

A SAFER
FLORIDA

HIGHWAY SAFETY AND MOTOR VEHICLES

Driver and Vehicle Information Database
(DAVID) Modernization

State of Florida

Division of Motorist Services

System Security Plan

Contact Information

To request copies, suggest changes, or submit corrections, contact:

Highway Safety & Motor Vehicles
2900 Apalachee Parkway
Tallahassee, FL 32399
Attention: Maureen Johnson
Bureau Chief, Bureau of Records

File Information

File Location:

Last Saved:

Revision History

Date	Version	Revised By	Description
07/11/2013	1.0	J. Matthews	Initial Draft
07/15/2013	2.0	D. Todd	Draft
03/12/2014	2.1	J. Matthews	Final Version

Table of Contents

1. Purpose of Document 4

2. Password 5

3. Timeout..... 12

4. User Access..... 13

5. Inactive Agency and User 14

6. Instructional Training and Exam 15

7. Audit..... 16

8. Signature and Acceptance Page 18

1. Purpose of Document

This Security Document provides guidelines for the Driver and Vehicle Information Database (DAVID) Modernization Project identifying the:

- Authorization Process
- Roles Descriptions
- Account and Use Controls
 - Password
 - Timeout
 - User Access
 - Inactive Agency and User
 - User Access Validation
 - Required Training and Exam Passage
 - Audit
- Data Identification and Classification
- Application Criticality
- Disaster Recovery/High Availability Requirements

2. Authorization Process

There are two options to register a new user in the DAVID System. The first option is the Agency Point of Contact will enter all required information directly into the Add User screen.

The second option is Self-Registration, see process below.

Step 1: Subscriber Information

Please provide the following information for determination of approval for access to the DAVID System.

User should be able to fill in the following information: (Note all fields are required)

- Full Name (First, Middle, Last)
- Business E-Mail
- Contact Phone Number (format field, should accept with and without dashes)
- Business Address – City, State and Zip
- Agency Name (Please select Agency) from the drop down list
- Supervisor Name and Supervisor Phone Number

Step 2: Agreement Section

This subscriber agreement will become effective on the date you submit the request for access to the DAVID System.

By submitting this request I agree:

To the terms and conditions of this governing agency.

I have legal access to view the data pertained in the DAVID System.

To maintain the integrity of this information.

Agree. Request will be sent to the Point of Contact for Approval.

Disagree. Requested action will be terminated.

Step 3: Approval and User Notification

Upon the Agency Point of Contact approving the Self Registrant, an email will be sent to the User with the information submitted by them including Temporary Password.

Information to be include in email

Hello (Name of Self Registrant),

Your request for access to DAVID has been sent to your POC for approval. Your POC will notify you by email.

Details submitted during self-registration:

Agency:	Agency Name
First Name:	Registrant's First Name
Middle Name:	Registrant's Middle Name
Last Name:	Registrant's Last Name

Name Suffix:
Phone Number: (123) 345-6789
Timezone: Eastern Standard Time
Supervisor Name: supervisor
Supervisor Phone: (123) 456-7890
Business Address: 1111
Some City, FL 32311

Email Address: email@email.email

Upon approval you will receive an e-mail confirmation including your new USERID. At that time you will be able to log in with your USERID and PASSWORD.

This e-mail was sent from an address which does not accept incoming e-mail. Please do not reply to this message.

3. Roles

Administrative Roles

- Agency Point of Contact – ability to assign roles to users in their agency; ability to setup sub-agencies within their agencies
- DAVID Administrator – ability to assign roles and setup agencies/sub-agencies; this role is only given to DHSMV staff
- Seatbelt Administrator – ability to associate law enforcement agencies to agencies in DAVID so the law enforcement agency can enter quarterly seatbelt data, ability to report the seatbelt information as required by statute F.S. 316.614(9); this role is only given to DHSMV staff

User Roles

The following roles define the information the user has access to in the DAVID system

- Ability To Search/View Audit Logs
- Activate/Inactivate Photos and Signature
- HazMat Form Processing
- Report Driver for Re-exam
- Search/View Driver License Records
- Search/View Scanned Documents
- Search Motor Vehicle Records
- Search/View/Add/Edit FSBI
- View Driver History
- View Emergency Contact Information
- View Inactivated Photos and Signature
- View Insurance Information
- View Photos and Signatures
- View/Add/Edit Seatbelts
- Ability To Set Default Purpose Code
- CDL Help Desk
- Manage Transactions and Photo/Signatures
- Search Motor Vehicles By Make and Model
- Search/View Motor Vehicle Records
- Search/View/Add Edit FSBI
- View Crash Reports
- View Driver License Transcripts
- View Full SSN
- View Inactivated Transactions
- View Last 4 of SSN
- View Public Official Blocked Information

4. Password

4.1. General

All passwords must adhere to agency standards as of July 1, 2013, Section A-04: Passwords, Section 2.0 Policy and Standards of the Department of Highway Safety & Motor Vehicles *Information Security Policy Manual*

2.0 Policy and Standards

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

1. All end-user passwords used to access DHSMV systems must be constructed and implemented based on system requirements and constraints and in accordance with the following rules to ensure strong password are established:

Must be routinely changed at an interval not greater than 90 days.

Must be different than the last 10 passwords.

Must adhere to a minimum length of 8 characters.

Must be a combination of alpha (upper and lower case), numeric and special characters (unless a particular system does not allow, passwords must consist of at least 3 of the above 4 categories).

Should not be anything that can be easily tied back to the account owner such as: user name, social security number, nickname, relative's names, pet's names, birth date, sports team, etc.

Should not be dictionary words or acronyms.

Newly created or reset passwords must be randomly generated. Use of a default or standard new/reset password is prohibited.

2. Stored passwords must be encrypted.

3. Passwords must not be divulged to anyone. Passwords must be treated as confidential information.

4. If the security of a password is in doubt, the password must be changed immediately.

5. Administrators must not circumvent this policy solely for ease of use.

6. Users should not circumvent password entry with auto logon, application remembering, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the ISM. In order for an exception to be approved, there must be a procedure to change the password.

7. Computing devices should not be left unattended without enabling a password-protected screensaver or logging off of the device.
8. Passwords must not be inserted into email or other forms of electronic communication, unless it is the temporary password that requires changing upon logging in.
9. Passwords should not be written down and stored at your workstation in your office.
10. Passwords stored on physical media must be protected by an approved encryption technology.
11. 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.

If the user password does not meet agency standards for minimum length and complexity, the user will receive a message indicating the password does not adhere to agency standards.

2.2 Expiration

The DAVID password will automatically expire every 90 Days following the Criminal Justice Information Security policy (CJIS). <http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center>

1. Passwords shall be a minimum of 8 characters
2. Passwords shall not be a dictionary word
3. Passwords shall not be a proper name
4. Passwords and User ID shall not be the same
5. Passwords shall be changed at least every 90 days
6. Cannot reuse the last 10 passwords
7. Passwords shall not be transmitted in the clear outside of the secure domain

Agencies may develop more restrictive passwords requirements.

If the user attempts to log in and their password has expired, the user will be re-directed to the change password screen. Once the user has entered their previous password and saved their new password, they will be re-directed to the login page.

2.3 Temporary Password

Users will request access to DAVID using the Self-Registration process. A temporary, one-time use system generated password based on an algorithm will be provided by the system and will expire in 14 days. The user will be required to change the temporary password on initial login.

2.4 Forgot Password

Forgot Password option will be available from log in page. If 'Forgot Password' option is selected, the user will be directed to an intermediate page where they will be required to enter their user id and answer security questions. The 'Answer Security Questions' page will be populated with the pre-selected questions set by the user on initial login. The user must correctly answer 2 questions. The password and answers to security questions are stored using a one-way hashing algorithm.

If the user successfully answers 2 questions, they will be re-directed to enter a new password.

If the user does not successfully answer two (2) questions, they will be presented with a CAPTCHA display. CAPTCHA is intended to ensure a human is attempting to login not a malicious program. The user will be required to respond correctly to the CAPTCHA as well as the correct answers. After ten (10) attempts the user's account will be locked. A message will display "Your account has been locked, contact your administrator." Failing to solve the CAPTCHA does not count as a failed login attempt.

2.5 Locked Account

Users will have five (5) attempts to enter the correct password. On the 5th attempt, the user will be presented with the message: "This is the last password attempt before the account is locked." If the user account is locked the message: "Access Denied. Your account has been locked, contact your administrator" will appear.

2.6 Password Security Questions

Upon initial login the system requires two (2) security questions to be selected and answered from the 15 possible questions. This information will be stored for future use when the forgotten password option is selected. The user is able to reset the security questions at any time. The password and answers to security questions are stored using a one-way hashing algorithm.

Below is a list of possible questions:

1. What was your childhood nickname?
2. In what city did you meet your spouse/significant other?
3. In what city or town was your first job?
4. What is the name of company of your first job?
5. What was your favorite place to visit as a child?
6. What was your dream job as a child?
7. What is the street number of the house you grew up in?
8. What was your high school mascot?
9. What is the name of the first school you attended?
10. Who was your childhood hero?
11. What is your mother's middle name?
12. What was the make and model of your first car?
13. What is the color of your mother or father's eyes?

14. What was the name of your first pet?
15. What is your maternal grandmother's maiden name?

5. Timeout

5.1. General

User timeout is 30 minute of inactivity for all users unless the user qualifies under the *Law Enforcement Exemption*. The *Law Enforcement Exemption* is eight (8) hours of inactivity. Logging on after such time will result in "Access Denied" error response.

5.2. Law Enforcement Exemption Option

The Law Enforcement Exemption option can only be modified by Users with the DHSMV Administrator or Agency Point of Contact (POC) Role. The message below will be displayed when the Extended Session Timeout for Law Enforcement is set to YES.

Please be aware, setting Extended Session Timeout (Law Enforcement) to "Yes" will allow User exemption from the Department's standard Security Access Controls.

In the interest of officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location, are exempt from the Department's standard Security Access Control requirement.

This Role should be granted to Law Enforcement or selected law enforcement personnel only.

If you are unsure about granting this exception, please contact your Administrator or Legal Department in your Agency for assistance.

6. User Access

User access times are designated by the Agency POC or DHSMV Administrator and cannot be altered by the User. Attempting to access the system during non-designated times will result in the user receiving the message: "Access Denied. Accessing System Outside of Designated Time Is Not Allowed".

User Access Validation

The Agency Point of Contact or their designee(s) are required to review and validate (to the application owner) that their user account list is up-to-date on a bi-annual basis.

7. Inactive Agency and User

There are only two statuses for agencies and users, active or inactive. An Agency POC can inactivate the users in their agency or sub-agency. The DHSMV Administrator has the ability to inactivate an agency or any user at any time.

When an agency with an *Inactive* status attempts to access the DAVID system, the user will receive the message: "Agency is inactive and to contact their POC".

When a user with an *Inactive* status attempts to access the DAVID system, the user will receive the message: "Your account has been inactivated, please contact your Agency POC for assistance".

8. Instructional Training and Exam

All users must take the mandatory Instructional Training and pass the Exam prior to gaining access into the DAVID system. Instructional Training and Exam completion date will be captured and stored. The Instructional Training and Exam is required on an annual basis in order for the user to maintain their access to the DAVID system.

The Instructional Training and Exam have the following features:

- Auto scoring of the responses
- Ten (10) random questions generated from list of questions
- No time limit for completing the training
- If a user exits the exam without completing, they will have to start over from the beginning
- Upon successful completion of the exam with an 80% score or higher, the user will gain access to the DAVID system

9. Audit

The DAVID system will log every call a user makes to view driver license and motor vehicle data. This will include User ID, user name, date and time of access, the page accessed, purpose code and the agency the user is assigned. Audits may be performed by DHSMV Administrator, Agency POC or assigned Supervisor.

The DHSMV Administrator can audit any Agency or User.

The Agency POC or Supervisor can only audit users within their agency or sub-agency.

Safeguarding Information Required by Memorandum of Understanding (MOU)

The Parties shall access, use and maintain the confidentiality of all information received under this agreement in accordance with Chapter 119, Florida Statutes, and DPPA. Information obtained under this agreement 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 knowingly discloses any information in violation of DPPA may be subject to criminal sanctions and civil liability.

The Parties mutually agree to the following:

- A.** Information exchanged will not be used for any purposes not specifically authorized by this agreement. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, and the dissemination, sharing, copying or passing of this information to unauthorized persons.
- B.** Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons.
- C.** Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.
- D.** All personnel with access to the information exchanged under the terms of this agreement will be instructed of, and acknowledge their understanding of, the confidential nature of the information and of the criminal sanctions specified in state law for unauthorized use of the data. These acknowledgements are automatically maintained electronically when the DAVID tutorial is completed by each user annually.
- E.** All access to the information must be monitored on an on-going basis by the Requesting Party. In addition, the Requesting Party must complete an annual affirmation indicating compliance with the requirements of this agreement to ensure proper and authorized use and dissemination. The Providing Agency shall receive an annual affirmation from the Requesting Party indicating compliance with the requirements of this agreement no later than 45 days after the anniversary date of this agreement.

F. By signing the MOU, the representatives of the Providing Agency and Requesting Party, on behalf of the respective Parties attest that their respective agency procedures will ensure the confidentiality of the information exchanged will be maintained.

Compliance and Control Measures

A. Internal Control Attestation - This MOU is contingent upon the Requesting Party having appropriate internal controls over personal data sold or used by the Requesting Party to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. Upon request from the Providing Agency, the Requesting Party must submit an attestation from a currently licensed Certified Public Accountant performed in accordance with American Institute of Certified Public Accountants (AICPA) "Statements on Standards for Attestation Engagement." In lieu of submitting the attestation from a currently licensed Certified Public Accountant, Requesting Party may submit an alternate certification with pre-approval from the Department. In the event the Requesting Party is a governmental entity, the attestation may be provided by the entity's internal auditor or inspector general. The attestation must 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 must be received by the Providing Agency within 180 days of the written request. The Providing Agency may extend the time to submit the attestation upon written request and for good cause shown by the Requesting Agency.

B. Misuse of Personal Information – The Requesting Party must immediately notify the Providing Agency and the affected individual following the determination that personal information has been compromised by any unauthorized access, distribution, use, modification, or disclosure. The statement to the Providing Agency must provide the date and the number of records affected by any unauthorized access, distribution, use, modification, or disclosure of personal information. Further, as provided in section 817.5681, Florida Statutes, the document must provide a statement advising if individuals whose personal information has been compromised have been notified and, if not, when they will be notified. The statement must include the corrective actions and the date these actions are completed by the Requesting Party.

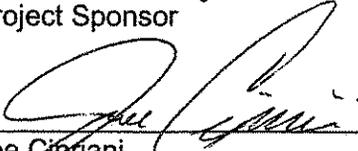
10. Signature and Acceptance Page

We have reviewed the DAVID Security Document and agree that the content of the document is accurate as of this point.



Maureen Johnson, Bureau Chief
Project Sponsor

3/26/14
Date



Joe Cipriani
Information Security Manager

3/12/2014
Date