MOVEit™ End User Request Form

MassDOT RMV-IS Security
25 Newport Avenue Ext. ● Quincy, MA 02171

REGISTRY OF MOTOR VEHICLES

Effective Date: _____

Instructions

This request form needs to be completed for all Business Partner end users that will need a MOVEit™ Logon for file exchange. Completed forms will need to be uploaded via the RMV's Community Portal.

A. Business Information

Legal Business Name

DBA | Federal Employer ID Number (FEIN)

Business Mailing Address:
Street | City | State | Zip Code

Business Contact (please print clearly) | Phone | Email

B. Request Type

☐ New User ☐ Change Access Roles or ☐ Reactivate Access – To delete access, email: RMVBusinessPartners@dot.state.ma.us

C. File Type

☐ Bulk Data ☐ Excise Tax Commitments ☐ Insurance Policy Management (IPM), formerly UMS ☐ Non-Renew ☐ SDIP

D. Business Partner Certification and Signature

I, _____, (print name) hereby certify the below named individual as a permitted user for this business.

Business Contact Signature: _____ Date: _____

E. End User Information

End User Name | End User MA Driver's License/ID #*:

Last 4 Digits of Social Security | *Non-Mass residents must attach a copy of their state-issued driver's license or if you are a local, state, or federal government employee, attach an unexpired employer-issued ID.

User's Business Mailing Address:

User's Business Email Address: | IP Address

F. RMV System Policy

End User Must read, understand, and follow this policy

The RMV System(s) stores personal data. The Federal Driver Privacy Protection Act (DPPA), the Massachusetts Identity Theft Act, G.L. c. 93H, Regulations Authorizing Disclosure of Massachusetts Driver's License or Learner's Permit Applicant Information, 940 CMR 37.00, and the Standards for the Protection of Personal Information of Residents of the Commonwealth 201 C.M.R. 17.00 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.

You have been granted access to RMV System(s) because your company is a permitted business partner allowed to access RMV records. If you are not clear on the business purpose for which you may access the RMV data, talk to your manager/supervisor.

The RMV may conduct background checks to ensure that you have not been convicted of a felony involving violence, dishonesty, deceit or indecency. If you have been convicted of such a felony you may not be authorized to access the RMV systems or view its data.

You will be held personally responsible for all activity that occurs on your issued security credentials including: any money collected, the accuracy of any transaction performed, and any inquiry conducted.

All transactions are the official records of the RMV; they are recorded, stored, monitored, and audited. The RMV may in its sole discretion require you to explain and/or demonstrate the legitimate business purpose or permitted use for accessing the RMV's data for any particular transaction.

As the end user you will:

1. Never divulge your password to anyone.
2. Only access the RMV data for approved business purposes.
3. Never use such records or information for the purpose of enforcing federal immigration law (including the investigation, participation, or cooperation with the enforcement of such law).
4. Never disclose RMV data to any agency that primarily enforces immigration law or to any employee or agent of any such agency; unless you are provided with a lawful court order or judicial warrant signed by a judge appointed pursuant to Article II of the U.S. Constitution, a federal grand jury or trial subpoena, or as otherwise required by federal law.
5. Notify the RMV immediately if you receive a court order or judicial warrant regarding RMV obtained data or records.
6. Never leave your computer unattended with the RMV System actively logged on. You must lock the computer or log off before leaving your computer unattended.
7. Ensure that RMV records are not visible to unauthorized individuals.
8. Shred or deposit RMV records into alocked shredder container when no longer needed.
9. Never bring RMV records or use the RMVsystem(s) outside the workplace, unlessrequired to perform your job duties.
10. Never knowingly obtain, disclose, or useRMV records for a purpose not permittedunder the DPPA. You may be liable forimpermissible dissemination of personalinformation to any individual to whom thepersonal information pertains.
11. Never misrepresent yourself or make afalse statement in connection with arequest for personal information with the intention of obtaining said information in a manner not authorized in your companies signed Agreement for Access to Records and Data Maintained by the Registry of Motor Vehicles or the DPPA.
12. Never disseminate RMV records unless such dissemination is required by your specific job duties.
13. Never use RMV data and records in the furtherance of an illegal act, including aviolation of any criminal or civil laws.
14. Never sell, barter, charge a fee or receive any other consideration for RMV records and data.

Contact RMV IS Security at RMVBusinesspartners@dot.state.ma.us or 857-368-7930 immediately if you suspect your account has been compromised.

G. End User Certification and Signature

I, _____, (print name) agree and will abide by the policy described above. Violation of this policy may be subjected to disciplinary actions, including termination of RMV access, criminal proceedings and/or fines per each violation.

Signed and sworn to under the pains and penalties of perjury.

End User Signature: _____ Date: _____