



ADR Security Form

ADR Account# _____

All ADR Subscribers must take precautions to secure any system or device used to access DMV Data and must adhere to the following security requirements.

Account Information. Subscriber:

- (a) shall remain fully responsible for protecting their ADR account number, User IDs, and passwords granted in connection with the ADR Subscription Agreement and shall be liable for any unauthorized use of account number, User IDs or passwords granted in connection with this Agreement;
- (b) shall not provide any such information to any unauthorized party;
- (c) agrees to limit access to DMV Data only to its current employees whose responsibilities require such access and only to the extent necessary for its proper use in accordance with, and as Authorized by, the ADR Subscription Agreement;
- (d) agrees to immediately terminate the User ID and password granted in connection with the ADR Subscription Agreement for any employee that leaves Subscriber's organization or violates any terms or conditions of this Agreement;
- (f) agrees Subscriber's employees will be forbidden to attempt to obtain DMV Data on themselves, associates or any other persons, except in the exercise of their official duties; and
- (g) Each user of your system access software must be assigned a unique User ID and password.

Information Security. Subscriber:

- (a) shall implement a reasonable system and data security procedures to protect DMV Data provided by ADR under this agreement from theft, unauthorized disclosure or any use not specifically permitted under this Agreement. Such reasonable procedures must include, but are not limited to, User ID and password access policies, firewalls, background investigations of employees or any other individuals authorized to access DMV Data, and execution of confidentiality agreements by such employees or other individuals with authorized access. Upon request, Subscriber will provide an electronic copy of their IT Security Policies and Procedures;
- (b) may transfer DMV Data over the Internet; provided: Subscriber (and, if applicable, its customers) uses current security technologies, including 128 bit encryption, firewall, and user authentication;
- (c) agrees all Subscriber information technology assets that house or process DMV data will be physically secured from unauthorized access and physical access must be tightly controlled;
- (d) agrees adequate measures will be employed to insure that unauthorized users cannot successfully attack Subscriber information technology assets in a manner that allows DMV data to be compromised;
- (e) Subscriber information technology hosts and networks that hold or process DMV data will be periodically scanned for known vulnerabilities to see if vulnerabilities could be exploited;
- (f) Subscriber will have a formal procedure in place to install vendor-recommended security patches in a timely manner for all information technology assets, hosts and networks, that process DMV data;

- (g) Subscriber will provide annual security training to educate their employees on best security practices, and have a confidentiality agreement signed by each individual who accesses DMV data;
- (h) Subscriber will have a Computer Incident Policy and Procedure program in place. If Subscriber experiences a computer Incident ADR will be notified within one (1) day; and
- (i) Subscriber must not use, compile, or store any DMV Data in any database, and shall promptly and adequately destroy any DMV Data in its possession when the DMV Data is no longer required for the purpose as stated in this agreement or sooner if required by law.

As an authorized representative of Subscriber you and your employees may have access to official government motor vehicle and/or driver record information contained in DMV Data. The Confidentiality of the information contained within these Records shall be maintained at all times. Information contained in records shall not be distributed, sold or shared with any third party nor used by you in any way except as expressly authorized by law. Disclosure of such information may be cause for criminal and/or civil legal action against you, the Subscriber, and any involved third party. Neither ADR nor any Jurisdiction providing DMV Data shall be in any way responsible for defense of any such action. ***Pursuant to State and Federal law, any person who willfully and knowingly obtains, resells, transfers, or uses information in violation of law may be subject to criminal charges and/or liable to any injured party for treble damages, reasonable attorneys; fees, and costs. Other civil and criminal laws may also apply.***

I, ON BEHALF OF SUBSCRIBER, AGREE TO COMPLY WITH THE SECURITY REQUIREMENTS NOTED HEREIN. I FURTHER CERTIFY THAT I HAVE DIRECT KNOWLEDGE OF THE FACTS CERTIFIED HEREIN AND AM AUTHORIZED TO AGREE TO THESE ITEMS HEREIN.

Subscriber

Address

Authorized Signature

Date

Name (Print)