

**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 an employee of the rights and protections provided to employees by the Merit System Law (Article 64A of the Annotated Code of Maryland).

The Office of Information Resources and its Client/Agencies adhere to the State Policy: Data Processing Resources Security, as authorized by the Governor's Executive Order 01.01.1983.18; the State Data Security Committee, State Agency Data System Security Practices; Article 27, Section 45A and 146 of the Annotated Code of Maryland. In addition, other Federal and State Laws and Regulations affect the access to and use of computer information such as the U. S. Computer Crime Statute (1984), Computer Security Act of 1987, National Driver Register Act of 1982 (Public Law 97-364), Privacy Act of 1974, Freedom of Information Act, Computer Software Rental Amendments Act (1990), Fair Credit Reporting Act, Computer Fraud and Abuse Act (1986), Federal Driver Privacy Act 1994; 18 U.S.C. § 2720 et seq. and, with §§ 10-611, 10-616, 10-626 of the State Government Article; § 12-111 through 12-113 of the Transportation Article, Annotated Code of Maryland, which limit access to personal information from public records in Maryland 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.

Date: _____

Name:

(Please print or type)

SSN: _____

(Signature)