awareness education and training so as to ensure they perform their information security-related duties and responsibilities consistent with agency policies and procedures. In doing so, each agency shall:

(a) Inform and train all workers (PR.AT-1).

(b) Ensure that privileged users understand their roles and responsibilities (PR.AT-2).

(c) Ensure that third-party stakeholders understand their roles and responsibilities (PR.AT-3).

(d) Ensure that senior executives understand their roles and responsibilities (PR.AT-4).

(e) Ensure that physical and information security personnel understand their roles and responsibilities (PR.AT-5).

(3) For each of the above subsections the following shall also be addressed:

(a) Appoint a worker to coordinate the agency information security awareness program. If an IT security worker does not coordinate the security awareness program, they shall be consulted for content development purposes. Agencies will ensure that all workers (including volunteer workers) are clearly notified of applicable obligations, established via agency policies, to maintain compliance with such controls.

(b) Establish a program that includes, at a minimum, annual security awareness training and on-going education and reinforcement of security practices.

(c) Provide training to workers within 30 days of start date.

(d) Include security policy adherence expectations for the following, at a minimum: disciplinary procedures and implications, acceptable use restrictions, data handling (procedures for handling exempt and confidential and exempt information), telework and computer security incident reporting procedures. Incident reporting procedures shall:

1. Establish requirements for workers to immediately report loss of mobile devices, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes according to agency reporting procedures.

(e) Where technology permits, provide training prior to system access. For specialized agency workers (e.g., law enforcement officers) who are required to receive extended off-site training prior to reporting to their permanent duty stations, initial security awareness training shall be provided within 30 days of the date they report to their permanent duty station.

(f) Require, prior to access, workers verify in writing that they will comply with agency IT security policies and procedures.

(g) Document parameters that govern personal use of agency IT resources and define what constitutes personal use. Personal use, if allowed by the agency, shall not interfere with the normal performance of any worker's duties, or consume significant or unreasonable amounts of state IT resources (e.g., bandwidth, storage).

(h) Inform workers of what constitutes inappropriate use of IT resources. Inappropriate use shall include, but may not be limited to, the following:

1. Distribution of malware;

2. Disablement or circumvention of security controls;

3. Forging headers;

4. Propagating "chain" letters;

5. Political campaigning or unauthorized fundraising;

6. Use for personal profit, benefit or gain;

7. Offensive, indecent, or obscene access or activities, unless required by job duties;

8. Harassing, threatening, or abusive activity;

9. Any activity that leads to performance degradation;

10. Auto-forwarding to external e-mail addresses;

11. Unauthorized, non-work related access to: chat rooms, political groups, singles clubs or dating services; peer-to-peer file sharing; material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, hate-speech, or violence; hacker web-site/software; and pornography and sites containing obscene materials.

(4) Data Security. Each agency shall manage and protect records and data, including data-at-rest, consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. Agencies shall establish procedures, and develop and maintain agency cryptographic implementations. Key management processes and procedures for cryptographic keys used for encryption of data will be fully documented and will cover key generation, distribution, storage,

periodic changes, compromised key processes, and prevention of unauthorized substitution. Also, key management processes must be in place and verified prior to encrypting data at rest, to prevent data loss and support availability. In protecting data security, agencies shall:

(a) Protect data-at-rest by establishing (PR.DS-1):

1. Procedures that ensure only agency-owned or approved IT resources are used to store confidential or exempt information.
2. Procedures that ensure agency-owned or approved portable IT resources containing confidential or mission critical data are encrypted.
3. Procedures that ensure agency-owned or approved portable IT resources that connect to the agency internal network use agency-managed security software.

4. Inform users not to store unique copies of agency data on workstations or mobile devices.

(b) Protect data-in-transit (PR.DS-2). Each agency shall:

1. Encrypt confidential and exempt information during transmission, except when the transport medium is owned or managed by the agency and controls are in place to protect the data during transit.
2. Ensure that wireless transmissions of agency data employ cryptography for authentication and transmission.
3. Make passwords unreadable during transmission and storage.
4. Encrypt mobile IT resources that store, process, or transmit exempt, or confidential and exempt agency data.

(c) Formally manage assets throughout removal, transfer, and disposition (PR.DS-3).

1. Before equipment is disposed of or released for reuse, sanitize or destroy media in accordance with the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies.
2. Destruction of confidential or exempt information shall be conducted such that the information is rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction.

3. Document procedures for sanitization of agency-owned IT resources prior to reassignment or disposal.

4. Equipment sanitization shall be performed such that confidential or exempt information is rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction. File deletion and media formatting are not acceptable methods of sanitization. Acceptable methods of sanitization include using software to overwrite data on computer media, degaussing, or physically destroying media.

(d) Maintain adequate capacity to ensure system availability and data integrity (PR.DS-4).

1. Ensure adequate audit/log capacity.
2. Protect against or limit the effects of denial of service attacks.

(e) Implement protections against data leaks or unauthorized data disclosures by establishing policies and procedures that address (PR.DS-5):

1. Appropriate handling and protection of exempt, and confidential and exempt information. Policies shall be reviewed and acknowledged by all workers.
2. Retention and destruction of confidential and exempt information in accordance with the records retention requirements as provided in the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies.
3. Access agreements for agency information systems.
4. Boundary protection.
5. Transmission confidentiality and integrity.

(f) Employ integrity checking mechanisms to verify software, firmware, and information integrity (PR.DS-6).

1. Application controls shall be established to ensure the accuracy and completeness of data, including validation and integrity checks, to detect data corruption that may occur through processing errors or deliberate actions.

(g) Physically or logically separate development and testing environment(s) from the production environment and ensure that production exempt, or confidential and exempt data is not used for development where technology permits. Production exempt, or confidential and exempt data may be used for testing if the data owner authorizes the use and regulatory prohibitions do not exist; the test environment limits access and access is audited; and production exempt, and confidential and exempt data is removed from the system when testing is completed. Data owner authorization shall be managed via technical means, to the extent practical (PR.DS-7).

(5) Information Protection Processes and Procedures. Each agency shall ensure that security policies, processes and procedures are maintained and used to manage protection of information systems and assets. Such policies, processes and procedures shall:

- (a) Include a current baseline configuration of information systems (PR.IP-1). Baselines shall:
 1. Specify standard hardware and secure standard configurations.
 2. Include documented firewall and router configuration standards, and include a current network diagram.
 3. Require that vendor default settings, posing security risks, are changed or disabled for agency-owned or managed IT resources, including encryption keys, accounts, passwords, and SNMP (Simple Network Management Protocol) community strings, and ensure device security settings are enabled where appropriate.
 4. Allow only agency-approved software to be installed on agency-owned IT resources.
- (b) Establish a System Development Life Cycle (SDLC) to manage system implementation and maintenance (PR.IP-2). In doing so, agencies shall:
 1. Develop and implement processes that include reviews of security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.
 2. Ensure security reviews are approved by the ISM and Chief Information Officer (or designee) before new or modified applications or technologies are moved into production. For IT resources housed in a state data center, the security review shall also be approved by the data center before the new or modified applications or technologies are moved into production.
 3. The application development team at each agency shall implement appropriate security controls to minimize risks to agency IT resources and meet the security requirements of the application owner. Agencies will identify in their policies, processes and procedures the security coding guidelines the agency will follow when obtaining, purchasing, leasing or developing software.
 4. Where technology permits, the agency shall ensure anti-malware software is maintained on agency IT resources.
- (c) Establish a configuration change control process to manage upgrades and modifications to existing IT resources (PR.IP-3). In doing so, agencies shall:
 1. Determine types of changes that are configuration-controlled (e.g. emergency patches, releases, and other out-of-band security packages).
 2. Develop a process to review and approve or disapprove proposed changes based on a security impact analysis (e.g., implementation is commensurate with the risk associated with the weakness or vulnerability).
 3. Develop a process to document change decisions.
 4. Develop a process to implement approved changes and review implemented changes.
 5. Develop an oversight capability for change control activities.
 6. Develop procedures to ensure security requirements are incorporated into the change control process.
- (d) Ensure backups of information are conducted, maintained, and tested periodically (PR.IP-4).
- (e) Establish policy and regulatory expectations for protection of the physical operating environment for agency-owned or managed IT resources (PR.IP-5).
- (f) Manage and dispose of records/data in accordance with the records retention requirements as provided in the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies (PR.IP-6).
- (g) Establish a policy and procedure review process that facilitates continuous improvement to protection processes (PR.IP-7). Each agency shall:
 1. Ensure system security control selection occurs during the beginning of the SDLC and is documented in final design documentation.
 2. Ensure system security plans shall document controls necessary to protect production data in the production environment and copies of production data used in non-production environments.
 3. Ensure system security plans are confidential per Section 282.318, F.S., and shall be available to the agency ISM.
 4. Require that each agency application or system with a categorization of moderate-impact or higher have a documented system security plan (SSP). For existing production systems that lack a SSP, a risk assessment shall be performed to determine prioritization of subsequent documentation efforts. The SSP shall include provisions that:
 - (I) Align the system with the agency's enterprise architecture;
 - (II) Define the authorization boundary for the system;
 - (III) Describe the mission-related business purpose;
 - (IV) Provide the security categorization, including security requirements and rationale (compliance, availability, etc.);
 - (V) Describe the operational environment, including relationships, interfaces, or dependencies on external services;
 - (VI) Provide an overview of system security requirements;

(VII) Identify authorizing official or designee, who reviews and approves prior to implementation.

5. Require information system owners (ISOs) to define application security-related business requirements using role-based access controls and rule-based security policies where technology permits.

6. Require ISOs to establish and authorize the types of privileges and access rights appropriate to system users, both internal and external.

7. Create procedures to address inspection of content stored, processed or transmitted on agency-owned or managed IT resources, including attached removable media. Inspection shall be performed where authorization has been provided by stakeholders that should or must receive this information.

8. Establish parameters for agency-managed devices that prohibit installation (without worker consent) of clients that allow the agency to inspect private partitions or personal data.

9. Require ISOs ensure segregation of duties when establishing system authorizations.

10. Establish controls that prohibit a single individual from having the ability to complete all steps in a transaction or control all stages of a critical process.

11. Require agency information owners to identify exempt, and confidential and exempt information in their systems.

(h) Ensure that effectiveness of protection technologies is shared with stakeholders that should or must receive this information (PR.IP-8).

(i) Develop, implement and manage response plans (e.g., Incident Response and Business Continuity) and recovery plans (e.g., Incident Recovery and Disaster Recovery) (PR.IP-9).

(j) Establish a procedure that ensures that agency response and recovery plans are regularly tested (PR.IP-10).

(k) Include cybersecurity in human resources practices (e.g., de-provisioning, personnel screening) (PR.IP-11).

(l) Each agency shall develop and implement a vulnerability management plan (PR.IP-12).

(6) Maintenance. Each agency shall perform maintenance and repairs of information systems and components consistent with agency-developed policies and procedures. Each agency shall:

(a) Perform and log maintenance and repair of IT resources in a timely manner, with tools that have been approved and are administered by the agency to be used for such activities (PR.MA-1).

(b) Approve, encrypt, log and perform remote maintenance of IT resources in a manner that prevents unauthorized access (PR.MA-2).

(c) Not engage in new development of custom authenticators. Agencies assess the feasibility of replacing agency-developed authenticators in legacy applications.

(7) Protective Technology. Each agency shall ensure that technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Specifically, each agency shall:

(a) Determine and document required audit/log records, implement logging of audit records, and protect and review logs in accordance with agency-developed policy. Agency-developed policy shall be based on resource criticality. Where possible, ensure that electronic audit records allow actions of users to be uniquely traced to those users so they can be held accountable for their actions. Maintain logs identifying where access to exempt, or confidential and exempt data was permitted. The logs shall support unique identification of individuals and permit an audit of the logs to trace activities through the system, including the capability to determine the exact confidential or exempt data accessed, acquired, viewed or transmitted by the individual (PR.PT-1).

(b) Protect and restrict removable media in accordance with agency-developed information security policy (PR.PT-2).

(c) Control access to systems and assets, utilizing the principle of least trust (PR.PT-3).

(d) Protect communications and control networks by establishing perimeter security measures to prevent unauthorized connections to agency IT resources (PR.PT-4). Agencies shall:

1. Place databases containing mission critical, exempt, or confidential and exempt data in an internal network zone, segregated from the demilitarized zone (DMZ).

2. Agencies shall require host-based (e.g., a system controlled by a central or main computer) boundary protection on mobile computing devices where technology permits (i.e., detection agent).

Rulemaking Authority 282.318(5) FS. Law Implemented 282.318(3) FS. History--New 3-10-16.

74-2.004 Detect.

The detect function of the FCS is visually represented as such:

Function	Category	Subcategory
Detect (DE)	Anomalies and Events (AE)	DE.AE-1: Establish and manage a baseline of network operations and expected data flows for users and systems
		DE.AE-2: Analyze detected events to understand attack targets and methods
		DE.AE-3: Aggregate and correlate event data from multiple sources and sensors
		DE.AE-4: Determine the impact of events
		DE.AE-5: Establish incident alert thresholds
	Security Continuous Monitoring (CM)	DE.CM-1: Monitor the network to detect potential cybersecurity events
		DE.CM-2: Monitor the physical environment to detect potential cybersecurity events
		DE.CM-3: Monitor personnel activity to detect potential cybersecurity events
		DE.CM-4: Detect malicious code
		DE.CM-5: Detect unauthorized mobile code
		DE.CM-6: Monitor external service provider activity to detect potential cybersecurity events
		DE.CM-7: Monitor for unauthorized personnel, connections, devices, and software
		DE.CM-8: Perform vulnerability scans
	Detection Processes (DP)	DE.DP-1: Define roles and responsibilities for detection to ensure accountability
		DE.DP-2: Ensure that detection activities comply with all applicable requirements
		DE.DP-3: Test detection processes
		DE.DP-4: Communicate event detection information to stakeholders that should or must receive this information
		DE.DP-5: Continuously improve detection processes

(1) Anomalies and Events. Each agency shall develop policies and procedures that will facilitate detection of anomalous activity in a timely manner and that will allow the agency to understand the potential impact of events. Such policies and procedures shall:

(a) Establish and manage a baseline of network operations and expected data flows for users and systems (DE.AE-1).

(b) Detect and analyze anomalous events to determine attack targets and methods (DE.AE-2).

1. Monitor unauthorized wireless access points when connected to the agency internal network, and immediately remove them upon detection.

2. Implement procedures to establish accountability for accessing and modifying exempt, or confidential and exempt data stores to ensure inappropriate access or modification is detectable.

(c) Aggregate and correlate event data from multiple sources and sensors (DE.AE-3).

(d) Determine the impact of events (DE.AE-4).

(e) Establish incident alert thresholds (DE.AE-5).

(2) Security Continuous Monitoring. Each agency shall determine the appropriate level of monitoring that will occur regarding IT resources necessary to identify cybersecurity events and verify the effectiveness of protective measures. Such activities shall include:

(a) Monitoring the network to detect potential cybersecurity events (DE.CM-1).

(b) Monitoring for unauthorized IT resource connections to the internal agency network.

(c) Monitoring the physical environment to detect potential cybersecurity events (DE.CM-2).

(d) Monitoring user activity to detect potential cybersecurity events (DE.CM-3).

(e) Monitoring for malicious code (DE.CM-4).

(f) Monitoring for unauthorized mobile code (DE.CM-5).

(g) Monitoring external service provider activity to detect potential cybersecurity events (DE.CM-6).

(h) Monitoring for unauthorized personnel, connections, devices, and software (DE.CM-7).

(i) Performing vulnerability scans (DE.CM-8). These shall be a part of the SDLC.

(3) Detection Processes. Each agency shall maintain and test detection processes and procedures to ensure timely and adequate awareness of anomalous events. These procedures shall be based on assigned risk and include the following:

(a) Defining roles and responsibilities for detection to ensure accountability (DE.DP-1).

(b) Ensuring that detection activities comply with all applicable requirements (DE.DP-2).

- (c) Testing detection processes (DE.DP-3).
- (d) Communicating event detection information to stakeholders that should or must receive this information (DE.DP-4).
- (e) Continuously improving detection processes (DE.DP-5).

Rulemaking Authority 282.318(5) FS. Law Implemented 282.318(3) FS. History--New 3-10-16.

74-2.005 Respond.

The respond function of the FCS is visually represented as such:

Function	Category	Subcategory
Respond (RS)	Response Planning (RP)	RS.RP-1: Execute response plan during or after an event
	Communications (CO)	RS.CO-1: Ensure that personnel know their roles and order of operations when a response is needed
		RS.CO-2: Report events consistent with established criteria
		RS.CO-3: Share information consistent with response plans
		RS.CO-4: Coordinate with stakeholders consistent with response plans
		RS.CO-5: Engage in voluntary information sharing with external stakeholders to achieve broader cybersecurity situational awareness
	Analysis (AN)	RS.AN-1: Investigate notifications from detection systems
		RS.AN-2: Understand the impact of incidents
		RS.AN-3: Perform forensic analysis
		RS.AN-4: Categorize incidents consistent with response plans
	Mitigation (MI)	RS.MI-1: Contain incidents
		RS.MI-2: Mitigate incidents
		RS.MI-3: Mitigate newly identified vulnerabilities or document accepted risks
	Improvements (IM)	RS.IM-1: Incorporate lessons learned in response plans
		RS.IM-2: Periodically update response strategies

(1) Response Planning. Each agency shall establish and maintain response processes and procedures and validate execution capability to ensure timely agency response for detected cybersecurity events. Each agency shall execute a response plan during or after an event (RS.RP-1).

(a) Agencies shall establish a Computer Security Incident Response Team (CSIRT) to respond to suspected computer security incidents. CSIRT members shall convene immediately, upon notice of suspected computer security incidents. Responsibilities of CSIRT members include:

1. Convening at least quarterly to review, at a minimum, established processes and escalation protocols.
2. Receiving training at least annually on cybersecurity threats, trends, and evolving practices. Training shall be coordinated as a part of the information security program.
3. CSIRT membership shall include, at a minimum, a member from the information security team, the CIO (or designee), and a member from the Inspector General’s Office. For agencies that are Health Information Portability and Accountability Act (HIPAA) covered entities as defined by 45 CFR 164.103, CSIRT membership shall also include the agency’s designated HIPAA privacy official or their designee. The CSIRT team shall report findings to agency management.
4. The CSIRT shall determine the appropriate response required for each suspected computer security incident.
5. The agency security incident reporting process must include notification procedures, established pursuant to Section 501.171, F.S., Section 282.318, F.S., and as specified in executed agreements with external parties. For reporting incidents to AST and the Cybercrime Office (as established within the Florida Department of Law Enforcement via Section 943.0415, F.S.), the following reporting timeframes shall be followed:

Rating	Initial Notification	Definition of Effect Rating
Minimal	Monthly aggregate	Effect on IT resources managed by internal processes
Low	Weekly	Minimal effect on IT resources
Medium	One business day	Moderate effect on IT resources

High	Within 4 hours	Severe effect on IT resources or delivery of services
Critical	Immediately	Severe effect on IT resources, believed to impact multiple agencies or delivery of services

(2) Communications. Each agency shall coordinate response activities with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. Each agency shall:

- (a) Inform workers of their roles and order of operations when a response is needed (RS.CO-1).
- (b) Require that events be reported consistent with established criteria and in accordance with agency incident reporting procedures. Criteria shall require immediate reporting, including instances of lost identification and authentication resources (RS.CO-2).
- (c) Share information, consistent with response plans (RS.CO-3).
- (d) Coordinate with stakeholders, consistent with response plans (RS.CO-4).
- (e) Establish communications with external stakeholders to share and receive information to achieve broader cybersecurity situational awareness (RS.CO-5). Where technology permits, enable automated security alerts. Establish processes to receive, assess, and act upon security advisories.

(3) Analysis. Each agency shall conduct analysis to adequately respond and support recovery activities. Related activities include:

- (a) Each agency shall establish notification thresholds and investigate notifications from detection systems (RS.AN-1).
- (b) Each agency shall assess and identify the impact of the incident (RS.AN-2).
- (c) Each agency shall perform forensics, where deemed appropriate (RS.AN-3).
- (d) Each agency shall categorize incidents, consistent with response plans (RS.AN-4). Each incident report and analysis, including findings and corrective actions, shall be documented.
- (4) Mitigation. Each agency shall perform incident mitigation activities. The objective of incident mitigation activities shall be to: attempt to contain and prevent recurrence of incidents (RS.MI-1); mitigate incident effects and eradicate the incident (RS.MI-2); and address vulnerabilities or document as accepted risks.

(5) Improvements. Each agency shall improve organizational response activities by incorporating lessons learned from current and previous detection/response activities into response plans (RS.IM-1). Agencies shall update response strategies in accordance with agency-established policy (RS.IM-2).

Rulemaking Authority 282.318(5) FS. Law Implemented 282.318(3) FS. History--New 3-10-16.

74-2.006 Recover.

The recover function of the FCS is visually represented as such:

Function	Category	Subcategory
Recover (RC)	Recovery Planning (RP)	RC.RP-1: Execute recovery plan during or after an event
	Improvements (IM)	RC.IM-1: Incorporate lessons learned in recovery plans
		RC.IM-2: Periodically update recovery strategies
	Communications (CO)	RC.CO-1: Manage public relations
		RC.CO-2: Repair reputation after an event
		RC.CO-3: Communicate recovery activities to internal stakeholders and executive and management teams

(1) Recovery Planning. Each agency shall execute and maintain recovery processes and procedures to ensure timely restoration of systems or assets affected by cybersecurity events. Each agency shall:

- (a) Execute a recovery plan during or after an event (RC.RP-1).
- (b) Mirror data and software, essential to the continued operation of critical agency functions, to an off-site location or regularly back up a current copy and store at an off-site location.
- (c) Develop procedures to prevent loss of data, and ensure that agency data, including unique copies, are backed up.
- (d) Document disaster recovery plans that address protection of critical IT resources and provide for the continuation of critical agency functions in the event of a disaster. Plans shall address shared resource systems, which require special consideration, when interdependencies may affect continuity of critical agency functions.

(e) IT disaster recovery plans shall be tested at least annually; results of the annual exercise shall document plan procedures that were successful and specify any modifications required to improve the plan.

(2) Improvements. Each agency shall improve recovery planning and processes by incorporating lessons learned into future activities. Such activities shall include:

(a) Incorporating lessons learned in recovery plans (RC.IM-1).

(b) Updating recovery strategies (RC.IM-2).

(3) Communications. Each agency shall coordinate restoration activities with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. Such activities shall include:

(a) Managing public relations (RC.CO-1).

(b) Attempts to repair reputation after an event, if applicable (RC.CO-2).

(c) Communicating recovery activities to stakeholders, internal and external where appropriate (RC.CO-3).

Rulemaking Authority 282.318(5) FS. Law Implemented 282.318(3) FS. History—New 3-10-16.

Terry L. Rhodes
Executive Director

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



Rick Scott
Governor

Pam Bondi
Attorney General

Jeff Atwater
Chief Financial Officer

Adam Putnam
Commissioner of Agriculture

Data Access Technical Specifications Questionnaire

Agency: Palm Beach County Board of County Commissioners

- I. **Access Method or Condition.** The Requesting Party shall attest to their respective statutory eligibility by completing the Florida Department of Highway Safety and Motor Vehicles Request for Exempt Personal information in a Driver License/Motor Vehicle Record form.
- II. **Access Specifications.** Please provide a description of the specific data being requested, the statutory authority/DPPA exemption, and which method of receiving the data is being requested in the space below:

Description of specific data needed	Description of specific use of data, to include statutory and/or DPPA authority to receive data.
1. Drivers license eligibility check (Batch process)	For determining the eligibility of driver license of current and prospective new hires operating government vehicles. Status checks will be provided through the DSS600, Batch/FTP process.
2. Drivers license eligibility check (Web Access)	For validating Palm Tran's bus operator and Paratransit driver licenses via the Public Access webservice.

III. **Method of receiving/accessing data:**

Public Access / Web service: This service provides basic driver information and eligibility. It also provides motor vehicle information. This service is available to private agencies for \$0.50 per record search and is at no charge for governmental agencies.

Driver Transcript / Web Service: 3 year, 7 year and complete driver license transcripts are available through this service. This service is available to private, city and county agencies for \$8.00 for a 3 year transcript and \$10.00 for a 7 year or complete transcript per record. Transcripts are provided at no charge to law enforcement agency, federal and state agencies.

The requestor's software communicates with our software over the Internet; The API specification for the driver transcripts and public access web service can be found within the following URL: <https://betaservices.flhsmv.gov/transcripts/> and URL: <https://betaservices.flhsmv.gov/PublicAccess/>. Access is by a user id and a password. There is no web page, as such, for the user.

Batch/FTP: The requestor submits a file with multiple records that they want matched through a standard file transfer protocol (SFTP) from their server to one of ours. Our processes pulls the file, run a program or series of programs, and return matching records or records meeting established criteria by FTP for the requestor to pick up. Driver license transcripts, DL status check, motor vehicle records, can be provided in this process also. Note: the requesting party must transition to web services as they become available for these processes.

We have different kinds of FTP processes to suit your various needs. A few are listed below.

DMS485 - This program provides a driver transcript. This program reviews each record and returns transcripts for only those driver records who have had a sanction or a conviction added onto their record within the past 1, 3, 6, 12, 24 or 36 month (lookback) period. A transcript will NOT be returned on those drivers who do not meet the above criteria. Transcripts requested can be (\$8.00) 3 year, (\$10.00) 7 year or (\$10.00) complete; \$2.00 for record not found and \$0.01 for a DL# not meeting the criteria.

DSS600/605 - This does not provide a driver transcript but will provide pertinent information only on those drivers whose status is ineligible. You will receive such information as the type of sanction, reason, and effective date. A response will not be given on eligible drivers. License type is NOT provided in the output file. A fee of .50 for each inquiry whose status is ineligible and a fee of .01 for all drivers whose status is eligible. This service is free to all government agencies.

DTR060 - Driver license transcript programs/ Returns transcripts on all DL# provided, no criteria set. This service is available to private entities, city, county and governmental agencies for \$8.00 for a 3 year transcript and \$10.00 for a 7 year or complete transcript per record. Transcripts are at no charge to LEA, federal and state agencies.

DL/MV database - We also provide a Driver License and Motor Vehicle Database for \$0.01 per record, with weekly or monthly updates.

Payment process: Automatic debits to your bank account will be made whenever the services are utilized. Prior to setup for above services, a debit authorization form should be completed by you and your banking institution and returned to us. This will allow DHSMV to debit your account. Please note that there is no other method of payment when utilizing the above services for a charge.

