

CONTRACT, LEASE, AGREEMENT CONTROL FORM

Date: 1/25/2023

Contract/Lease Control #: C17-2555-HR

Procurement#: N/A

Contract/Lease Type: CONTRACT-AGREEMENT

Award To/Lessee: FLORIDA DEPARTMENT OF HIGHWAY AND MOTOR VEHICLES

Owner/Lessor: OKALOOSA COUNTY

Effective Date: 03/28/2017

Expiration Date: 01/08/2029

Description of: DRIVER AND VEHICLE INFORMATION DATABASE SYSTEM

Department: HR

Department Monitor: SISSON

Monitor's Telephone #: 850-689-5870

Monitor's FAX # or E-mail: ESISSON@MYOKALOOSA.COM

Closed: _____

CC: FINANCE DEPARTMENT CONTRACTS & GRANTS OFFICE



Florida Department of Highway Safety and Motor Vehicles

Contract / Agreement Review

DHSMV Contract No.: HSMV-0255-23 Division: Motorist Services Date: 12/19/2022

Contractor Name: Okaloosa County Board of County Commissioners

Contract Summary: Replacing DAVID Government MOU HSMV-0323-17; Terminate HSMV-0323-17 upon execution

HSMV Functional POC: Kaci Edwards

Total Cost / Revenue: NA or No Cost [X] Term: Six (6) years

Contract Manager: Bradley Perry Phone: 850-617-2805

[X] New Contract (Procurement): [] ITB [] RFP [] ITN [] RFQ [] Single Source [] Informal Quote [] Exempt per Florida Statutes [X] Not Required

[] Renewal [] Amendment [] Extension [] Settlement Agreement [] New / Revised Template

Contract: # C17-2555-HR FLORIDA DEPARTMENT OF HIGHWAY AND MOTOR VEHICLES DRIVER & VEHICLE INFORMATION DATABASE SYSTEM Expires: 01/08/2029

Approvals

Table with 2 columns: Approval Category (Contract Administrator, Division Director, Budget, Accounting, Information Services, DAS Chief, Legal, Purchasing, Administrative Services, Deputy Executive Director, Chief of Staff) and Approval Details (Signature, Date, and checkboxes for required review).



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

February 7, 2022

TO: Kevin Bailey, Director
Division of Administrative Services

THROUGH: Robert R. Kynoch, Director
Division of Motorist Services

FROM: Stephanie D. Duhart, Chief Administrative Officer
Program Planning Administration, Division of Motorist Services

SUBJECT: Delegation of Authority for Motorist Services Agreements

Effective February 14, 2022, Division of Motorist Services Director Robert Kynoch has requested that all Memorandums of Understanding (MOUs) related to Driver and Vehicle Information Database (D.A.V.I.D – law enforcement agencies or government entities) be signed via DocuSign by Bradley Perry, Bureau Chief of Records. In addition to D.A.V.I.D., Chief Perry will also sign all Facial Recognition MOUs. Bradley will be the last, and final approver regarding both Facial Recognition and D.A.V.I.D. MOUs (LEAs and government entities). All other MOUs and/or agreements related to Data Exchange, whether amendments, templates, contracts or updates, will be signed by Director Kynoch.

Please feel free to contact me if you have questions. I can be reached at (850) 617-2596 or stephanieduhart@flhsmv.gov.

CC: Richie Frederick, Deputy Division Director, Division of Motorist Services
Bradley Perry, Chief, Bureau of Records, Division of Motorist Services
Mark Hernandez, Chief, Purchasing and Contracts, Division of Administrative Services
Elizabeth Miles, Contract Administrator and Team Supervisor, Division of Administrative Services

SDD/nd
C. File

| REQUESTOR | APPROVAL 1 |
|---|---|
| DocuSigned by: Signed: <i>Stephanie D. Duhart</i> Date: 2/7/2022 <small>0C53B794943A...</small> | DocuSigned by: Signed: <i>Robert Kynoch</i> Date: 2/7/2022 <small>0C53B794943A...</small> |
| APPROVAL 2 | AGENCY HEAD OR DESIGNEE APPROVAL |
| DocuSigned by: Signed: <i>Kevin Bailey</i> Date: 2/14/2022 <small>0C461C0DEA24460...</small> | Signed: _____ Date: _____ |

DAVID
Memorandum of Understanding (MOU) – Item check list

Agency Name: Okaloosa County Board of County Commissioners

Documentation of current licensure or certification from resident state of corporation

- Reviewed copy of requestor's business license.
- In state corporation status obtained from www.sunbiz.org.
- Or
- Out of State Corporation licensure or certification submitted by requestor (attached).
- Reviewed requestor's website comparing DPPA exemption claimed to the business needs or services provided to third parties.
- 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

- Current forms have been provided.
- Requester has provided appropriate signatures.
- Letter of delegation is required if signed by other than authorized official.

Reviewed by: DocuSigned by:
Deepa Vasudevan

Deepa Vasudevan
Bureau of Records

Date: 12/19/2022



MEMORANDUM OF UNDERSTANDING FOR GOVERNMENTAL ENTITY ACCESS TO DRIVER AND VEHICLE INFORMATION DATABASE SYSTEM (DAVID)

This Memorandum of Understanding (MOU) is made and entered into by and between Okaloosa 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. This information is stored in the Department's Driver and Vehicle Information Database system, commonly referred to as "DAVID." 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"), Section 119.0712(2), Florida Statutes, and other statutory provisions.

The Requesting Party is a government entity operating under the laws and authority of the state of Florida and/or operating under Federal laws. As a government entity, the Requesting Party may receive personal information from DAVID under the government agency exception provided in DPPA as indicated in Attachment I. The Requesting Party utilizes DAVID information for the purposes of carrying out its statutorily mandated duties and functions.

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 DAVID information to the Requesting Party. Use of the data by the Requesting Party shall only be for lawful purpose.

II. Definitions

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

- A. DAVID - The Providing Agency's Driver and Vehicle Information Database system that accesses and transmits driver and vehicle information.
- B. Driver License Information - Driver license and identification card data collected and maintained by the Providing Agency. This information includes personal information as defined below.
- C. Emergency Contact Information (ECI) - Information contained in a motor vehicle record listing individuals to be contacted in the event of an emergency. Emergency contact information may be released to law enforcement agencies through the DAVID system for purposes of contacting those listed in the event of an emergency, as noted in Section 119.0712 (2)(d), Florida Statutes.
- D. 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.
- E. Government Entity - Any non-law enforcement agency of the state, city or county government and all Federal agencies, which may include Federal law enforcement agencies.
- F. Insurance Record - Insurance information, such as Insurance Company name, policy type, policy status, insurance creation and expiration date provided to the Requesting Party, pursuant to Section 324.242(2), Florida Statutes.

- G. Parties - The Providing Agency and the Requesting Party.
- H. Personal Information - As described in Chapter 119, Florida Statutes, information found in the motor vehicle record, which includes, but is not limited to, the subject's driver identification number, name, address, telephone number, social security number, medical or disability information, and emergency contact information.
- I. Point-of-Contact (POC) - A person(s) appointed by the Requesting Party as the administrator of the DAVID program in their agency.
- J. Providing Agency - The Florida Department of Highway Safety and Motor Vehicles. The Providing Agency is responsible for granting access to DAVID information to the Requesting Party.
- K. Quarterly Quality Control Review Report - Report completed each quarter by the Requesting Party's POC to monitor compliance with the MOU. The following must be included in the Quarterly Quality Control Review Report:
 - 1. A comparison of the DAVID users by agency report with the agency user list;
 - 2. A listing of any new or inactivated users since the last quarterly quality control review; and
 - 3. Documentation verifying that usage has been internally monitored to ensure proper, authorized use and dissemination.
- L. Requesting Party - Any Government Entity that is expressly authorized by Florida Statutes and DPPA to receive personal information contained in a motor vehicle record maintained by the Providing Agency.
- M. Vehicle Information - Title and registration data collected and maintained by the Providing Agency for vehicles.

III. Legal Authority

The Providing Agency maintains computer databases containing information pertaining to driver's licenses and vehicles pursuant to Chapters 317, 319, 320, 322, 328, and Section 324.242(2), Florida Statutes. The driver license and motor vehicle 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 and may do so by remote electronic means, pursuant to Sections 119.0712(2), 320.05, 321.23, 322.20, and 324.242(2), Florida Statutes, and applicable rules.

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 agreement and to ensure that any person or entity accessing or utilizing said information shall do so in compliance with Section 119.0712(2), Florida Statutes and DPPA. In addition, the Requesting Party agrees that insurance policy information shall be utilized pursuant to Section 324.242(2), Florida Statutes. Furthermore, the deceased date of an individual shall only be provided to a Requesting Party that meets the qualifications of 15 CFR §1110.102. Disclosure of the deceased date of an individual, which is not in compliance with 15 CFR §1110.102, is punishable under 15 CFR §1110.200. Additionally, because the Social Security Administration does not guarantee the accuracy of the Death Master File (DMF), the Requesting Party is reminded that adverse action should not be taken against any individual without further investigation to verify the death information listed (A notice from the Social Security Administration addressing the foregoing is attached hereto and incorporated herein by reference).

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. Allow the Requesting Party to electronically access DAVID as authorized under this agreement.
2. Provide electronic access pursuant to established roles and times, which shall be uninterrupted except for periods of scheduled maintenance or due to a disruption beyond the Providing Agency's control, or in the event of breach of this MOU by the Requesting Party. Scheduled maintenance will normally occur Sunday mornings between the hours of 6:00 A.M. and 10:00 A.M., EST.
3. Provide an agency contact person for assistance with the implementation and administration of this MOU.

B. The Requesting Party agrees to:

1. Utilize information obtained pursuant to this MOU, including Emergency Contact Information (ECI), only as authorized by law and for the purposes prescribed by law and as further described in this MOU. In the case of ECI, such information shall only be used for the purposes of notifying a person's registered emergency contact in the event of a serious injury, death, or other incapacitation. ECI shall not be released or utilized for any other purpose, including developing leads or for criminal investigative purposes.
2. Retain information obtained from the Providing Agency only if necessary for law enforcement purposes. If retained, information shall be safeguarded in compliance with Section V. Safeguarding Information, subsection C.
3. Ensure that its employees and agents comply with Section V. Safeguarding Information.
4. Refrain from assigning, sub-contracting, or otherwise transferring its rights, duties, or obligations under this MOU, without the prior written consent of the Providing Agency.
5. Not share, provide, or release any DAVID information to any law enforcement, other governmental agency, person, or entity not a party or otherwise subject to the terms and conditions of this MOU.
6. 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 law.
7. 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 access, use, or dissemination of information provided by the Providing Agency, to the extent allowed by law.
8. Immediately inactivate user access/permissions following termination or the determination of negligent, improper, or unauthorized use or dissemination of information and to update user access/permissions upon reassignment of users within five (5) business work days.
9. Complete and maintain Quarterly Quality Control Review Reports as defined in Section II. Definitions, K, and utilizing the form attached as Attachment II.
10. Update any changes to the name of the Requesting Party, its Agency head, its POC, address, telephone number and/or e-mail address in the DAVID system within ten calendar days of occurrence. The Requesting Party is hereby put on notice that failure to timely update this information may adversely affect the time frames for receipt of information from the Providing Agency.

11. Immediately comply with any restriction, limitation, or condition enacted by the Florida Legislature following the date of signature of this MOU, affecting any of the provisions herein stated. The Requesting Party understands and agrees that it is obligated to comply with the applicable provisions of law regarding the subject matter of this Agreement at all times that it is receiving, accessing, or utilizing DAVID information.
12. Timely submit the Attestation and Certification statements as required in Section VI. Compliance and Control Measures, subsections B and C.
13. For Federal Agencies Only: 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, 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.
14. Access and utilize the deceased date of an individual, or other information from the NTIS Limited Access Death Master File, as defined in 15 CFR §1110.2, in conformity with the following requirements:
 - a) Pursuant to 15 CFR §1110.102, the Requesting Party certifies that its access to DMF information is appropriate because the Requesting Party: (i) has a legitimate fraud prevention interest, or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty; (ii) has systems, facilities, and procedures in place to safeguard such information, and experience in maintaining the confidentiality, security, and appropriate use of such information, pursuant to requirements reasonably similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986; and (iii) agrees to satisfy such similar requirements.
 - b) Pursuant to 15 CFR §1110.102, the Requesting Party certifies that it will not: (i) disclose DMF information to any person other than a person who meets the requirements of Section IV. Statement of Work, subsection B. paragraph 14 (a), above; (ii) disclose DMF information to any person who uses the information for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty; (iii) disclose DMF information to any person who further discloses the information to any person other than a person who meets the requirements of subsection IV. B. 14 (a), above; or (iv) use DMF information for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation or fiduciary duty.

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 law.

Any person who willfully and knowingly violates any of the provisions of this section is guilty of a misdemeanor of the first degree punishable as provided in Sections 119.10 and 775.083, Florida Statutes. In addition, any person who willfully and knowingly discloses any information in violation of DPPA may be subject to criminal sanctions and civil liability. Furthermore, failure to comply with 15 CFR §1110.102 pertaining to the deceased date of an individual may result in penalties of \$1,000 for each disclosure or use, up to a maximum of \$250,000 in penalties per calendar year, pursuant to 15 CFR §1110.200.

The Parties mutually agree to the following:

- A. Information exchanged will not be used for any purposes not specifically authorized by this MOU. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, or the dissemination, sharing, copying, or passing of this 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. Any and all DAVID-related information provided to the Requesting Party as a result of this MOU, particularly data from the DAVID system, will be stored in a place physically secure from access by unauthorized persons.
- D. The Requesting Party shall comply with Rule 60GG-2, Florida Administrative Code, and with Providing Agency's security policies, and employ adequate security measures to protect Providing Agency's information, applications, data, resources, and services. The applicable Providing Agency's security policies shall be made available to Requesting Party. Additionally, with respect to the deceased date of an individual, the Requesting Party shall have systems, facilities, and procedures in place to safeguard such information, and experience in maintaining the confidentiality, security, and appropriate use of such information, pursuant to requirements reasonably similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986 and agrees to satisfy such similar requirements.
- E. When printed information from DAVID is no longer needed, it shall be destroyed by cross-cut shredding or incineration in accordance with Florida law.
- F. The Requesting Party shall maintain a list of all persons authorized within the agency to access DAVID information, which must be provided to the Providing Agency upon request.
- G. Access to DAVID-related information, particularly data from the DAVID System, will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information.
- H. Under this MOU agreement, access to DAVID shall be provided to users who are direct employees of the Requesting Party and shall not be provided to any non-employee or contractors of the Requesting Party.
- I. By signing this MOU, the Parties, through their signatories, affirm and agree to maintain the confidentiality of the information exchanged through this agreement.

VI. Compliance and Control Measures

- A. **Quarterly Quality Control Review Report** - Must be completed by the Requesting Party, utilizing Attachment II, Quarterly Quality Control Review Report, within 10 days after the end of each quarter and maintained for two years. The following must be included in the Quarterly Quality Control Review Report:
 - 1. A comparison of the DAVID users by agency report with the agency user list;
 - 2. A listing of any new or inactivated users since the last quarterly quality control review; and
 - 3. Documentation verifying that usage has been internally monitored to ensure proper, authorized use and dissemination utilizing the auditing features available in DAVID.
- B. **Internal Control Attestation** - 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 Attestation Statement from their Agency's Internal Auditor, Inspector General, Risk Management IT Security Professional, or a currently licensed Certified Public

Accountant, on or before the third and sixth anniversary of the agreement or within 180 days from receipt of a request for an Attestation from the Providing Agency. The Attestation Statement shall indicate that the internal controls over personal data have been evaluated and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. The Attestation Statement shall also certify that any and all deficiencies/issues found during the review have been corrected and measures enacted to prevent recurrence. The Providing Agency may extend the time for submission of the Attestation Statement upon written request by the Requesting Party for good cause shown by the Requesting Party.

The Attestation Statement must have an original signature of the Agency Head or person designated by Letter of Delegation to execute contracts/agreements on their behalf, and may be sent via U.S. Mail, facsimile transmission, or e-mailed to the Providing Agency's Bureau of Records at the following address:

Department of Highway Safety and Motor Vehicles
Chief, Bureau of Records
2900 Apalachee Parkway, MS89
Tallahassee, Florida 32399-0500
Fax: (850) 617-5168
E-mail: DataListingUnit@flhsmv.gov

- C. **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. The Requesting Party shall submit this statement annually, within 45 days after the anniversary date of this MOU. (NOTE: During any year in which an Attestation Statement is provided, submission of the Internal Control Attestation will satisfy the requirement to submit an Annual Certification Statement.)

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.

- D. **Misuse of Personal Information** - The Requesting Party must notify the Providing Agency in writing of any incident where determination is made that personal information has been compromised as a result of unauthorized access, distribution, use, modification, or disclosure, by any means, within 30 days of such determination. The statement must be provided on the Requesting Agency'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 owners of the compromised records were notified. The statement shall also indicate the steps taken, or to be taken, by the Requesting Agency to ensure that misuse of DAVID data does not continue. This statement shall be mailed to the Bureau Chief of Records at the address indicated in Section VI. Compliance and Control Measures, subsection B., above. (NOTE: If an incident involving breach of personal information did occur and Requesting Party did not notify the owner(s) of the compromised records, the Requesting Party must indicate why notice was not provided, for example "Notice not statutorily required".)

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 with the provisions regarding notice provided therein.

VII. Agreement Term

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

matter.

VIII. 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.

IX. Termination

- 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 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 Section 119.0712(2), Florida Statutes.
- C. This MOU may also be cancelled by either party, without penalty, upon 30 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) day notice period.

X. Notices

Any notices required to be provided under this MOU may be sent via U.S. Mail, facsimile transmission, or e-mail to the following individuals:

For the Providing Agency:

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

For the Requesting Party:

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

XI. 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 agreement. 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 **Compliance and Control Measures**.

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, attestations, and reports for each executed MOU. Accordingly, should the Requesting Party execute any subsequent MOU 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: Quarterly Quality Control Review Report; Certification; and Attestation; 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 negative audit findings.

XII. Application of Public Records Law

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 Department to perform the service.
2. Upon request from the Department's custodian of public records, provide the Department 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 contractor does not transfer the records to the public agency.
4. Upon completion of the contract, transfer, at no cost, to the Department all public records in possession of the Requesting Party or keep and maintain public records required by the public agency to perform the service. If the Requesting Party transfers all public records to the Department upon completion of the contract, the Requesting Party shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Requesting Party keeps and maintains public records upon completion of the contract, the contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the Department, upon request from the Department's custodian of public records, in a format that is compatible with the information technology systems of the Department.

IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLA. STAT., TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATED TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (850) 617-3101, OGCFILING@FLHSMV.GOV, OFFICE OF GENERAL COUNSEL, 2900 APALACHEE PARKWAY, STE. A432, TALLAHASSEE, FL 32399-0504.

XIII. Certification Information

Pursuant to Section IV. Statement of Work, subsection B. paragraph 14(a) above, the Requesting Party certifies that access to DMF information is appropriate based on the following specific purpose (please describe the legitimate purpose):

Pre/Employment Background Screening/MVR

Please indicate whether the Requesting Party desires to re-disclose the deceased date of any individual to any other person or entity: Yes No

If the Requesting Party desires to re-disclose the deceased date of any individual to any other person or entity, the Requesting Party agrees that it will not re-disclose the data received from the Providing Agency, but rather, will contact NTIS at <https://classic.ntis.gov/products/ssa-dmf/#> to become a Certified Person, as defined by 15 CFR §1110.2. A Requesting Party who is a Certified Person may only disclose the deceased date of an individual pursuant to the Requesting Party's obligations under 15 CFR §1110.102.

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

REQUESTING PARTY

Okaloosa County Board of County Commissioners

Agency Name
302 N. Wilson Street

Street Address

Suite
Crestview FL 32536

City State Zip Code

PROVIDING AGENCY:

Florida Department of Highway Safety and Motor
Vehicles
2900 Apalachee Parkway
Tallahassee, Florida 32399

BY:

John Hofstad Digitally signed by John Hofstad
Date: 2022.11.29 08:44:19 -06'00'

Signature of Authorized Official
John Hofstad

Printed/Typed Name
County Administrator

Title
11.29.2022

Date
hrinfo@myokaloosa.com

Official Agency Email Address
850-689-5030

Phone Number

BY:

DocuSigned by:
Mark Hernandez

4057FC0DDCB6421...
Signature of Authorized Official
Mark Hernandez

Printed/Typed Name
Bureau Chief, Purchasing & Contracts

Title
1/11/2023

Date

Agency Point of Contact:
Shannon Clowes

Printed/Typed Name
sclowes@myokaloosa.com

Official Agency Email Address

(850) 689-5875 / Phone Number

(850) 689-5889 / Fax Number

ATTACHMENT I

**FLORIDA DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES
Request For Access to Driver And Vehicle Information Database System (DAVID)**

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.

I am an authorized 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 2 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 laws or statutes may subject me to criminal sanctions and civil liability.

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

| DPPA Exemption Claimed: | Description of how Requesting Party qualifies for exemption: | Description of how data will be used: |
|-------------------------|--|---|
| 1 | Government Agency | Pre/Employment Background Screening/MVR |

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 Access to Driver And Vehicle Information Database System and that I am entitled to receive Exempt Personal Information in A Motor Vehicle/Driver License Record and that the facts stated in it are true and correct.

John Hofstad Digitally signed by John Hofstad
Date: 2022.11.29 08:44:59
-06'00'

Signature of Authorized Official

John Hofstad

Printed Name

11/29/2022

Date

County Administrator

Title

Okaloosa County Board of County Commissioners

Name of Agency/Entity

ATTACHMENT I

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, CFR, 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 in accordance with 18 USC 2721 (b).
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, CFR.
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.



U.S. Department of Commerce
National Technical Information Service
Alexandria, VA 22312

IMPORTANT NOTICE

On November 1, 2011, the Social Security Administration (SSA) implemented an important change in the Death Master File (DMF) data. NTIS, a cost-recovery government agency, disseminates the Limited Access DMF on behalf of SSA. The Limited Access Death Master File contains data on decedants who died less than 3 years ago.

Please see the Q and A below, provided by SSA (and edited by NTIS to change the tense once the change had been implemented) for an explanation of the change.

Should you have any questions, please email jhounsell@ntis.gov who will forward any questions not answered below to the Social Security Administration for reply.

IMPORTANT NOTICE: Change in Public Death Master File Records

NTIS receives Death Master File (DMF) data from the Social Security Administration (SSA). SSA receives death reports from various sources, including family members, funeral homes, hospitals, and financial institutions.

Q: What change has SSA made to the Public DMF?

A: Effective November 1, 2011, the DMF data that NTIS receives from SSA no longer contains protected state death records. Section 205(r) of the [Social Security] Act prohibits SSA from disclosing the state death records SSA receives through its contracts with the states, except in limited circumstances. (Section 205r link - http://www.ssa.gov/OP_Home/ssact/title02/0205.htm)

Q: How did this change affect the size of the Public DMF?

A: The historical Public DMF contained 89 million records. SSA removed approximately 4.2 million records from this file and adds about 1 million fewer records annually.

**REMINDER:
DMF users should always investigate and verify the death listed before taking any adverse action against any individual."**

Terry L. Rhodes
Executive Director



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

ANNUAL CERTIFICATION STATEMENT

In accordance with Section VI., Part C, of the Memorandum of Understanding between Department of Highway Safety and Motor Vehicles (Providing Agency) and _____ (Requesting Party) hereby Affirms that the Requesting Party has evaluated and have adequate controls in place to protect the personal data from unauthorized access, distribution, use and modification or disclosure and is in full compliance as required in the contractual agreement _____ (contract number).

Signature

Printed Name

Title

Date

NAME OF AGENCY



Terry L. Rhodes
Executive Director

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

ATTESTATION STATEMENT

Contract Number _____

In accordance with Section VI., Part B, of the Memorandum of Understanding between **Department of Highway Safety and Motor Vehicles** and _____ (Requesting Party), this MOU is contingent upon the Requesting Party having appropriate internal controls in place to ensure that data provided/received pursuant to this MOU is protected from unauthorized access, distribution, use, modification, or disclosure. The Requesting Party must submit an Attestation Statement from their Agency's Internal Auditor, Inspector General, Risk Management IT Security Professional, or a currently licensed Certified Public Accountant, on or before the third and sixth anniversary of the agreement or within 180 days from receipt of an Attestation review request from the Providing Agency. The Attestation Statement shall indicate that the internal controls over personal data have been evaluated and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. The Attestation Statement shall also certify that any and all deficiencies/issues found during the review have been corrected and measures enacted to prevent recurrence. The Providing Agency may extend the time for submission of the Attestation Statement upon written request by the Requesting Party for good cause shown by the Requesting Party.

_____ (Requesting Agency) hereby attests that the Requesting Party's controls were evaluated as required in Section VI. Part B of the MOU and the controls are adequate to protect personal data from unauthorized access, distribution, use, modification or disclosure, and is in full compliance with requirements of the contractual agreement. Furthermore, any and all deficiencies/issues found during the review were corrected and measures enacted to prevent recurrence.

The above evaluation was conducted by Requesting Party's Internal Auditor; Inspector General; Risk Management IT Security Professional; Currently licensed Certified Public Accountant, identified below as the Auditor.

Signature of Authorized Official or
Delegated Official with letter of Authority

Signature of Auditor

Printed Name

Printed Name

Title

Title

Date

Date

ATTACHMENT II



QUARTERLY QUALITY CONTROL REVIEW REPORT

Point of Contacts (POC) must do the following to satisfy the MOU Quarterly Quality Control Review:

- Compare the DAVID Users by Agency report with the agency user list.
 - Reconcile any differences to ensure state and agency records are consistent.
- Keep a record of any new or inactivated users since the last Quarterly Quality Control Review.
 - Update any users/user information as needed, document the reason for the change in access, and the date the change is made.
- Monitor usage to ensure proper, authorized use and dissemination.
 - Randomly select a sample of users and run an audit report for a period during the quarter. Look for any misuse, including, but not limited to reason codes, running siblings, spouses, ex-spouses, celebrities, and political figures. Look at the times of day the data was accessed, repeated runs of same record, and unexplained access to the Emergency Contact Information.
 - **Please note:** DHSMV highly recommends the agency audit users as frequently as possible to ensure misuse is not occurring.
- Complete the below report and ensure all actions are documented.

| | |
|--|-------|
| Quarter: | Year: |
| | |
| Total active users in DAVID: | |
| Total active users in agency records: | |
| Users inactivated during quarter: | |
| Users audited during quarter: | |
| Total cases of misuse found: | |
| Total cases of misuse reported to DHSMV: | |

POC Signature

Date

POC Name Printed

Certificate Of Completion

Envelope Id: 271099F8C25A45F3A290808D1983F713

Status: Completed

Subject: Okaloosa County Board of County Commissioners- DAVID MOU Renewal

Source Envelope:

Document Pages: 18

Signatures: 7

Envelope Originator:

Certificate Pages: 4

Initials: 0

Kaci Edwards

AutoNav: Enabled

2900 Apalachee Parkway

Enveloped Stamping: Enabled

Tallahassee, 32399

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

kaciedwards@flhsmv.gov

IP Address: 164.51.75.1

Record Tracking

Status: Original

Holder: Kaci Edwards

Location: DocuSign

12/19/2022 12:33:08 PM

kaciedwards@flhsmv.gov

Signer Events

Signature

Timestamp

Deepa Vasudevan

deepavasudevan@flhsmv.gov

Operations Manager

HSMV - MS

Security Level: Email, Account Authentication (None)

DocuSigned by:

Deepa Vasudevan

485F5F7353394D2...

Sent: 12/19/2022 12:41:13 PM

Viewed: 12/19/2022 12:55:47 PM

Signed: 12/19/2022 12:57:04 PM

Signature Adoption: Pre-selected Style

Using IP Address: 164.51.75.1

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

Bradley Perry

bradleperry@flhsmv.gov

Chief of Records

HSMV - MS

Security Level: Email, Account Authentication (None)

DocuSigned by:

Bradley Perry

E7EA769D32D94F1...

Sent: 12/19/2022 12:57:09 PM

Viewed: 12/20/2022 4:33:27 PM

Signed: 12/20/2022 4:35:50 PM

Signature Adoption: Pre-selected Style

Using IP Address: 164.51.75.1

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

Elizabeth Miles

ElizabethMiles@flhsmv.gov

Contract Administrator

HSMV - DAS

Security Level: Email, Account Authentication (None)

DocuSigned by:

Emiles.

92AF769313994C3...

Sent: 12/20/2022 4:35:55 PM

Viewed: 12/21/2022 1:18:30 PM

Signed: 12/21/2022 1:19:04 PM

Signature Adoption: Uploaded Signature Image

Using IP Address: 217.180.192.178

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

Mark Hernandez

MarkHernandez@flhsmv.gov

Bureau Chief, Purchasing & Contracts

HSMV - DAS

Security Level: Email, Account Authentication (None)

DocuSigned by:

Mark Hernandez

4057F0DDCB6421...

Sent: 12/21/2022 1:19:12 PM

Viewed: 12/22/2022 9:26:27 AM

Signed: 12/22/2022 9:26:46 AM

Signature Adoption: Pre-selected Style

Using IP Address: 164.51.75.1

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

| Signer Events | Signature | Timestamp |
|---------------|-----------|-----------|
|---------------|-----------|-----------|

Kevin Bailey
 KevinBailey@flhsmv.gov
 Director, Division of Administrative Services
 HSMV - DAS
 Security Level: Email, Account Authentication (None)

DocuSigned by:

0C461C0DEA24460...

Signature Adoption: Pre-selected Style
 Using IP Address: 164.51.75.1

Sent: 12/22/2022 9:26:53 AM
 Resent: 12/27/2022 3:38:31 PM
 Viewed: 1/9/2023 12:11:23 PM
 Signed: 1/9/2023 12:11:28 PM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

Jennifer Langston
 JenniferLangston@flhsmv.gov
 Chief of Staff
 HSMV - OED
 Security Level: Email, Account Authentication (None)

DocuSigned by:

DD82CD2535C441C...

Signature Adoption: Pre-selected Style
 Using IP Address: 164.51.75.1

Sent: 1/9/2023 12:11:33 PM
 Viewed: 1/9/2023 1:05:44 PM
 Signed: 1/9/2023 1:06:09 PM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

Jennie Carpenter
 jenniecarpenter@flhsmv.gov
 Contracts Specialist
 HSMV - DAS
 Security Level: Email, Account Authentication (None)

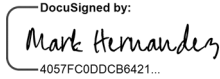
Completed

Using IP Address: 164.51.75.1

Sent: 1/9/2023 1:06:14 PM
 Viewed: 1/9/2023 3:01:53 PM
 Signed: 1/9/2023 3:04:48 PM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

Mark Hernandez
 MarkHernandez@flhsmv.gov
 Bureau Chief, Purchasing & Contracts
 HSMV - DAS
 Security Level: Email, Account Authentication (None)

DocuSigned by:

4057FC0DDCB6421...

Signature Adoption: Pre-selected Style
 Using IP Address: 164.51.75.1

Sent: 1/9/2023 3:04:53 PM
 Viewed: 1/11/2023 9:11:10 AM
 Signed: 1/11/2023 9:11:27 AM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

| 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 |
|--------------------|--------|-----------|
|--------------------|--------|-----------|

Elizabeth Miles
 ElizabethMiles@flhsmv.gov
 Contract Administrator
 HSMV - DAS
 Security Level: Email, Account Authentication (None)

COPIED

Sent: 1/11/2023 9:11:37 AM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

| Carbon Copy Events | Status | Timestamp |
|---|---------------|--|
| <p>Rita Ventry ritaventry@flhsmv.gov Contract Analyst HSMV - DAS Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p> | COPIED | Sent: 1/11/2023 9:11:37 AM |
| <p>Data Listing Unit DataListingUnit@flhsmv.gov Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p> | COPIED | Sent: 1/11/2023 9:11:37 AM |
| <p>Jennie Carpenter jenniecarpenter@flhsmv.gov Contracts Specialist HSMV - DAS Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p> | COPIED | Sent: 1/11/2023 9:11:37 AM |
| <p>Jennifer Dunkle jenniferdunkle@flhsmv.gov Senior Purchasing & Contracts Analyst HSMV - DAS Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p> | COPIED | Sent: 1/11/2023 9:11:37 AM |
| <p>Shannon Clowes sclowes@myokaloosa.com Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p> | COPIED | Sent: 1/11/2023 9:11:37 AM Viewed: 1/11/2023 9:51:29 AM |
| <p>Teresa Mann teresamann@flhsmv.gov Compliance Auditor HSMV - MS Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p> | COPIED | Sent: 1/11/2023 9:11:43 AM |

| Witness Events | Signature | Timestamp |
|----------------|-----------|-----------|
|----------------|-----------|-----------|

| Notary Events | Signature | Timestamp |
|---------------|-----------|-----------|
|---------------|-----------|-----------|

| Envelope Summary Events | Status | Timestamps |
|-------------------------|--------|------------|
|-------------------------|--------|------------|

| | | |
|---------------------|------------------|------------------------|
| Envelope Sent | Hashed/Encrypted | 12/19/2022 12:41:13 PM |
| Certified Delivered | Security Checked | 1/11/2023 9:11:10 AM |
| Signing Complete | Security Checked | 1/11/2023 9:11:27 AM |
| Completed | Security Checked | 1/11/2023 9:11:43 AM |

Payment Events

Status

Timestamps

Information and Cyber Security Awareness for External Entities

The following document is a printable version of an interactive online training.

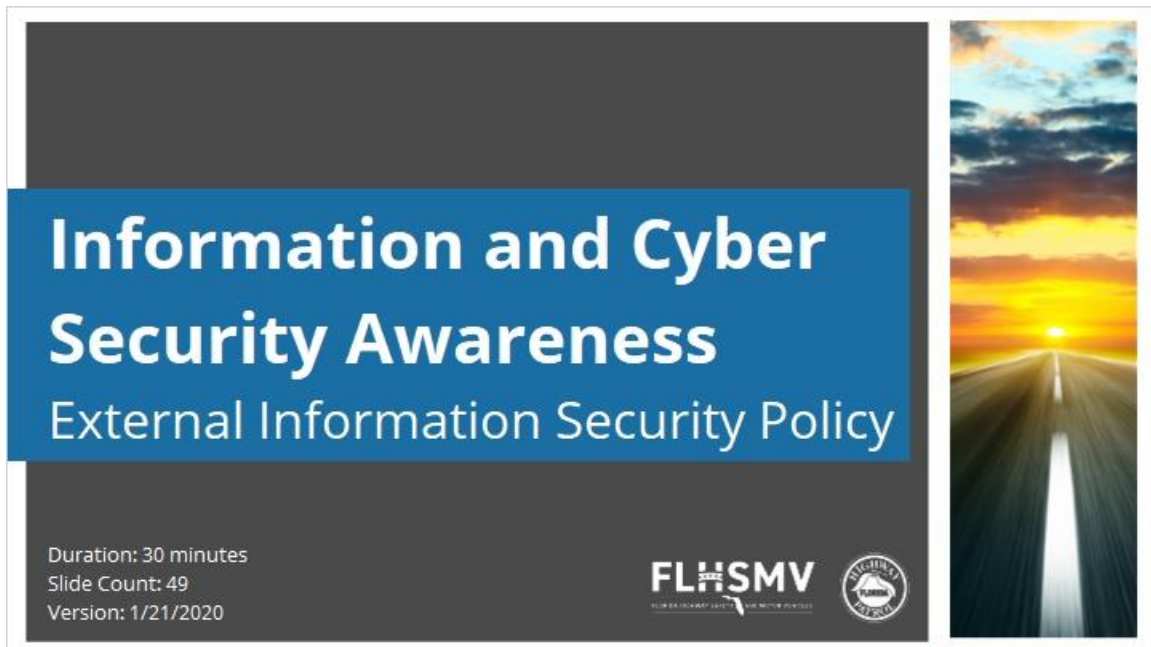
The slide heading is listed above each slide. Please note that there are multiple screenshots of some slides for two reasons:

1. Slide Layers- other layers of content on the same slide.
2. Animations- content appears at different times on the same slide.

If you see (Continued) in the slide heading, you are viewing additional screenshots of the same slide to show content that overlaps or appears at different times.

1. Introduction

1.1 Welcome



Notes:

Welcome to the Information and Cyber Security Awareness course. This course covers the External Information Security Policy. We recommend you review this policy in its entirety.

1.2 Purpose

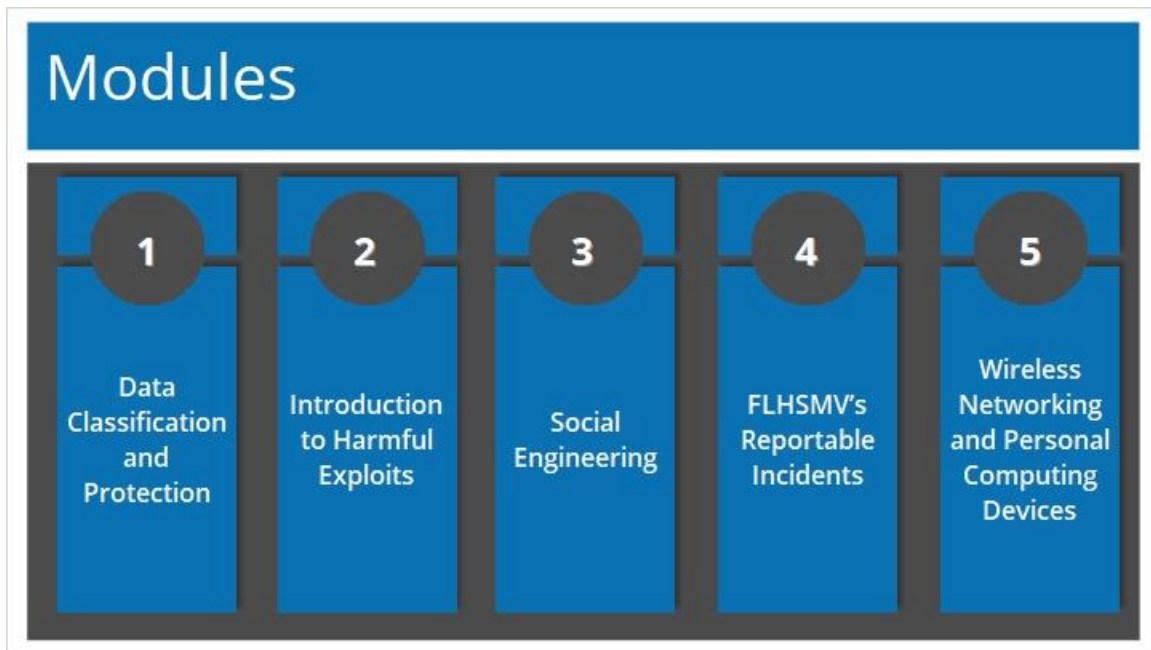
Purpose

- Bring awareness to the importance of **information security and cyber security** when working with the FLHSMV systems and data.
- Measures to prevent security breaches through **hacking, social engineering, and email spam.**
- You must follow all controls in place to prevent departmental information from being **accidentally lost, intentionally destroyed, improperly used, or fraudulently altered.**

Notes:

This means that access to department data and systems **MUST** be maintained in a manner that allows controlled access, accuracy, and is in a logical location.

1.3 Modules



Module Table of Contents:

| <u>Module</u> | <u>Name</u> | <u>Page</u> |
|----------------------|--|--------------------|
| Module 1 | Data Classification and Protection | 5 |
| Module 2 | Introduction to Harmful Exploits | 17 |
| Module 3 | Social Engineering | 22 |
| Module 4 | FLHSMV's Reportable Incidents | 32 |
| Module 5 | Wireless Networking and Personal Computing Devices | 44 |

1.4 Objectives

Objectives

The objectives of this course are to:

- Define the Federal Driver Privacy Protection Act (DPPA) and explain what information is protected under DPPA
- Introduce hacking techniques and identify what type of information hackers want to exploit from FLHSMV systems
- Review common tools of social engineering and how to protect data
- Discuss how to prevent and report security incidents
- Review the department standards for use of wireless devices, services, and technologies

Notes:

2. Module 1:

2.1 Data Classification and Protection



Notes:

In this module, we'll define the Federal Driver Privacy Protection Act (DPPA) and explain what information is protected under DPPA.

2.2 Data Classification

Data Classification

External entities must:

- Abide by the department's data classification requirements
- Classify data in accordance with FIPS Publication 199



Data classification is vitally important to ensure compliance with [Chapter 119 Florida Statutes](#) Public Records.

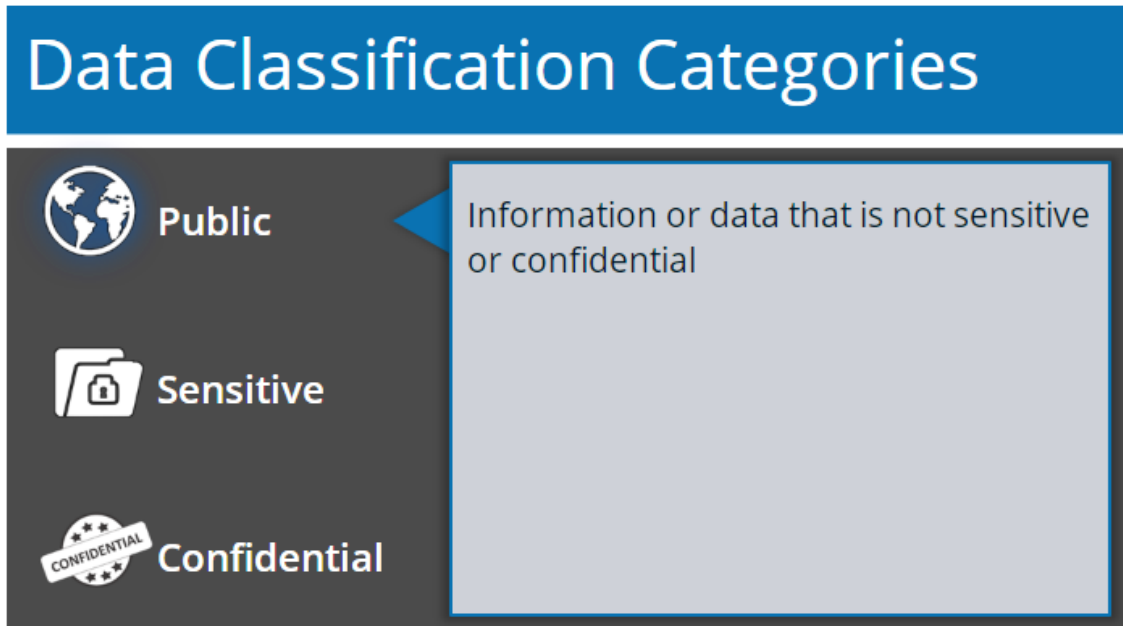
Notes:

An example of classifying data can be seen in the External Information Security Policy.

Chapter 119 Florida Statutes is found at the following link,

http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0100-0199/0119/0119.html.

2.3 Data Classification Categories, Public Slide Layer



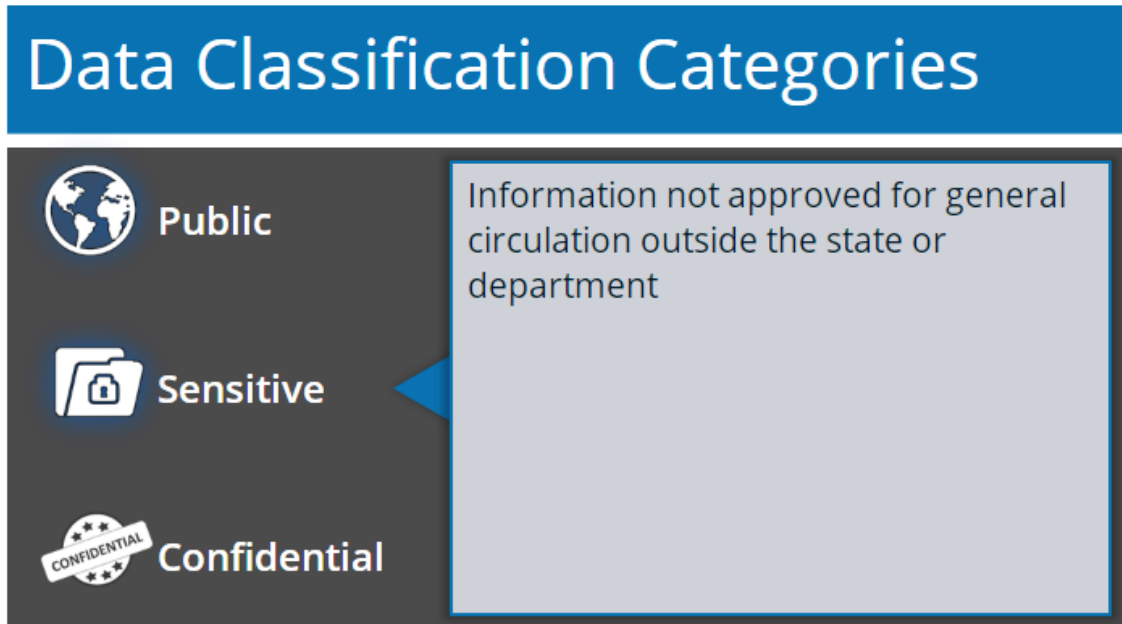
Notes:

Data must be classified into one of three categories: public, sensitive, and confidential.

Public:

Public data would not harm the state, department, employees, customers, or business partners. This data may be made generally available without approval.

2.3 Data Classification Categories, Sensitive Slide Layer

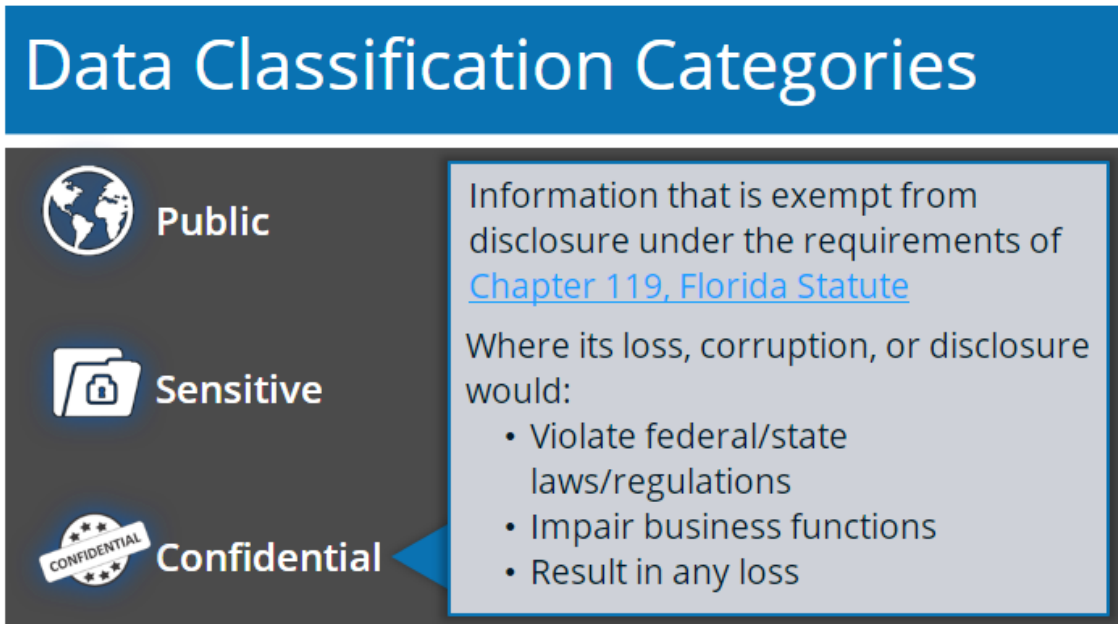


Notes:

Sensitive:

Sensitive data is information where its loss would be an inconvenience, but unlikely to result in financial loss or serious damage to credibility. Such as internal memos, minutes of meetings, and internal project reports.

2.3 Data Classification Categories, Confidential Slide Layer



The slide features a blue header with the title "Data Classification Categories". Below the header, on a dark grey background, are three categories: "Public" with a globe icon, "Sensitive" with a folder and lock icon, and "Confidential" with a starburst icon. A light grey callout box points to the "Confidential" category, containing text about exemption from disclosure and a list of consequences.

Data Classification Categories

- Public**: Information that is exempt from disclosure under the requirements of [Chapter 119, Florida Statute](#)
- Sensitive**: Where its loss, corruption, or disclosure would:
 - Violate federal/state laws/regulations
 - Impair business functions
 - Result in any loss
- Confidential**

Notes:

Confidential:

Confidential data includes data that involves issues of personal credibility, reputation, and other issues of privacy or contains highly sensitive internal documents, such as procedures, operational work routines, project plans, designs, or specifications that define the way in which the organization operates.

Please review Chapter 119, Florida Statutes at http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0100-0199/0119/0119.html. It is important to reference this statute as classification of confidential data helps prevent inadvertent public disclosure.

2.4 DPPA

DPPA

Federal Driver Privacy Protection Act (DPPA)



A United States federal statute governing the privacy and disclosure of personal information gathered by FLHSMV.

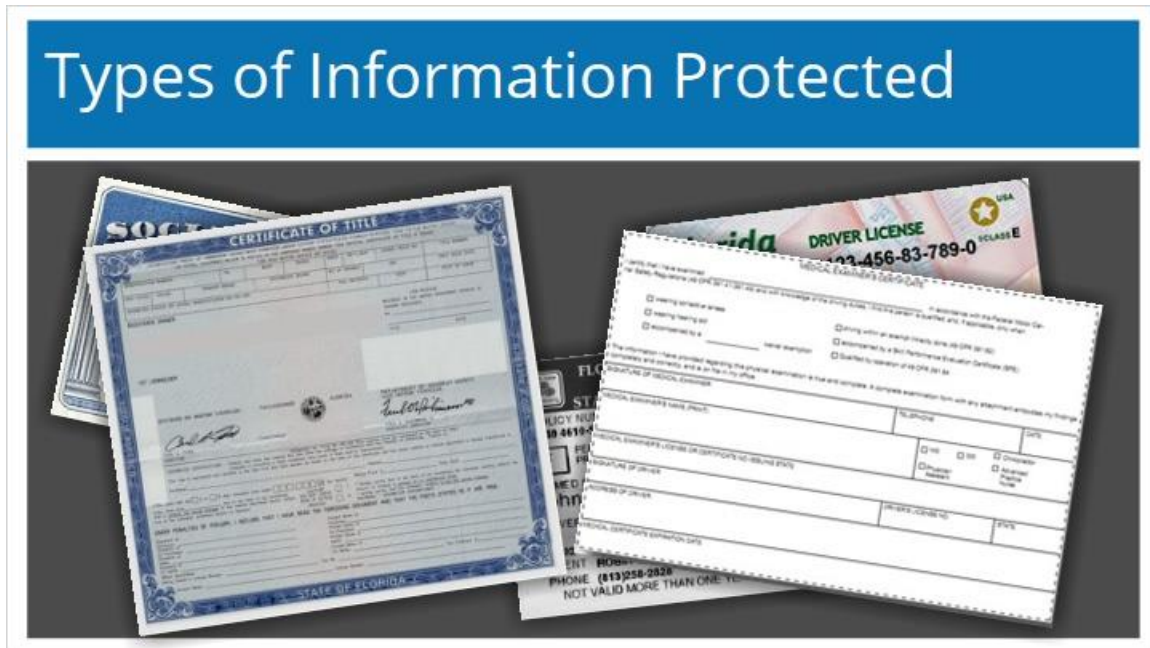
Notes:

Data Life Cycle Management

Data is managed through its lifecycle, from creation, to use, sharing, archiving, and deletion. You are involved in protecting data during the store, use, and share phases.

Being DPPA compliant means you are keeping personal information private by limiting those who have access to it.

2.5 Types of Information Protected



Notes:

So, what types of personal information are protected under DPPA?

Social security numbers or Social Security Administration (SSA) data, driver's license or identification card numbers, names, addresses, phone numbers, emergency contact information, medical or disability information, and deceased dates are all protected.

But it doesn't end there. Driving records with personal information, titles and registration, or any forms, letters, or emails related to confidential information are also protected.

This means that most of the documents and data you handle within FRVIS, FDLIS, ORION, and DAVID would be considered restricted from public access.

You have been entrusted to keep data safe and secure. Misuse of SSA data can result in criminal and civil sanctions and penalties.

2.6 Protection of Data

Protection of Data

Credential Management

1. Create a strong password
2. Never share your credentials

A man in a dark suit and tie is holding a tablet computer. Overlaid on the image is a digital network of glowing green and red nodes connected by dotted lines. In the center of the network is a white icon of a document with a padlock, symbolizing secure data or credential management.

Notes:

It is important that you follow the security measures and guidelines presented in this training and in the department's policy to ensure personal information under DPPA is protected and not compromised.

The easiest way for you to protect all information is to have secure credential management in place.

2.7 Responsibilities, All Users

The graphic features a blue header with the word "Responsibilities" in white. Below the header is a dark grey rectangular area containing three white text labels: "All Users", "Managers", and "FLHSMV/ESM". To the right of these labels is a light grey callout box with a blue arrow pointing left towards the "All Users" label. The callout box contains two bullet points.

Responsibilities

- All Users
- Managers
- FLHSMV/ESM

- Must adhere to the department's External Information Security Policy.
- Are responsible for maintaining the confidentiality and integrity of department information on all devices.

Notes:

2.7 Responsibilities, Managers (Continued)

Responsibilities

| | |
|------------|---|
| All Users | <p>Must maintain adequate logs and audit trails that:</p> <ul style="list-style-type: none">• Record access to data and records• Use industry recognized security mechanisms for the protection of confidential and sensitive data. <p>Managers may contact ISA if further guidance is needed.</p> |
| Managers | |
| FLHSMV/ESM | |

Notes:

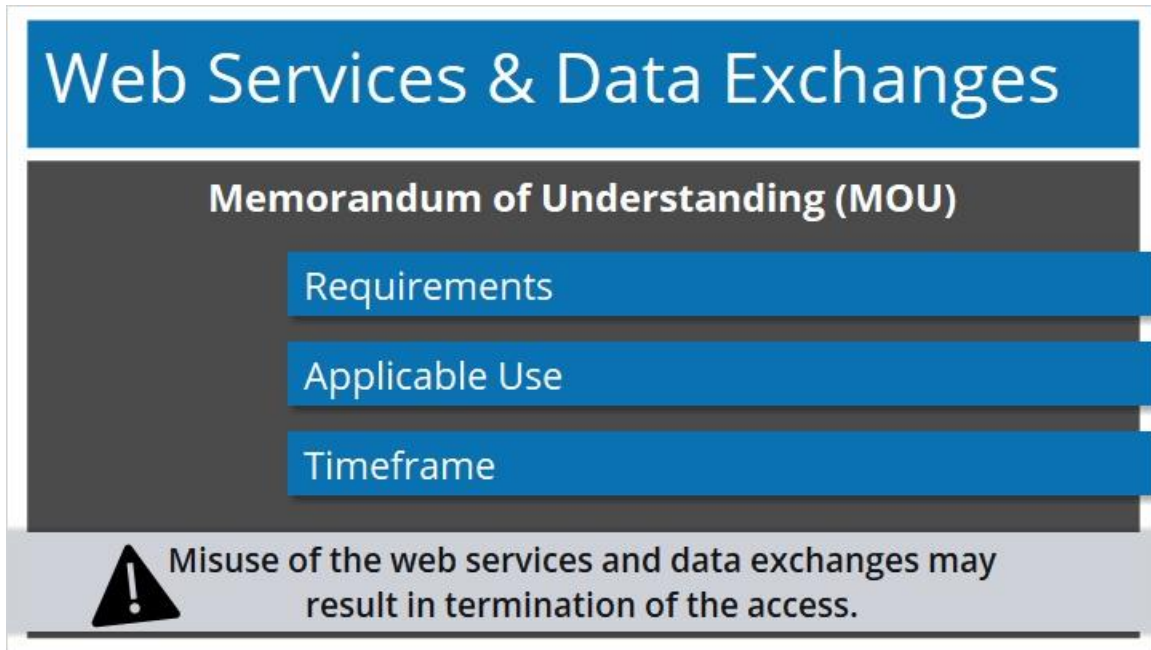
2.7 Responsibilities, FLHSMV/ESM (Continued)



Notes:

FLHSMV/ESM - The Enterprise Security Management (ESM) team's main role is to improve the security of the department. They ensure county networks are separated from the state's network by a firewall at each site.


2.8 Web Services & Data Exchanges



Web Services & Data Exchanges

Memorandum of Understanding (MOU)

- Requirements
- Applicable Use
- Timeframe

 Misuse of the web services and data exchanges may result in termination of the access.

Notes:

All external entities who utilize web-based services and data exchanges must meet various technical standards, requirements, and statutory authority as outlined in the Memorandum of Understanding (MOU) with the department.

3. Module 2:

3.1 Introduction to Harmful Exploits



Notes:

In this module, you'll receive an introduction to hacking techniques and learn what type of information hackers want to exploit from department systems.

3.2 Evolution of Hackers



Notes:

Years ago, when hacking first emerged on the internet, it consisted of tricks and petty vandalism. Hackers have evolved over time and have become more sophisticated.

3.3 Face of Threats



Notes:

The face of the threat has also changed.

Now there are hacktivists, groups like Anonymous, who go out and hack as if they are the moral conscience of the world.

3.4 Examples of Hacking, Victims of Cyber Espionage



Notes:

Let's look at some examples of hacking.

Here is a map from the National Security Agency (NSA). The red dots mark more than 600 "Victims of Chinese Cyber Espionage" that were attacked over a five-year period.

Victims of these attacks include major firms like Google, Lockheed Martin, and the U.S. government and military.

3.4 Examples of Hacking, Equifax 2017 Data Breach (Continued)



Notes:

Another example of hacking is the Equifax 2017 data breach. This massive breach affected 147.9 million consumers in some way, including compromised partial driver's license data.

These examples show just how widespread cyber-attacks are and demonstrates just how important it is to improve security measures.

4. Module 3:

4.1 Social Engineering




Notes:

In this module, we'll review common tools of social engineering and how you can protect data.

4.2 Social Engineering Defined

Social Engineering Defined

The use of **deception** to **manipulate** individuals into **exposing** confidential or **personal information** that may be used for **criminal purposes**.



Notes:


One way security incidents occur is known as social engineering.

4.3 Types of Social Engineering, Pretexting Slide Layer

Types of Social Engineering

- Pretexting
- Baiting
- Quid Pro Quo
- Heartstring

Lies used to obtain access to data



Notes:

The four types of social engineering include pretexting, baiting, quid pro quo, and heartstring.

Pretexting:

Pretexting is simply a good fabrication. Social engineers have used pretexting by calling individuals and pretending to be from Microsoft or the IT department to fix a problem with your computer.


A good example of pretexting were the techniques used by Kevin Mitnick. Mitnick compromised computers by using passwords and codes gained through social engineering. By doing careful research, learning insider jargon, and impersonating company personnel, he could gain access to systems and data.

4.3 Types of Social Engineering, Baiting Slide Layer

Types of Social Engineering

- Pretexting
- Baiting**
- Quid Pro Quo
- Heartstring

Enticement of an item, good, or inside scoop



Notes:

Baiting:

Baiting is used to attract victims by enticing them with an item, good, or the inside scoop on a "hot topic". Baiting can be either digital or physical. Digital baiting is often used in web advertisements to show victims enticing deals only to then re-directed them to malicious sites that download malware, or ransomware type exploits. Physical baiting examples are leaving a USB drive in a public area that has malware on it or other malicious code that executes once it is accessed.

4.3 Types of Social Engineering, Quid Pro Quo Slide Layer

Types of Social Engineering

- Pretexting
- Baiting
- Quid Pro Quo**
- Heartstring

Offer large sums of money in exchange for help or services

Dear Friend,
I know this message will come to you as a surprise. I am the Manager in the Central Bank of Nigeria.
I need your urgent assistance in transferring the sum of (USD \$20m) to your account within 14 banking days. Upon reply, I will give you full details on how the business will be executed and also note that you will have 40% of the above mentioned sum if you agree to handle this business with me? Please reply to me at pof.ccsoludo101@bank.cboa.com.
Yours Faithfully,
Prof. Charles C. Soludo (CBOA Manager)

Notes:

Quid Pro Quo:


Quid Pro Quo is used by scammers by offering victims a large sum of money in exchange for help or services. This is usually done via email by providing a story about money being 'trapped' in a bank account because of government restrictions. Scammers ask victims for bank account details or to pay fees, charges, or taxes but the victims are never sent what was promised. The general rule here, if it sounds too good to be true, it probably is.

4.3 Types of Social Engineering, Heartstring Slide Layer

Types of Social Engineering

- Pretexting
- Baiting
- Quid Pro Quo
- Heartstring

Draws upon human sympathy



The image shows a person's hands typing on a laptop. The laptop screen displays a blue background with the word 'DONATE' in white capital letters at the top. Below the text is a graphic of two white hands holding a red heart. A small red 'x' icon is visible at the bottom of the graphic. The person is wearing a grey sweater and is sitting at a desk with a window in the background.

Notes:


Heartstring:

Heartstring draws upon human sympathy. Anytime a disaster or tragedy occurs, fraud websites are set up and hackers send emails within 2-3 hours of the occurrence to get funds from those who want to give money. Keep in mind who you are donating to and always go directly to their website.

4.4 Tools of Social Engineering

Tools of Social Engineering

- Phishing** is used to acquire sensitive information by email
- Vishing** is used to acquire sensitive information by phone
- Smishing** is used to acquire sensitive information by text
- Malvertising** is the use of online advertising to spread malware



Notes:

Here are some common tools of social engineering:

Phishing is an enticement to the recipient to click a link that appears to be genuine but it's not. Loss of personal information, user-account compromise, or downloading of malicious malware or ransomware are often the results of a successful phishing attack.

Vishing essentially implements the same techniques used for phishing, but instead by phone.

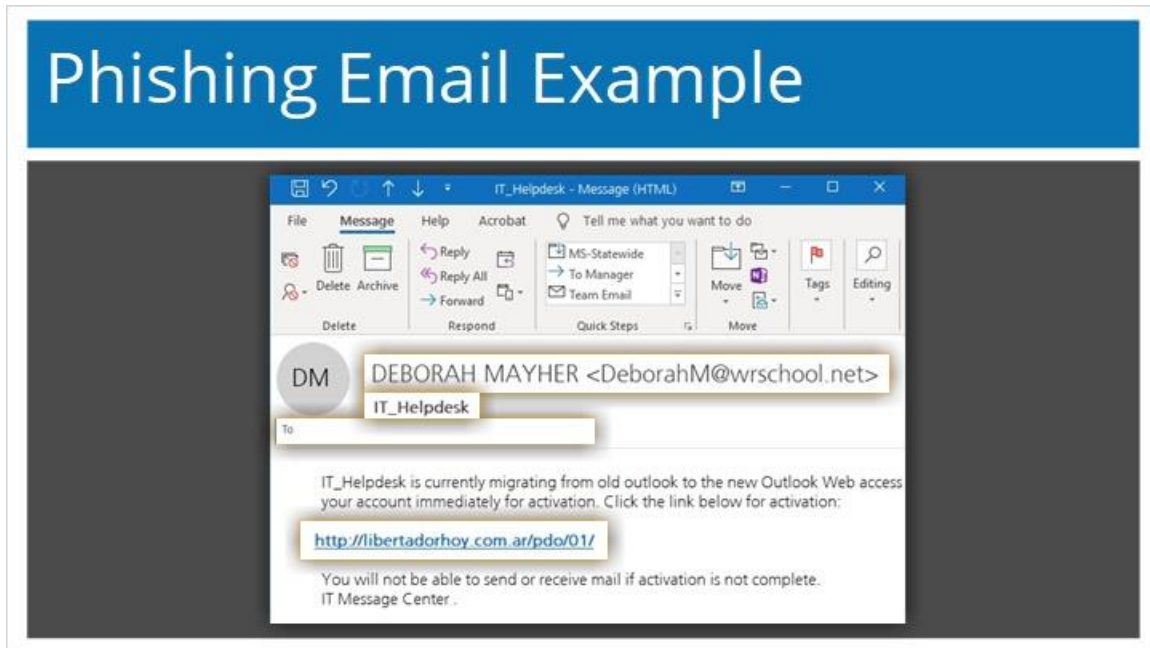
Smishing - You shouldn't respond to suspicious text messages received on mobile phones.

Malvertising -

Malware is any virus that can infect a system with something that an antivirus doesn't catch and clean. Typically, this means that the system is infected and must be re-imaged. In these cases, any critical data saved on the computer is written over and lost.

Ransomware is a specific type of malware in which the data becomes encrypted and a flash screen appears that requests money in exchange for the data.

4.5 Phishing Email Example



Notes:

Phishing is the preferred method of cyber attacks.

This is an actual phishing email that made it through the departments filtering system. However, the ESM team blocked the link in the email.

The four indicators that this is a phishing email are:

1. The **From** email address has nothing to do with our department.
2. The **To** email address is blank. Having a blank to email box indicates that the sender blind copied the email addresses.
3. The **Subject** and body of the email reference IT_Helpdesk. Our department's helpdesk is called Technical Assistance Center or TAC.
4. The **Link** name itself is suspicious as it does not relate to the email content or our department.

4.6 Lost or Stolen Devices

Lost or Stolen Devices



- Do **NOT** store any critical data on your local workstation
- Report lost or stolen devices immediately

Notes:

You should always be mindful of any department devices you are responsible for. If any devices are lost or stolen this could compromise any systems or data on the device.

4.7 Tips for Recognizing Threats



The infographic features a blue header with the title "Tips for Recognizing Threats". Below the header, four blue boxes list the following tips: "Never click links or open attachments in unsolicited emails", "Hover your mouse over a link to reveal the URL", "Discuss security incidents with your coworkers and staff", and "Report any unusual activity". To the right of these tips is a white line-art illustration of a glowing lightbulb with radiating lines above it, symbolizing an idea or awareness.

Notes:

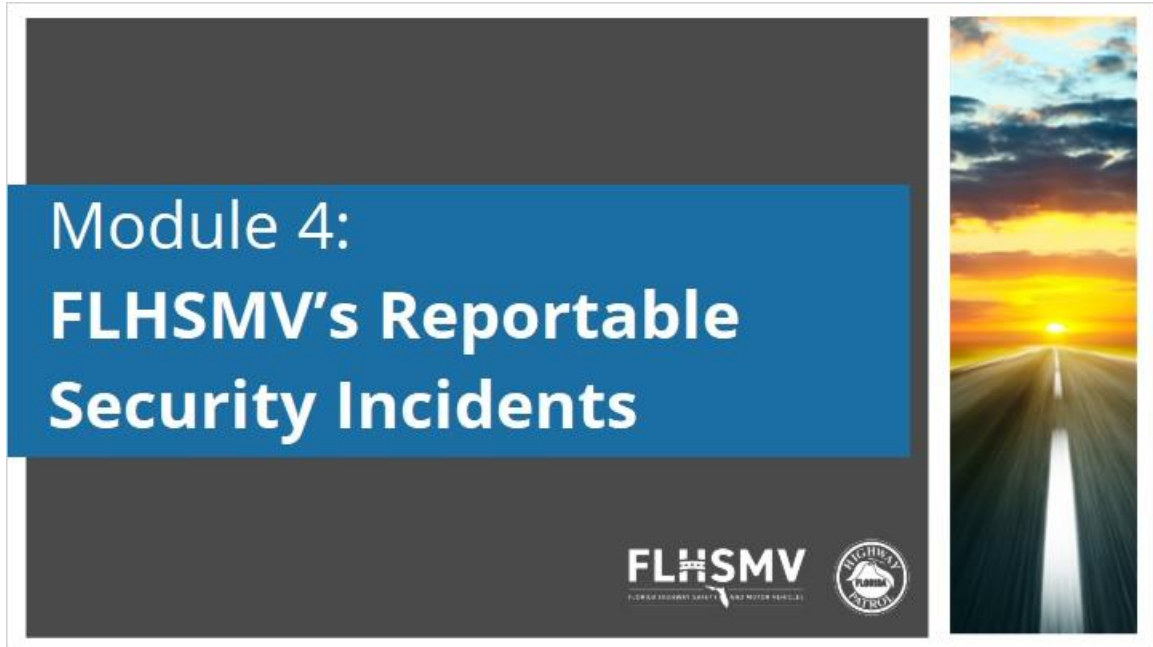
As we covered, phishing, vishing, smishing, and malware, along with lost or stolen devices are all ways data can be compromised.

The department has numerous security tools and protection mechanisms, but your awareness and diligence are the best defenses against cyber security attacks.

These are all ways you can protect yourself and the data you are responsible for.

5. Module 4:

5.1 FLHSMV's Reportable Security Incidents



Notes:

In this module, you'll learn how to prevent and report security incidents.

5.2 Security Incidents



Notes:

For specific details pertaining to security incidents and reporting, please see the External Information Security Policy.

5.3 Credential Management

Credential Management

The first line of defense for the protection of department information resources.

Constructed and implemented based on systems requirements, which ensure strong passwords are established.

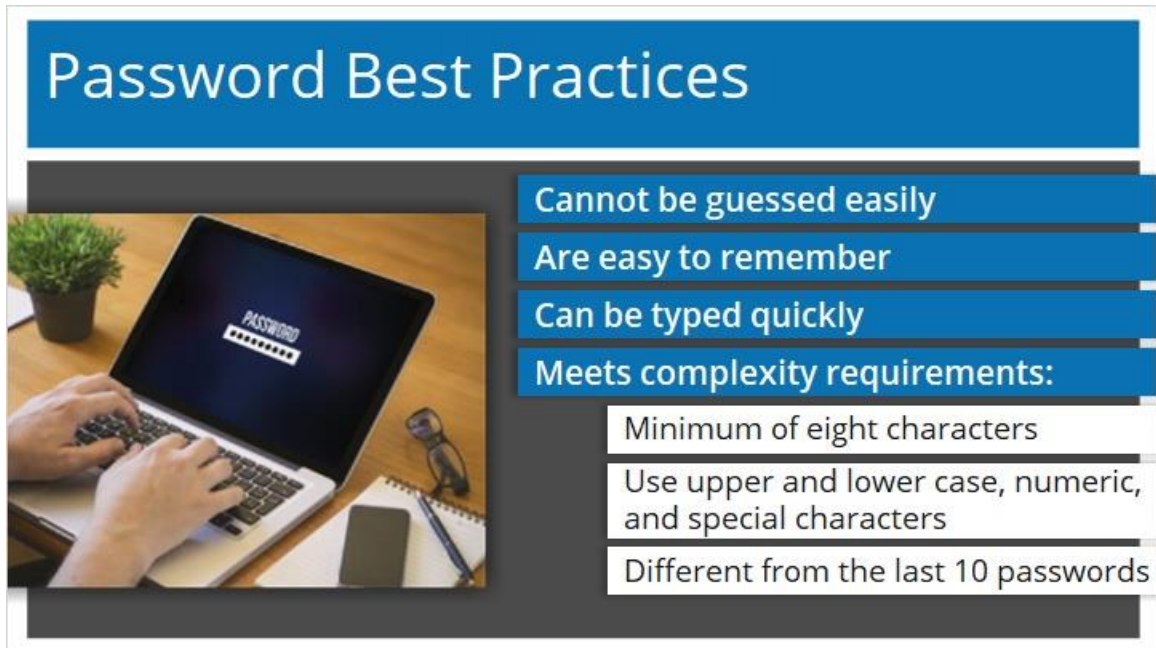
A person in a dark suit and tie is holding a tablet computer. Overlaid on the person's torso is a digital network diagram. The diagram consists of a central white document icon with a padlock, surrounded by several smaller icons of people and documents, all connected by dotted lines. Some of the icons are highlighted with green and red circles, suggesting active connections or security alerts.

Notes:

Your credentials consist of your uniquely assigned username and a password which meets the requirements of password complexity.

Passwords are especially important because they cannot be seen when being entered and they can be changed if compromised.

5.4 Password Best Practices



The infographic features a blue header with the title 'Password Best Practices'. Below the header is a photograph of a person's hands typing on a laptop. The laptop screen displays the word 'PASSWORD' above a series of eight asterisks. To the right of the photograph is a list of password best practices, each in a blue box. The first three are 'Cannot be guessed easily', 'Are easy to remember', and 'Can be typed quickly'. The fourth is 'Meets complexity requirements:', which is followed by three white boxes with black text: 'Minimum of eight characters', 'Use upper and lower case, numeric, and special characters', and 'Different from the last 10 passwords'.

Password Best Practices

- Cannot be guessed easily
- Are easy to remember
- Can be typed quickly
- Meets complexity requirements:
 - Minimum of eight characters
 - Use upper and lower case, numeric, and special characters
 - Different from the last 10 passwords

Notes:

Here are some things you can do to ensure you've created a strong password to protect devices.

5.5 Passwords Should Not

Passwords Should Not


| | | |
|---|---|---|
|  |  |  |
| <p>Passwords should not be anything tied back to you:</p> <ul style="list-style-type: none">• User name• Social security number• Relative or pet name• Birthdays• Sport teams | <p>Passwords should not be a dictionary word or acronym</p> | <p>Passwords should not use or be sequential in all the same digits or letters</p> |

Notes:

5.6 When to Change Passwords

When to Change Passwords

- All default passwords **must** be changed
- Passwords must be changed **every 90 days** minimum
- Stored passwords must be changed **immediately** if the security of a password is in doubt



! Never share your user credentials with anyone.

Notes:

5.7 Passwords Shall Not

The graphic features a blue header with the text "Passwords Shall Not". Below the header, on a dark grey background, are two columns of blue boxes. The left column is headed "Never allow the following:" and lists four items: "Auto logon", "Application remembering", "Embedded scripts", and "Non-encrypted passwords". The right column is headed "Devices should not be left unattended without:" and lists two items: "Enabling a password protected screen" and "Logging off of device".

| Never allow the following: | Devices should not be left unattended without: |
|----------------------------|--|
| Auto logon | Enabling a password protected screen |
| Application remembering | Logging off of device |
| Embedded scripts | |
| Non-encrypted passwords | |

Notes:

You can also follow these password requirements to protect devices.

5.8 Security Incidents

Security Incidents



Events, whether suspected or proven, deliberate or inadvertent, that threatens or has the potential to threaten or affect, the confidentiality, integrity, and availability of department information resources.

Notes:

Resources are assets which include: hardware, systems, software, and data vital to the functions of the department.

5.9 Video - Why Report?



Notes:

Watch a quick video on why it is very important that you report security incidents at the following link, <https://www.youtube.com/watch?v=Q8Z5v46ltn8>.

Video Transcript:

*If you see suspicious activity or you get suspicious communications, maybe people asking for information, then **it's important to report that** because you may not be the only person inside the organization who is receiving that. You may not be the only target of someone who is trying to break in and get information out of the organization. So, if two or three people are seeing that activity, then everyone can be warned that this is going on and everyone has heightened awareness of it to **ensure that information is not going to be lost.***

5.10 Reportable Incidents

| Reportable Incidents | |
|--|--|
| Physical loss, theft, or destruction of department information resources | Editing of files when no changes in them should have occurred |
| Unauthorized disclosure, modification, misuse, or disposal of critical information | Appearance or disappearance of files, or significant/unexpected changes in file size |
| Suspected or known unauthorized access activity, such as sharing user credentials | Systems that display strange messages or mislabeled files and directories |
| Unauthorized activity or transmissions using department information resources | Data that has been altered or destroyed or access that is denied |
| Intrusions or interference with department networks | |

Notes:


When a security incident occurs, you should determine if it is a reportable security incident as not all security incidents are considered reportable.

Please see the External Information Security Policy for the full list of reportable incidents.

5.11 FLHSMV Non-Reportable Incidents

FLHSMV Non-Reportable Incidents

- County maintained HR system is unavailable
- County maintained systems where department data is stored or processed is inaccessible
- Lost ID badges or devices used to grant access to county-maintained resources that do not store, process, or otherwise have access to department data or systems
- Spam email received by a county employee in the county email system



Notes:

5.12 Reporting Incidents

Reporting Incidents



Report immediately!

Information Security Manager (ISM)
ISM@flhsmv.gov

! Failure to report suspected or known breaches of SSA data can result in criminal and civil sanctions, and penalties.

Notes:

6. Module 5:

6.1 Wireless Networking and Personal Computing Devices



Notes:

In this module, we'll review the department's standards for use of wireless devices, services, and technologies.

6.2 Wireless Devices

Wireless Devices



Any wireless devices, services, and technologies used in the state-maintained network must be approved by :

- ESM Office
- Information Systems Administration

Department wireless devices must be configured and maintained according to department standards.

Notes:

6.3 Access Points

Access Points

An access point is a wireless receiver which provides connectivity from wireless network devices to a wired network.

Only access points approved by the Enterprise Security Management (ESM) Office and ISA shall be added to the department network.




Unauthorized access points must be removed immediately.

Notes:

You should know that the department monitors all wireless access points.

6.4 Internal Wireless Network

Internal Wireless Network



Wireless access into the network requires:

- Approval from ESM and ISA
- User-authentication
- Wireless transmission of department data be encrypted

Notes:

6.5 Personal Computing Devices

Personal Computing Devices

The use of personal mobile devices in conducting official business, or the physical or logical connection to department resources, is strictly **PROHIBITED**.




Only department approved USB devices may be used.

Notes:

6.6 Usage and Monitoring

Usage and Monitoring

| | | | |
|---|--|--|--|
|  | The department reserves the right to monitor usage of data and systems |  | Users should have no expectation of privacy |
|  | Be aware that it is dangerous to use social media on workstations that process FLHSMV data |  | Personal computing devices shall never be connected to department devices and networks |

Notes:

Monitoring of use can occur at any time without knowledge of the user, and the department has the right to inspect any files created, stored, sent, received, or deleted on department computers and networks.

7. Conclusion

Summary

The graphic consists of a white border containing three blue horizontal bars with white text. The top bar is the largest and contains the word 'Summary'. The middle bar is smaller and contains the first point. The bottom bar is the smallest and contains the second point. The text is centered within each bar.

Summary

Security incidents can compromise DPPA, so it's critical to manage credentials responsibility.

Malware from hacking or phishing attacks can spread to multiple systems, make them corrupt, or lose data.

If you suspect or know of a reportable incident, you have a responsibility to report it to ISM via email at ISM@flhsmv.gov

Notes:

Please report completion of this training to your office management. Thank you

External Information Security
Policy Manual



CONFIDENTIAL

**Department of Highway Safety
and Motor Vehicles**

Prepared By:

Office of Enterprise Security Management

External Information Security Policy

Revision History

| Version | Author | Release Notes | Issue Date |
|---------|--|---|------------|
| 1.2* | Joe Cipriani | Baseline document | 9/30/2015 |
| 1.21 | Tom Trunda | Add definitions and clarifications | 03/17/2016 |
| 2.0 | Scott Morgan and Carl Ford in conjunction with the Tax Collector InfoSec Coalition - Terry Skinner, Kirk Sexton, Dan Andrews and the Honorable Ken Burton Jr., Tax Collector, Manatee County | Revised to align with Department policies in congruence with requirements for External Entities. Added scope for further clarification and applicability. Revised to align with Rule 74-2, F.A.C., Information Technology Security | 08/18/2017 |
| 2.0 | Scott Morgan | Removed draft watermark, formatting check; added statutory reference for section 282.318, F.S., in the footer, added effective issue date | 12/7/2017 |
| 2.1 | Scott Morgan | Reviewed all policies. Revised to align with Rule 60GG-2, F.A.C., State of Florida Cybersecurity Standards. | 8/3/2020 |
| 3.0 | Scott Morgan Crill Merryday Bonny Allen | Reviewed all policies and revised policies. Added an additional policy specifically addressing patch management requirements for external entities. Provided guidance on applicability of policies to specific entities. Removed 30-day training grace period. #B-02, 2.0, #3 – added a specific time frame as per compliance with Florida Commission on Accreditation (CFA) Standard 26.04M (Mandatory), for Access Control. | 11/2/2022 |

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

External Information Security Policy

Scope:

This policy applies to all agents, vendors, contractors, and consultants (External Entities) who use and/or have access to Department information resources. External Entities who use and/or have access to Department information resources shall adhere to the policies outlined herein. The authority for these policies derives from Florida Statutes 282.318, Security of Data and Information Technology Resources and Florida Administrative Code Chapter 60GG-2, Information Technology Security.

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

#A-02: Data Security

1.0 Purpose

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

2.0 Policy

Other than data defined as public, which may be accessible to public access inquiries (as well as authenticated users), all data and system resources are only accessible on a need-to-know basis to specifically identified, authenticated, and authorized entities with an executed Memorandum of Understanding (MOU) which is held by the Department.

3.0 Data Usage

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

Information resources which include Department data are strategic assets vital to the business performance of the Department. These strategic assets must be protected commensurate with their tangible value, legal and regulatory requirements, and their critical role in the Department's ability to conduct its mission. Ownership and management of these information resources reside with the Department, and not to any External Entity granted access to use of these resources.

4.0 Data Storage or Transmission

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

5.0 Data Disposal

Access control mechanisms must be utilized to ensure that, during the disposal process, users can access only data to which they have been granted explicit access rights. External Entities shall follow an established process approved by the Department for the disposal of data to include the disposal of confidential data in accordance with The Florida Public Records Act and Federal Standards. Additional requirements based on specific use cases may be outlined in the MOU between the Department and the External Entity.

6.0 Management Responsibilities

Network operations and systems administration personnel shall ensure that adequate logs and audit trails are maintained. Logs and audit trails must at a minimum record access to data,

records, and activation of industry recognized security mechanism for protection of confidential and sensitive data. Logs shall be maintained in a manner that provides timely reviews of access to confidential and sensitive data and will be made available on request to the Department for validation and compliance purposes.

7.0 Data Classification

The Department is responsible for classification of data. External Entities are required to abide by data classification requirements as outlined by the Department. Data classification shall be done in accordance with FLHSMV requirements, which are based on 60GG-2, F.A.C., and is necessary to enable the allocation of resources for the protection of data assets, as well as determining the potential loss or damage from the corruption, loss, or disclosure of data. To ensure the security and integrity of all data, any data asset is Public, Sensitive or Confidential and should be labeled accordingly.

All data falls into one of the following categories:

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

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

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

8.0 Web Services and Data Exchanges

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

MOU shall govern the applicable use, timeframe, and requirements of each web service and data exchange.

For Confidential Department Data Shared Outside of Departmental Systems:

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

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

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

- Non-Department Web sites, mobile applications, web services, or computer systems which utilize Department data to conduct transactions are prohibited without written consent from the Department.
- As required to protect customer information, public facing websites, mobile applications, web services, and any system accessible through a public interface which utilizes confidential data shared by the Department with authorized external entities must utilize Department approved system access controls to protect confidential information.
- Changes to customer addresses through any public facing service as described above must be updated only through approved FLHSMV Department systems.

| | | | |
|-------------------------|------------------------------------|--------------------------------|------------------------------------|
| #A-04: Passwords | Review Date: 05/14//2022 | Issue Date: 12/01/08 | Revised Date: 05/14/2022 |
|-------------------------|------------------------------------|--------------------------------|------------------------------------|

#A-04: Passwords

1.0 Purpose

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

2.0 Policy and Standards

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

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

- System Support
 - Troubleshooting Activities
6. If the security of a password is in doubt, the password must be changed immediately.
 7. Administrators shall not circumvent this policy solely for ease of use.
 8. Users shall not circumvent password entry with auto logon, application remembering, embedded scripts or hard-coded passwords in client software.
 9. Computing devices shall not be left unattended without enabling a password-protected screensaver that is activated after 15 minutes of inactivity or logging off the device.
 10. User accounts must be locked after 5 unsuccessful login attempts.
 11. Passwords must not be transmitted via e-mail or other forms of electronic communication.
 12. Passwords must be encrypted during transmission and storage using appropriate encryption technology.
 13. Passwords shall not be written down and stored at your workstation in your office.
 14. Passwords stored on physical media must be protected by an encryption technology outlined in Policy #B-01 Acceptable Encryption.
 15. Initial use passwords that have been assigned must expire at the time of first use in a manner that requires the password owner to supply a new password, provided that this functionality is available within that particular product or facility.
 16. For all password resets, the identity of the person requesting the password reset must be verified. Note: At no time shall a user call TAC requesting a password change for another user. TAC has been instructed to lock both accounts immediately when encountering this type of call, as it is a violation of this policy.

| | | | |
|-------------------------------------|-----------------------------------|--------------------------------|------------------------------------|
| #B-01: Acceptable Encryption | Review Date: 05/14/2022 | Issue Date: 12/01/08 | Revised Date: 05/14/2022 |
|-------------------------------------|-----------------------------------|--------------------------------|------------------------------------|

#B-01: Acceptable Encryption

1.0 Overview

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

2.0 Purpose

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

3.0 Scope

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

4.0 Policy

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

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

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

| | | | |
|------------------------------|-----------------------------------|--------------------------------|------------------------------------|
| #B-02: Access Control | Review Date: 05/14/2022 | Issue Date: 12/01/08 | Revised Date: 05/14/2022 |
|------------------------------|-----------------------------------|--------------------------------|------------------------------------|

#B-02: Access Control

1.0 Purpose

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

2.0 Policy

1. Each user accessing a Department information resource shall be assigned a unique personal identifier, commonly referred to as either a user account, Logon ID, user identification, or User ID. Exceptions: public systems where such access is authorized or for situations where risk analysis by the Department demonstrates such use to be applicable and appropriate. (Example: DL check on the FLHSMV website)
2. Users shall not under any circumstances use another user's account logon or credentials. This includes network logon accounts and accounts used in agency systems (ORION, FRVIS, etc.). A user shall never call the Technical Assistance Center (TAC) to have another user's account unlocked.
3. User access rights shall be established based on approved written requests. The user identification shall be traceable to the user for the lifetime of the records or reports in which they appear.
4. A user's access shall be removed and/or disabled immediately, no later than within three (3) business days, from systems which access Department information resources when access is no longer required. Examples include, but are not limited to, termination, transfer, or removal of the duties that require access. Notification of changes in the status of users with established Department credentials is the responsibility of the authorizing External Entity to report such changes to the Department.
5. Each user shall agree in writing to use the access only for the purpose intended.
6. An automatic workstation time-out shall occur no later than 15 minutes after inactivity. A password shall be required to unlock the user account. User accounts shall be locked after 5 unsuccessful attempts.
7. External Entities must monitor the access rights of those whom they have authorized.
8. Established controls must ensure that Department information resources are accessed only by users authorized to do so.
9. Access to accounts with elevated access rights shall follow the principle of least privilege and should be restricted to systems personnel only; usage of these accounts shall be logged and subject to audit.
10. Administrative access shall incorporate Separation of Duties to ensure no individual has the ability to control an entire process.
11. Access rights to Department information resources by systems personnel shall be based on specific job requirements. Responsibility for production systems must be separated from

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

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

| | | | |
|--|-----------------------------------|--------------------------------|------------------------------------|
| #B-03: Account Management for User Accounts | Review Date: 05/14/2022 | Issue Date: 12/01/08 | Revised Date: 05/16/2022 |
|--|-----------------------------------|--------------------------------|------------------------------------|

#B-03: Account Management for User Accounts

1.0 Purpose

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

2.0 Background

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

3.0 Policy

1. All accounts created must have an associated request and approval that is appropriate for the Department's information resource or service.
2. External Entities must complete the Information and Cyber Security Awareness for External Entities online training course in iLearn prior to receiving account credentials. Additionally, external entities must complete the Information Security Training in iLearn on an annual basis within 90 days of assignment. Failure to complete the training may result in termination of account access.
3. All accounts must be uniquely identifiable using the assigned username. User accounts and the associated passwords constitute a user's credentials and shall never be shared.
4. All default passwords for accounts must comply with password policy # A-04.
5. All accounts must have a password expiration that complies with password policy # A-04.
6. The appropriate system administrator or other designated staff should disable accounts of individuals on extended leave. Extended leave is defined as greater than 60 days.
7. External Entity user accounts established by the Department that have not been accessed within 30 days are subject to being disabled.
 - a. External Entities' System Administrators are responsible for modifying the accounts of individuals that change duties or are separated from their relationship with the External Entity upon notification of change or separation.
 - b. Must have a documented process to modify a user account to accommodate situations such as name changes, account changes, and permission changes.
 - c. Must have a documented process for periodically reviewing existing accounts for validity and timely removal of access to Department resources and data.
 - d. Department information resources utilized by External Entities are subject to independent audit review of user account management.
 - e. Must provide a list of accounts for the systems they administer when requested by authorized Department management.
 - f. Must cooperate with authorized Department management investigating security incidents.

| | | | |
|--|-----------------------------------|--------------------------------|------------------------------------|
| #B-06: Application Service Provider | Review Date: 05/15/2022 | Issue Date: 12/01/08 | Revised Date: 05/15/2022 |
|--|-----------------------------------|--------------------------------|------------------------------------|

#B-06: Application Service Provider

1.0 Purpose

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

2.0 Policy and Standards

1. General Security:

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

Physical Security:

- a. The ASP's application infrastructure (hosts, network equipment, etc.) must be located in a physically secure facility and in a locked environment.
- b. The ASP must disclose who amongst their personnel will have access to the environment hosting the application for the authorizing External Entity.
- c. The Department requires that the ASP disclose their ASP background check procedures and results prior to the Department's ISM approval.

3. Network Security:

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

- If the Department or the authorizing External Entity will be connecting to the ASP via a private circuit, then that circuit must terminate on the authorizing External Entity's infrastructure, and the operation of that circuit will adhere to this policy.
- If the data between the authorizing External Entity and the ASP traverses a public network such as the Internet, the ASP must deploy appropriate firewall technology, and the traffic between the authorizing External Entity and the ASP must be protected and authenticated by cryptographic technology.

4. Host Security:

- a. The ASP must disclose how and to what extent the hosts or servers (Unix, Windows, etc.) comprising its application infrastructure have been hardened against potential threats and attack vectors. The ASP shall provide any hardening documentation it has for the Department or authorizing External Entity's application infrastructure as well.
- b. The ASP must provide a methodology and plan for ensuring systems are patched or updated according to industry best practices and guidelines. Patches include, but are not limited to, host OS, web server, database, and any other system or application.
- c. The ASP must disclose its processes for monitoring the confidentiality, integrity, and availability of those hosts.
- d. The ASP must provide to the Department information on its password policy for the application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.
- e. The ASP must provide information on account creation, maintenance, and termination processes, for service, system, and user accounts. This should include information as to how an account is created, how account information is communicated to the user, and how accounts are terminated when no longer needed.

5. Web Security:

- a. The ASP will disclose the use of various web architecture and programming languages, including, but not limited to Java, JavaScript, ActiveX, PHP, Python, C, Perl, VBScript, etc.
- b. The ASP will describe the process for performing security testing for the application and or system accessing Department data. For example, testing of authentication, authorization, and accounting functions, or any other activity designed to validate the security architecture, including external and internal penetration testing.
- c. The ASP will disclose the methodology utilized for web code reviews, including CGI, Java, etc., for the explicit purposes of finding and remediating security vulnerabilities, the authorizing party who performed the review, results of the review, and what remediation activity has taken place.

6. Encryption:

- a. The Department's application data in the custody of the authorizing External Entity must be stored and transmitted using acceptable encryption technology as outlined in Policy #B-01, Acceptable Encryption, and must comply with all relevant Department MOU's.
- b. Connections to the ASP utilizing the Internet must be protected using any of the following encryption technologies: IPsec, TLS, SSH/SCP, PGP, or any other encryption technologies approved by the Department's ISM.

| | | | |
|--|-----------------------------------|--------------------------------|------------------------------------|
| #B-10: Incident Handling (Security Incidents) | Review Date: 05/16/2022 | Issue Date: 12/01/08 | Revised Date: 05/16/2022 |
|--|-----------------------------------|--------------------------------|------------------------------------|

#B-10: Incident Handling (Security Incidents)

1.0 Purpose

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

2.0 Policy

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

1. The Department's ISM is responsible for the coordination of any security incident that occurs. All known or suspected incidents must be reported immediately to the Department's ISM using the email address: ISM@flhsmv.gov.
2. All suspected incidents of ransomware or other malware type activity must be reported immediately to the Florida Digital Service's statewide portal. All state, local, and county governments must comply with this requirement.
3. Whenever a security incident, such as a virus, Denial of Service, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed that impacts or has the potential to impact the Department's information resources, the Department's ISM must be notified immediately, and the appropriate incident management procedures must be followed.

Reportable Incidents:

Reportable incidents include, but are not limited to, the following:

- Physical loss, theft, or destruction of the Department's information resources, including Department data.
- Ransomware, malware, or related anomalous activity, once known OR suspected.
- Unauthorized disclosure, modification, misuse, or disposal of sensitive, critical, or business-controlled data and information.
- Suspected or known unauthorized internal or external access activity, including, but not limited to, sharing of user credentials and accounts which must be reported immediately.
- Unauthorized activity or transmissions using Department information resources.
- Internal/external intrusions/interference with Department networks (denial of service attacks, unauthorized activity on restricted systems, unauthorized modification or deletion of files, or unauthorized attempts to control information resources.
- Editing of files when no changes in them should have occurred.
- Appearance / disappearance of files, or significant /unexpected changes in file size.

- Systems that display strange messages or that mislabel files and directories.
- Data that has been altered or destroyed or access that is denied outside of normal business procedures.
- Detection of unauthorized personnel in controlled information security areas.
- Lost security tokens, smart cards, identification badges, or other devices used for identification and authentication shall be reported immediately.
- Fraud, embezzlement, and other illegal activities.
- Violation of any portion of the External Information Security Policy.

| | | | |
|--|-----------------------------------|--------------------------------|------------------------------------|
| #B-20: Security Monitoring and Auditing | Review Date: 05/18/2022 | Issue Date: 12/01/08 | Revised Date: 05/19/2022 |
|--|-----------------------------------|--------------------------------|------------------------------------|

#B-20: Security Monitoring and Auditing

1.0 Purpose

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

2.0 Background

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

3.0 Policy

1. Security monitoring will be used as a method to confirm that security practices, controls, and policies are functional, adhered to, and are effective.
2. Monitoring consists of activities such as the periodic review of:
 - a. Automated intrusion detection system logs
 - b. Firewall logs
 - c. User account logs
 - d. Network scanning logs
 - e. Application logs
 - f. Data backup recovery logs
 - g. Technical Assistance Center (TAC) logs
3. Audits may be conducted to:
 - a. Ensure integrity, confidentiality and availability of the Department's information resources
 - b. Investigate possible security incidents
 - c. Ensure conformance to the Department's security policies and relevant MOUs.
 - d. Monitor user or system activity where appropriate
4. The Department shall use automated tools to provide real time notification of detected anomalies or vulnerability exploitation. These tools will be deployed to monitor network traffic and/or operating system security parameters.
5. The following files may be checked for signs of misuse, fraudulent activity, and vulnerability exploitation periodically, or as requested for investigative purposes:
 - a. Automated intrusion detection system logs
 - b. Firewall logs

- c. User account logs
 - d. Network scanning logs
 - e. System error logs
 - f. Application logs
 - g. Data backup and recovery logs
 - h. Telephone activity – Call Detail Reports
6. The following audit review may be performed periodically or upon request by assigned technical staff:
- a. Password strength
 - b. Unauthorized network devices
 - c. Unauthorized personal web servers
 - d. Unsecured sharing of devices
 - e. Unauthorized modem use
 - f. Operating system and software licenses
 - g. Unauthorized wireless access points
7. When requested, and for the purpose of performing an audit, any access needed will be provided to members of ESM as designated by the Department's ISM. This access may include:
- a. User level and/or system level access to any computing or communications device
 - b. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on the Department's information resources
 - c. Access to work areas that access or process Department information resources
 - d. Access to interactively monitor and log traffic on the Department's networks.
8. Any security issues discovered will be reported to the Department's ISM for follow-up review and possible improvement to security settings.

| | | | |
|---|-----------------------------------|--------------------------------|------------------------------------|
| #B-23: Network Interconnectivity | Review Date: 05/19/2022 | Issue Date: 12/01/08 | Revised Date: 05/19/2022 |
|---|-----------------------------------|--------------------------------|------------------------------------|

#B-23: Network Interconnectivity

1.0 Purpose

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

2.0 Policy

1. Access to the Department's networks via External Entities' networks shall be protected via firewall or firewall feature sets. No connectivity between the Department's network and an external network shall be permitted without the use of firewall features to the appropriate degree based on level of risk, as determined by ISA, in conjunction with the Department's ISM.
2. Access to devices (servers) within the confines of the Department's core network from External Entities' networks shall be limited to the minimum manageable set of users/connections, as determined by ISA in conjunction with the Department's ISM, via firewall or firewall features.
3. All External Entities' network connections must meet the requirements of the Florida Information Resource Security Policies and Standards (Rule 60GG-2). Blanket access is prohibited, and the principle of least privilege shall apply at all times. Interconnectivity is limited to services, devices, and equipment needed.
4. Through system monitoring, alerting, or due to a reported incident, the Department's ISA and ESM teams reserve the right to immediately terminate and drop connectivity from the External Entities' environment to the Department's network. The Department takes the security of the HSMV network and the state MFN2 network seriously. All decisions for termination of access will be made with a risk-based decision in consultation between the Department's ISM and CIO.

External Entity Agreements:

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

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

#B-24: Malware/Virus Protection

1.0 Purpose

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

2.0 Policy

1. All computing devices (workstations, servers, laptops, tablets, etc.) whether connected to the Department’s network, processing, or accessing Department data, must utilize a modern and supported anti-virus protection system. The Department’s ISM will maintain a list of any non-approved protection vendors, typically which are known or suspected to have security issues. Exceptions to this list will be considered for approval by the Department’s ISM on a case-by-case basis.
2. The virus protection system must be enabled on workstations and servers at start-up, employ resident scanning, and never be disabled or bypassed for production usage. The settings for the virus protection system must not be altered in a manner that will reduce the effectiveness of the system.
3. External Entities which access and utilize the Department’s information resources and data are required to update virus signature files immediately upon release.
4. The automatic update frequency of the virus protection system must not be altered to reduce the frequency of updates. Each computing device which accesses Department information resources and data must utilize a antivirus protection system and setup to detect and clean viruses that may infect file shares.
5. External Entities which access or utilize the Department’s information resources shall ensure that email is scanned to ensure email and attachments are free from malware and viruses.
6. Each virus, malware, or ransomware exploit those impacts, or potentially impacts the Department’s information resources constitutes a security incident and must be reported to the Department’s ISM as outlined in #B-10, Incident Handling. The computing device shall be removed from the External Entities network until it is verified as free of viruses and malware and coordinated incident response with the Department’s ISM.

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

#B-23: Patch and Vulnerability Management

1.0 Purpose

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

2.0 Policy

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

1. External Entities who connect to Department systems, or store or process Department data shall follow a documented and regimented process for mitigation of critical security patches and remediation of vulnerabilities.
2. The documented process for patching and vulnerability remediation shall follow a patch management approach as outlined in NIST Special Publication 800-40r4 "Guide to Enterprise Patch Management Patching Planning" which can be found at the following URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf>
3. Documentation outlining conformance with this policy will be provided when requested to confirm compliance with Department policy and the MOU executed between the Department and the External Entity.
4. Non-compliance by an External Entity for this policy may include termination of access to Department systems, data, and resources if not remediated to reduce and mitigate critical vulnerabilities which may affect the confidentiality, integrity, and availability of Department information resources.

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

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

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

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