

TENNESSEE DEPARTMENT OF REVENUE  
SECURITY REVISION FORM

SECURITY GROUP: \_\_\_\_\_ RACF KEY: \_\_\_\_\_

USER NAME: \_\_\_\_\_ SSN: \_\_\_\_\_

**PLEASE CHECK ONLY ONE:**

- Add a new USERID  
 Delete an existing USERID  
 Modify an existing USERID  
 Other (specify in Addition User Security Access section)

Date Hired \_\_\_\_\_

Date Left \_\_\_\_\_

Work Address \_\_\_\_\_

City/State/Zip \_\_\_\_\_

COUNTY \_\_\_\_\_

Work Phone (615) \_\_\_\_\_

**VEHICLE REGISTRATION:** (Place 'x' in appropriate box(es). Place DRS or RMT printer numbers in last column.)

DRS/RMT #

<input type="checkbox"/>	DIGIMARE Digital Photo Group for DL Use	<input type="checkbox"/>	Motor Vehicle Inquiry Screens	<input type="checkbox"/>	Renewal	<input type="checkbox"/>	Renewal Print (DRS#)	
<input type="checkbox"/>		<input type="checkbox"/>	Handicap Placards	<input type="checkbox"/>	Title	<input type="checkbox"/>	Title Print (DRS#)	
<input type="checkbox"/>	DL Issuance	<input type="checkbox"/>	Tag Inventory	<input type="checkbox"/>	Application	<input type="checkbox"/>	Application Print (DRS#)	
<input type="checkbox"/>		<input type="checkbox"/>	NMVTIS	<input type="checkbox"/>	Letter System	<input type="checkbox"/>	Letter Print (DRS#)	
<input type="checkbox"/>	DL Inquiry	<input type="checkbox"/>	INFOPAC	<input type="checkbox"/>		<input type="checkbox"/>	Invoice Print (RMT#)	

**ADDITIONAL USER SECURITY ACCESS:**

SECURITY GROUP APPROVAL: \_\_\_\_\_ DATE: \_\_\_\_\_

ITR APPROVED BY: \_\_\_\_\_ DATE: \_\_\_\_\_

ITR COMPLETED BY: \_\_\_\_\_ DATE: \_\_\_\_\_



## STATE OF TENNESSEE

### Acceptable Use Policy Network Access Rights and Obligations

**Purpose:**

To establish guidelines for State-owned hardware and software, computer network access and usage, Internet and email usage, telephony, and security and privacy for users of the State of Tennessee Wide Area Network.

**Reference:**

*Tennessee Code Annotated, Section 4-3-5501, et seq.*, effective May 10, 1994.

*Tennessee Code Annotated, Section 10-7-512*, effective July 1, 2000.

*Tennessee Code Annotated, Section 10-7-504*, effective July 1, 2001.

*State of Tennessee Security Policies.*

**Objectives:**

- Ensure the protection of proprietary, personal, privileged, or otherwise sensitive data and resources that may be processed in any manner by the State, or any agent for the State.
- Provide uninterrupted network resources to users.
- Ensure proper usage of networked information, programs and facilities offered by the State of Tennessee networks.
- Maintain security of and access to networked data and resources on an authorized basis.
- Secure email from unauthorized access.
- Protect the confidentiality and integrity of files and programs from unauthorized users.
- Inform users there is no expectation of privacy in their use of State-owned hardware, software, or computer network access and usage.
- Provide Internet and email access to the users of the State of Tennessee networks.

**Scope:**

This Acceptable Use Policy applies to all individuals who have been provided access rights to the State of Tennessee networks, State provided email, and/or Internet via agency issued network or system User ID's. The scope does not include State phone systems, fax machines, copiers, State issued cell phones or pagers unless those services are delivered over the State's IP network.

**Use and Prohibitions:****A. Network Resources**

State employees, vendors/business partners/subrecipients, local governments, and other governmental agencies may be authorized to access state network resources to perform business functions with or on behalf of the State. Users must be acting within the scope of their employment or contractual relationship with the State and must agree to abide by the terms of this agreement as evidenced by his/her signature. It is recognized that there may be incidental personal use of State Network Resources. This practice is not encouraged and

employees should be aware that all usage may be monitored and that there is no right to privacy. Various transactions resulting from network usage are the property of the state and are thus subject to open records laws.

#### **Prohibitions**

- Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation.
- Installing software that has not been authorized by the Office for Information Resources of the Department of Finance and Administration.
- Attaching processing devices that have not been authorized by the Office for Information Resources of the Department of Finance and Administration.
- Using network resources to play or download games, music or videos that are not in support of business functions.
- Leaving workstation unattended without engaging password protection for the keyboard or workstation.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using network resources in support of unlawful activities as defined by federal, state, and local law.
- Utilizing network resources for activities that violate conduct policies established by the Department of Human Resources or the Agency where the user is employed or under contract.

#### **B. Email**

Email and calendar functions are provided to expedite and improve communications among network users.

#### **Prohibitions**

- Sending unsolicited junk email or chain letters (e.g. "spam") to any users of the network.
- Sending any material that contains viruses, Trojan horses, worms, time bombs, cancel bots, or any other harmful or deleterious programs.
- Sending copyrighted materials via email that is either not within the fair use guidelines or without prior permission from the author or publisher.
- Sending or receiving communications that violate conduct policies established by the Department of Human Resources or the Agency where the user is employed or under contract.
- Sending confidential material to an unauthorized recipient, or sending confidential e-mail without the proper security standards (including encryption if necessary) being met.

Email created, sent or received in conjunction with the transaction of official business are public records in accordance with T.C.A 10-7-301 through 10-7-308, and the rules of the Public Records Commission. A public record is defined as follows:

*"Public record(s)" or "state record(s)" means all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency. (T.C.A. 10-7-301 (6)).*

State records are open to public inspection unless they are protected by State or Federal law, rule, or regulation. Because a court could interpret state records to include draft letters, working drafts of reports, and what are intended to be casual comments, be aware that anything sent as electronic mail could be made available to the public.

### **C. Internet Access**

Internet access is provided to network users to assist them in performing the duties and responsibilities associated with their positions.

#### **Prohibitions**

- Using the Internet to access non-State provided web email services.
- Using Instant Messaging or Internet Relay Chat (IRC).
- Using the Internet for broadcast audio for non-business use.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using the Internet when it violates any federal, state or local law.

#### **Statement of Consequences**

Noncompliance with this policy may constitute a legal risk to the State of Tennessee, an organizational risk to the State of Tennessee in terms of potential harm to employees or citizen security, or a security risk to the State of Tennessee's Network Operations and the user community, and/or a potential personal liability. The presence of unauthorized data in the State network could lead to liability on the part of the State as well as the individuals responsible for obtaining it.

#### **Statement of Enforcement**

Noncompliance with this policy may result in the following immediate actions.

1. Written notification will be sent to the Agency Head and to designated points of contact in the User Agency's Human Resources and Information Technology Resource Offices to identify the user and the nature of the noncompliance as "cause". In the case of a vendor, subrecipient, or contractor, the contract administrator will be notified.
2. User access may be terminated immediately by the Systems Administrator, and the user may be subject to subsequent review and action as determined by the agency, department, board, or commission leadership, or contract administrator.



STATE OF TENNESSEE  
**Acceptable Use Policy**  
**Network Access Rights and Obligations**  
**User Agreement Acknowledgement**

As a user of State of Tennessee data and resources, I agree to abide by the Acceptable Use Network Access Rights and Obligations Policy and the following promises and guidelines as they relate to the policy established:

1. I will protect State confidential data, facilities and systems against unauthorized disclosure and/or use.
2. I will maintain all computer access codes in the strictest of confidence; immediately change them if I suspect their secrecy has been compromised, and will report activity that is contrary to the provisions of this agreement to my supervisor or a State-authorized Security Administrator.
3. I will be accountable for all transactions performed using my computer access codes.
4. I will not disclose any confidential information other than to persons authorized to access such information as identified by my section supervisor.
5. I agree to report to the Office for Information Resources (OIR) any suspicious network activity or security breach.

**Privacy Expectations**

The State of Tennessee actively monitors network services and resources, including, but not limited to, real time monitoring. Users should have no expectation of privacy. These communications are considered to be State property and may be examined by management for any reason including, but not limited to, security and/or employee conduct.

I acknowledge that I must adhere to this policy as a condition for receiving access to State of Tennessee data and resources.

I understand the willful violation or disregard of any of these guidelines, statute or policies may result in my loss of access and disciplinary action, up to and including termination of my employment, termination of my business relationship with the State of Tennessee, and any other appropriate legal action, including possible prosecution under the provisions of the Computer Crimes Act as cited at TCA 39-14-601 et seq., and other applicable laws.

I have read and agree to comply with the policy set forth herein.

\_\_\_\_\_  
 Type or Print Name

\_\_\_\_\_  
 Last 4 digits of Social Security Number

\_\_\_\_\_  
 Signature

\_\_\_\_\_  
 Date



STATE OF TENNESSEE  
DEPARTMENT OF REVENUE  
ANDREW JACKSON STATE OFFICE BUILDING  
NASHVILLE, TENNESSEE 37242

**BILL HASLAM**  
GOVERNOR

**DAVID GERREGANO**  
COMMISSIONER

**Confidentiality and Disclosure of Tennessee  
Motor Vehicle Title and Registration Information  
To Federal, State or Local Government Employees**

I acknowledge that my official duties involve access to Tennessee motor vehicle title and registration information. Such information may include motor vehicle titles, motor vehicle registrations, information that identifies individuals, photographs or images of individuals, social security numbers, names, addresses, telephone numbers, and medical or disability information.

I have been advised that Tennessee motor vehicle title and registration information requires special protection and may be accessed and used only in the performance of my official duties.

I have received and read the attached copies of Tennessee's Uniform Motor Vehicle Records Disclosure Act found in Tenn. Code Ann. § 55-25-101 et seq. and the Federal Drivers' Privacy Protection Act (Prohibition on Release and Use of Information from State Motor Vehicle Records) found in Title 18 U.S.C. § 2721 et seq., which pertain to the unauthorized access or disclosure of information from state motor vehicle records.

I have been advised that it is unlawful to access or disclose Tennessee motor vehicle title and registration information for any purpose not authorized as part of my official duties and that it is unlawful to disclose such information except as provided in the above referenced statutes. I have also been advised that these disclosure restrictions continue to apply even after my government employment ceases. I agree to comply with the attached Federal and Tennessee statutes described above.

I will not access or disclose any Tennessee motor vehicle title and registration information in any manner whatsoever, except to the extent, and in a manner specifically permitted by applicable laws, rules, or regulations.

I also understand that Title 18 U.S.C. §§ 2723 and 2724 state that a person who knowingly obtains, discloses or uses motor vehicle records and information for a purpose not permitted under Title 18 U.S.C. § 2721 et seq. is subject to a fine and is liable to the individual to whom the information pertains. The person whose privacy rights were violated may bring a civil action in a United States District Court and be awarded actual damages, punitive damages, reasonable attorney fees, litigation costs and other preliminary and equitable relief.

I understand that violation of any of the foregoing requirements will be grounds for my being denied further access to Tennessee motor vehicle title and registration information and also grounds for my immediate dismissal from employment. In addition, I will also be subject to the penalties outlined above.

\_\_\_\_\_  
User ID

\_\_\_\_\_  
Organization or Department

\_\_\_\_\_  
Division and Location

\_\_\_\_\_  
Name (please print)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date