Appendix I: Security Policy

The RMV is committed to maintaining a secure system. Therefore, it is the responsibility of the user to read, understand, and follow this policy. A user who fails to follow this policy may result in termination of your System ID, criminal proceedings and/or $5,000 fine per violation. You, as the user, have been granted access to the RMV system for the express purpose of fulfilling your job duties. All activity on your RMV System ID(s) is recorded, stored, monitored and audited.

RMV System ID(s) and Passwords

RMV System ID(s) is the term for an ID that allows users access to information contained in the RMV system, including the ALARS/UMS Signon ID.

The RMV System ID(s) controls the specific function(s) access that you are authorized to use. These functions are determined by your agency needs. The RMV System ID(s) and Password are for the exclusive use of the individual to whom they are assigned. The password associated with an RMV System ID(s) must not be divulged to another person. You are not permitted to use, or attempt to use, an RMV System ID(s) or password issued to another person. You must take all reasonable precautions to protect your RMV System ID(s) and password. You are personally responsible for all activity that occurs when your RMV System ID(s) is in use. This means that you will be held personally accountable for the money collected (if applicable), the accuracy of any transaction performed, and any inquiry conducted using your RMV System ID(s) and Password. All transactions are official records of the RMV. If you suspect that a password has been compromised, you should contact RMV IS Security immediately at 857-368-7930. The system will automatically prompt you to change your password. Your RMV System ID will be deactivated if you do not change your password for 60 days or within 30 days of issuance of your RMV System ID. If your RMV System ID(s) get deactivated, you must contact your agency's RMV contact and they will need to re-complete a User Request form to get your RMV System ID reactivated.

It is a violation of RMV policy to leave your computers unattended with the RMV System ID(s) and passwords actively logged on. You must lock the computer or log off the RMV system before leaving your computer.

ALARS Password Requirements for System IDs

Standards for Selecting Strong ALARS Passwords

Passwords must meet the following requirements:

- ✓ Must be ***EXACTLY*** 8 characters
- ✓ First character of password must be a letter

- ✓ Must have at least one number
- ✓ Password must contain at least one letter or number, symbols are not allowed
- ✓ Password cannot be equal to old passwords
- ✓ Repeating characters are not allowed such as A**PP**LE123
- ✓ Passwords may not be changed twice in one day

Password Protection Standards

DO NOT:

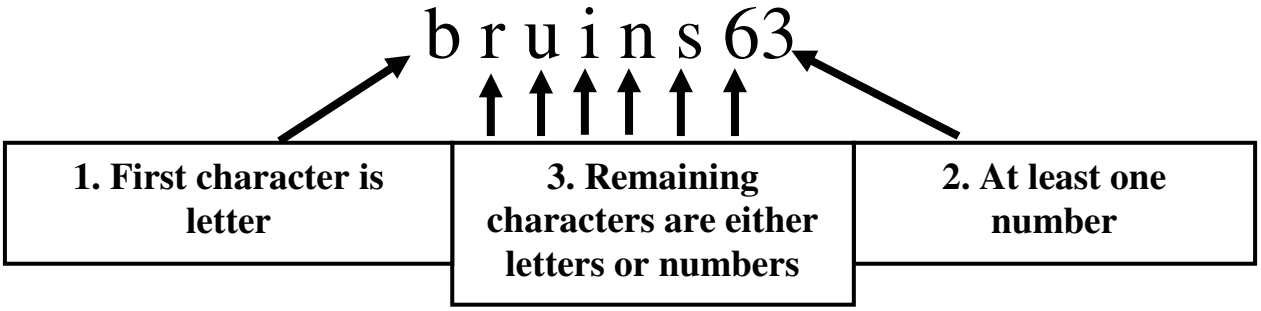
- ✓ Use MassDOT account passwords for non-MassDOT access (for example, an account on an Internet Website)
- ✓ Use the same passwords for all accounts such as Outlook or ALARS
- ✓ Use generic or group passwords
- ✓ Share passwords with anyone, including administrative assistants or secretaries, your boss, co-workers while on vacation, or family members
- ✓ Reveal a password over the phone to ANYONE
- ✓ Put a password in an email message
- ✓ Talk about a password in front of others
- ✓ Hint at the format of a password (e.g., "my family name")
- ✓ Reveal a password on questionnaires or security forms
- ✓ Use the "Remember Password" feature of applications

  If you see a prompt asking you if you want your password remembered, click "Never."
- ✓ Write passwords down and store them anywhere in your office
- ✓ Store passwords in a file on ANY computer system (including *Palm Pilot*, *Blackberry*, mobile phones or similar devices) without encryption (converting data into code)

All passwords should be treated as sensitive, confidential MassDOT information. If an account or password is suspected to have been compromised, report the incident to IS Security at 857-368-7930.

Password cracking or guessing may be performed periodically by IT Security. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Example of a valid password:



Do NOT use any example passwords!

How to Change Your Password for ALARS System IDs

Your password for ALARS/UMS expires upon issuance of your RMV System ID and every 60 days thereafter. Once you log into ALARS/UMS Signon Screen/Main Menu, the system will automatically bring you to the NPAS Screen (Change User Password Screen) to change your password.

Please note: The message line will help you with changing your password tremendously. The message line is located next to the function after the MSG. **DO NOT HIT TAB OR ENTER in between typing your password on each line; once you type in an 8 character password, the system will automatically move the cursor to the next field. Once both passwords have been typed twice, the cursor will move to the function field and you must hit ENTER.**

```
MM/DD/YY  HH:MM   MASSACHUSETTS REGISTRY OF MOTOR VEHICLES    UGN0280
                          CHANGE USER PASSWORD
FUNCTION: NPAS MSG: PF12 TO UPDATE DATABASE

CURRENT USER:                    XXXX
NEW PASSWORD:
RETYPE NEW PASSWORD
```

1. Type in a password you created using the password strong standards, THEN type in the same password again.
2. After you type in the password twice, press ENTER.
3. The message will appear 'PF12 TO UPDATE DATABASE'. Press the F12 key.
4. The message will appear 'UPDATE COMPLETED, NEW FUNCTION REQUIRED'. You have successfully updated your password and you can now type in a function to move to different screen.

To change your password at any time: Go to the NPAS screen, and follow the instructions above.

Common Error Messages when change a password:

PASSWORD 1 MUST BE SAME AS PASSWORD 2

Solution 1: Do not hit the tab or enter key after typing the password in the 1st field.
Solution 2: Make sure you are typing the same password in both fields.

PASSWORD MUST HAVE A NUMERIC AND ALPHA CHARACTER

Solution: Password must contain at least one letter or number.

NEW PASSWORD SAME AS CURRENT PASSWORD

Solution: You can not use the password given by the RMV or your former password; you must create a new password.

SAME CHARACTER TWICE IN A ROW

Solution: No repeating characters such as a**pp**le123; however **p**eo**p**le12 is acceptable.

INVALID CHARACTERS IN PASSWORD

Solution: Symbols and spaces are not allowed in passwords.

Error Messages when logging into the Signon Screen

PASSWORD ENTER IS INVALID

Type current password. If you do not know your current password, call IS Security at 857-368-7930.

CLERK EFFECTIVE DATE NOT REACHED OR INVALID

You have typed your password incorrectly 3 times or more or your ID has been deactivated by IS Security. Call IS Security at 857-368-7930.

Data Confidentiality

The RMV system stores personal and confidential information. The Federal Driver Privacy Protection Act (DPPA) protects this information. The DPPA broadly defines personal information as information that identifies an individual, including an **individual's photograph, social security number, driver identification number, name, address, telephone number, and medical or disability information.** Specifically excluded from the definition of personal information is information on vehicular accidents, driving violations, and driver's status.

The following rules apply for all personal information contained in RMV records:

- Personal information must not be visible to customers
- Personal information must be shredded or deposited into a locked shredder box when no longer needed
- Personal information must never be brought outside of the workplace, unless required to perform your job duties
- Personal information must not be used in furtherance of any illegal act, including violation of any criminal or civil laws, for any political purpose, or for any commercial purpose
- Personal information must never be disseminated, unless such dissemination is required by your job duties
- Personal information must never be sold or bartered. You must never charge a fee for, or receive any other consideration for, RMV System information
- You must never knowingly obtain, disclose, or use RMV System information for a purpose not permitted under 18 USC §2721. If you do, you will be liable to the individual to whom the personal information pertains
- You must never misrepresent your identity or make a false statement in connection with any request for personal information with the intent to obtain personal information in a manner not authorized

Under no circumstances is it permissible for you to acquire access to the RMV system unless such access is required to perform your job duties. You may not attempt to gain or assist others in gaining unauthorized access to the RMV system.