STATE OF TENNESSEE

DEPARTMENT OF SAFETY AND HOMELAND SECURITY

Acceptable Use Policy
External Partner/Agency Portal
eServices Court Portal – Driver History Records Review

Purpose:
To establish guidelines for courts and other external partners to access the eServices Court Portal for the purpose of reviewing driver history records as authorized by state and federal law ("Purpose").

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.
Tennessee Code Annotated, Section 55-25-101*, et seq.,* effective July 1, 1997
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 State-authorized external partner.
- 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.
- 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.

Scope:
This Acceptable Use Policy applies to all individuals who have been provided access rights to the eServices Court Portal for the Purpose stated herein.

Use and Prohibitions:

A. Resources
External partners may be authorized to access the eServices Court Portal for the Purpose stated herein. Each State-authorized external partner shall be issued a username and password to login to the eServices Court Portal. It is understood that by signing this document, the signer agrees to abide by the terms of this Acceptable Use Policy and understands that access to the eServices Court Portal shall be terminated in the event of any misuse of the login credentials.

Prohibitions

- Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation.
- Using the eServices Court Portal for anything other than the Purpose stated herein.
- Walking away and leaving the eServices Court Portal accessible without engaging password protection.
- Allowing unauthorized persons to access the eServices Court Portal.
- Sharing login credentials, even with another State-authorized user.
- Using the eServices Court Portal for unlawful activities as defined by federal, state, and local law.
- Utilizing the eServices Court Portal for activities that violate conduct policies established by the State or the external partner agency where the user is employed.

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 data, and/or a potential personal liability.

Unauthorized access, use, misuse, or modification of the eServices Court Portal or of the data accessed via the eServices Court Portal or in transit to/from the eServices Court Portal constitutes a violation of state and federal laws including, but not limited to Title 18, United States Code, Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Title 26, United States Code, Sections 7213 (a), 7213A (the Taxpayer Browsing Protection Act), and 7431.

Monitoring and Statement of Enforcement

Use of the eServices Court Portal is subject to monitoring to ensure proper usage. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to law enforcement personnel. Use of the eServices Court Portal constitutes automatic consent to such monitoring.

Noncompliance with this Policy may result in the immediate termination of user access to the eServices Court Portal.

[INTENTIONALLY LEFT BLANK]

ACKNOWLEDGE AND SIGN ON NEXT PAGE

STATE OF TENNESSEE
DEPARTMENT OF SAFETY AND HOMELAND SECURITY

Acceptable Use Policy
External Partner/Agency Portal
eServices Court Portal – Driver History Records Review

User Agreement Acknowledgement

By signing below, I agree to abide by the Acceptable Use Policy – External Partner/Agency Portal – eServices Court Portal – Driver History Records Review and the following promises and guidelines as they relate to the Policy:

1. I will protect the login credentials issued to me for access to the eServices Court Portal against unauthorized disclosure and/or use.
2. I will maintain the login credentials issued to me 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 Policy to the State.
3. I will be accountable for all transactions performed using my login credentials.
4. I will not disclose any confidential information other than to persons authorized to access such information as identified by my section supervisor.

Monitoring and Privacy Expectations

The State actively monitors network services and resources, including, but not limited to, real time monitoring. Users should have no expectation of privacy. Use of the eServices Court Portal may be examined and monitored by the State for any reason including, but not limited to, security and/or user conduct.

I acknowledge that I must adhere to this Policy as a condition for receiving login credentials to access the eServices Court Portal.

I understand the willful violation or disregard of any of these guidelines, statute, or policies may result in my loss of access to the eServices Court Portal and termination of my business relationship with the State, 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

FEDERAL DRIVERS PROTECTION ACT (DPPA)

Effective June 1, 2000, the Federal Drivers Protection Act (DPPA) (18 U.S.C.A. 2721) as amended by Section 350 of Public Law 106-69 *Appropriations Act* prohibits the dissemination or disclosure of a photograph, social security numbers, medical or disability information from motor vehicle records without the express consent of the person to whom the information pertains. However, this information may be released even without the express consent of the person for the following reasons:

1. **For use by any government agency, including any court or law enforcement agency, in Carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.**

2. **For use in connection with any civil, criminal, administrative, or arbitral proceeding in Any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.**

3. **For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.**

4. **For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.**

Other personal information consisting of a driver's identification number, name, address, or telephone number shall not be released without the express consent of the person to whom it pertains unless the person requesting the information needs it for one of the following permitted uses.

1. **For use by any government agency, including any court or law enforcement, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State of local agency in carrying out its functions.**

2. **For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.**

3. **For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only –**

   (A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and

   (B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.

4. **For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.**

5. **For use in research activities and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.**

6. **For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.**

7. **For use in providing notice to the owners of towed or impounded vehicles.**

8. **For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.**

9. **For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.**

10. **For use in connection with the operation of private toll transportation facilities.**

11. **For any other use in response to requests for individual motor vehicle records if the motor vehicle department has provided in a clear and conspicuous manner on forms for issuance or renewal of operator's permits, titles, registrations, or identification cards, notice that personal information collected by the department may be disclosed to any business or person, and has provided in a clear and conspicuous manner on such forms an opportunity to prohibit such disclosures.**

12. **For bulk distribution for surveys, marketing or solicitations/if the motor vehicle department has implemented methods and procedures to ensure that –**

    (A) individuals are provided an opportunity, in a clear and conspicuous manner, to prohibit such uses; and

    (B) the information will be used, rented, or sold solely for bulk distribution for surveys, marketing, and solicitations, and that surveys, marketing, and solicitations will not be directed at those individuals who have requested in a timely fashion that they not be directed at them.

13. **For use by a requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.**

14. **For any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety.**

STATE OF TENNESSEE
DEPARTMENT OF SAFETY AND HOMELAND SECURITY

Federal Drivers Protection Act (DPPA) Acknowledgment

By my signature below, I acknowledge that:

- **I have read the attached Federal Drivers Protection Act (DPPA) and understand it.**
- **I agree to comply with the Federal Drivers Protection Act (DPPA)**

_____

Signature **Date**

_____

Print Name Signed Above