Motor Vehicle Administration
6601 Ritchie Highway, N.E.
Glen Burnie, Maryland 21062

ICD-072 (10-14)

MD MVA eFR-19 Remote Access Request Form

REQUESTER INSTRUCTIONS: **DATE of REQUEST :**

Complete top section of form, listing each "Insurer" company you are authorized to issue Maryland Insurance Certifications (Form FR-19), "SignDate" sign, and date. This request may require approval from your Insurance Company or Agency Officer. Mail to ICD Business Administrator at MVA Room 140, 6601 Ritchie Hwy, Glen Burnie, MD 21062, for authorization signature. ICD Business Administrator will submit signed form to MVA Security Officer for verification of access type(s).

ACTION: ❑ New Request ❑ Account Change ❑ Account Deletion ❑ Add Insurer Association ❑ Remove Insurer Association

USERID: ______________________ Producer License No issued by MD Ins Admin ______________________
(assigned by MVA)

MD Insurance Agent: ____ Phone: ( ) ______________
Last First MI Suffix

Ins Co / Agency Name: ____________________________ Address: ________________________________

____

Agency Phone Number: ( )______________________ Agency Fax Number: ( )______________________

EMail Address: ____

Insurer's Agent is Authorized to Issue Maryland Insurance Certifications (form FR-19) for: (use additional sheet if more than 6 insurers)

Insurer NAIC Code is the 5 Digit Number assigned by the National Association of Insurance Commissioners

Insurer NAIC	**Insurer Name**	**Insurer NAIC**	**Insurer Name**

Purpose of Remote Access: To report Maryland Insurance Certifications Forms FR-19 electronically to Insurance Compliance Division.

ACKNOWLEDGMENT: Remote Access to the MDOT/MVA network is a privilege. I hereby acknowledge that remote access is authorized for my use only and that all passwords and user names are to be kept confidential at all times. By requesting a remote access account, I acknowledge that I will install or already have installed virus protection software on my remote (this includes business, home or laptop) system. In addition, I authorize MVA and/or their contractor to test the security of my connection to the MVA network by performing a coordinated vulnerability assessment when needed of my connection to the MVA network. Installation of the virus protection and applying virus signature updates is my responsibility. I understand that failure to do so may result in loss of remote access privileges. MVA employees are not responsible for any operating system, hardware or software application problems encountered by any MVA Remote Access User when using the designated applications to connect to the MVA network. I have signed the MDOT Security Advisory agreement and I am aware of terms and conditions of the agreement.

Requester Signature/Date: ____

INSURANCE CO/AGENCY OFFICER: I authorize the requestor to be granted access to the MD ACIS eFR-19 Internet application.

ON BEHALF OF INSURANCE COMPANY AGENCY ____

INSURANCE CO/AGENCY OFFICER Name & Title (*Please Print*): ______________________________

INSURANCE CO/AGENCY OFFICER Signature/Date: ______________________________

MD MVA ACIS BUSINESS ADMINISTRATOR: I authorize the requestor to be granted access to the ACIS eFR-19 internet application.

MVA ACIS Business Administrator Name (*Please Print*): ______________________________

MVA ACIS Business Administrator Signature/Date: ______________________________

IMPLEMENTATION DETAILS (TO BE COMPLETED BY MVA ONLY)

MVA Security Officer Signature/Date: ______________________________

For more information, please call: **410-768-7000** (to speak with a customer agent).
TTY for the hearing impaired: **1-800-492-4575**. Visit our website at: **www.MVA.Maryland.gov**

MARYLAND DEPARTMENT OF TRANSPORTATION
OTTS OFFICE OF DATA SECURITY
SECURITY ADVISORY

This ADVISORY is initiated for INFORMATIONAL purposes only. The following paragraphs shall in no way be construed as a waiver by the undersigned of the rights and protections provided by COMAR (Code of Maryland Regulations) Title 11, Department of Transportation, Subtitle 2, Transportation Service Human Resources System, if applicable, and/or by law or regulation.

The Office of Information Resources, its client agencies and their customers adhere to State data processing security policies as set forth in Executive Order 01.01.1983.18 (Privacy and State Data system Security); MD Code Ann., Criminal Law Article, §§ 8-606 (Making false entries in public records and related crimes) and 7-302 (Unauthorized access to computers and related material); MD Code Ann., General Provision Article, Title 4 (Maryland Public Information Act); MD Code Ann., Transportation Article, §§12-111 through 12-113 (Motor Vehicle Administration Records); and, as published by the Secretary of the Department of Budget and Management from time to time under MD Code Ann., State Finance and Procurement Article, Title 3A, Subtitle 3 (Information Processing).

Federal laws affecting access to and use of computer information include, but are not limited to, the following: 15 U.S.C. § 271 *et seq*. (National Institute of Standards and Technology); 44 U.S.C. § 3541 *et seq*. (Federal Information Security Management Act of 2002); 49 U.S.C. § 30301 *et seq*. (National Driver Register Act of 1982); 5 U.S.C. § 552 (Freedom of Information Act); 5 U.S.C. § 552a (Privacy Act of 1974); 18 U.S.C. § 1001 *et seq*. (Computer Fraud and Abuse Act of 1986); 17 U.S.C. § 109 (Computer Software Rental Amendments Act of 1990); 15 U.S.C. § 1681 *et seq*. (Fair Credit Reporting Act); 18 U.S.C. § 1030 (Computer Crime Statute of 1984); 18 U.S.C. § 2721 *et seq*. (Driver's Privacy Protection Act of 1994); and Federal Copyright Law.

Specifically **PROHIBITED ACTS** include, but are not limited to:

1. Unauthorized access to or use of a computer, data or software.
2. Unauthorized copying or disclosure of data or software.
3. Obtaining unauthorized confidential information.
4. Unauthorized modification or altering of data or software.
5. Introduction of false information (public records).
6. Disruption or interruption of the operation of a computer.
7. Disruption of government operations or public services.
8. Denying services to authorized users.
9. Taking or destroying data or software.
10. Creating/altering a financial instrument or fund transfer.
11. Misusing or disclosing passwords.
12. Breaching a computer security system.
13. Damaging, altering, taking or destroying computer equipment or supplies.
14. Devising or executing a scheme to defraud.
15. Obtaining or controlling money, property, or services by false pretenses.

Authorized access to, including **INTERNET** and **INTRANET**, and use of information and computer resources is limited to the **PURPOSE** for which these privileges are granted. All authorized users during the term of their access and thereafter, shall hold in strictest confidence and not willfully disclose to any person, firm or corporation without the express authorization of the Director, OIR, any information related to security, operations, techniques, procedures or any other security matters. Any breach of security will be promptly reported to the Director, Office of Information Resources, designee or security officer.

I acknowledge that I have read and understand the foregoing security advisory.

Name: ______________________________
(Please print or type)

Date: ______________________ ______________________________
(Signature)