Maryland Department of Transportation
Office of Transportation Technology Services

SECURITY ADVISORY FORM

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) Volume XII Title II Transportation, if applicable, and/or by law or regulation.

The Office of Transportation Technology Services, 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. Ann. Code, art. 27 §§ 45A (falsification of public records) and 146 (unauthorized access); Md. Code Ann., State Gov't §§ 10-611, 10-616 and 10-626 (Maryland Public Information Act); and, as published by the Secretary of the Department of Budget and Management from time to time under Md. Code Ann., State Fin. & Proc. § 3-403.

Federal laws affecting access to and use of computer information include, but are not limited to, the following: 15 U.S.C.S. § 271, 40 U.S.C.S. § 759 (Computer Security Act of 1987); 5 U.S.C.S. § 552 (Freedom of Information Act); 5 U.S.C.S. § 552a (Privacy Act of 1974); 18 U.S.C.S. § 1001 (Computer Fraud and Abuse Act of 1986); § 17 U.S.C.S. § 109 (Computer Software Rental Amendments Act of 1990); and 15 U.S.C.S. § 1681 (Fair Credit Reporting Act.

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

1. Unauthorized access to, use, modification, or destruction of a computer, data or software.
2. Unauthorized disclosure or distribution of Personally Identifiable Information (PII).
3. Unauthorized copying or disclosure of data or software.
4. Obtaining unauthorized confidential information.
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. Creating/altering a financial instrument or fund transfer.
10. Misusing or disclosing passwords.
11. Breaching a computer security system.
12. Damaging, altering, taking or destroying computer equipment or supplies.
13. Devising or executing a scheme to defraud.
14. 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, OTTS, any information related to security, operations, techniques, procedures or any other security matters. Any breach of security will be promptly reported to the Director, MDOT Office of Cybersecurity, designee or security officer.

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

Date: _____ Name: _____
(Please print or type)

EIN: _____ _____
(Signature)

Badge Number: _____ Logonid: _____