Tennessee Valley Authority
Privacy Impact Assessment (PIA)

Web Record Management System (WebRMS)

This PIA is a tool used by the TVA Privacy Office to identify privacy risks at the planning/initiation phase of the system development lifecycle (SDLC) or early stages of project/program development. The PIA should be reviewed and updated on an annual basis, or sooner, if the system undergoes a major change. Questions regarding this document should be directed to privacy@tva.gov.

PIA should be submitted to:
TVA Privacy Office
privacy@tva.gov

Version 3.0
September 2018

PROGRAM MANAGEMENT

Author Name

[redacted]

Date of Submission

02/19/2020

Responsible TVA Business Unit

TVA Police Emergency Management

Name of System

Web Records Management System (WebRMS)

System Owner Details

Name [redacted]

Title

Phone

Email

Reason for Completing PIA

- ○ New system
- ○ Significant modification to an existing system
- ◉ To update existing PIA for a security authorization

PRIVACY DETERMINATION

(To be completed by the TVA Privacy Program)

Privacy Office Comments

This system is up for re-authorization to update the System Owner of WebRMS. No PII/RPII changes have been made.

The signatures below certify that the information in this document has been reviewed and approved:

	Name	Signature	Date
System Owner	[redacted]		02/19/2020
Senior Privacy Program Manager	Chris Marsalis	Chris Marsalis	02/19/2020

SYSTEM OVERVIEW

1. Please describe the purpose of the system/collection:

WebRMS is a Police agency-wide system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations. RMS covers the entire life span of records development- from the initial generation to its completion.

For WebRMS, records are limited to electronic files directly related to law enforcement operations such as incident and accident reports, arrests, citations, warrants, case management, field contacts, etc.

2. About whom does the system collect, maintain, use and/or disseminate information? Check all that apply:

☒ TVA employees ☒ TVA contractor ☒ Members of the public

3. Is the information collected directly from the individual?

◉ Yes ○ No

4. What type of personally identifiable information (PII) can be/is collected, maintained, used, and/or disseminated? Check all that apply: (Per the Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.)

☒ Home Phone	☐ Financial Information	☐ Biometric Information
☒ Home Address	☐ Clearance Information	☐ Citizenship
☐ Home Email	☐ Mother's Maiden Name	☐ Driver's License Number
☐ Employment Information	☒ Date of Birth	☐ Username/Password
☐ Work Address	☐ Place of Birth	☐ Passport Number
☐ Work Phone	☐ Criminal History	☐ Other:
☐ Work Email	☒ Social Security number (SSN)	
☒ Name	☐ Medical or Health Information	

If none of the above data elements are checked, stop and submit this PTA as-is to TVA Privacy Office at privacy@tva.gov. Otherwise, please continue completing the remaining questions in the document.

Privacy Notice and Transparency

5. Legal authority to collect, use, maintain, and share data in the system:

TVA Act of 1933, 16 U.S.C. 831-ee; 5 U.S.C. 552a; and 28 U.S.C. 534.

6. Does the system have a SORN? (If PII in the system is retrieved using one or more of the identifiers listed in Question 4, a System of Records Notice (SORN) is required.)

◉ Yes ○ No

List name(s) of applicable SORN(s): *TVA-37- U.S. TVA Security Records*

7. How are individuals notified as to how their information will be collected, maintained, used, and/or disseminated within this system?

Individuals are not notified.

8. What consent options do individuals have regarding specific uses or sharing of their information?

There are no consent options.

DATA MINIMIZATION

9. Are only the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose collected, used and retained?

(•) Yes ( ) No

10. What are the retention periods for the information in the system?

7 years- Adminstration piece, status reports, program activities
25 years- Case Management

DATA QUALITY

11. How is data quality (i.e., accuracy, relevance, timeliness, and completeness) ensured throughout the data lifecycle and business processes associated with the use of the information? Check all that apply.

☐ Information is collected directly from individuals (preferred method of collection, whenever possible)
If collected via a form, please list form(s) name and number here:

☐ Cross referencing information enties with other systems ☐ Third party information verification

☐ Character limits on text submissions ☐ Numerical restrictions in text boxes

☒ Other: *N/A*

12. How is inaccurate or outdated information checked for and corrected?

Manager and Senior Manager audit entries.

Access and Redress

13. How can an individual access their information and have it corrected, amended, or deleted?

Subject to the limitations of the Privacy Act, individuals may request access to information about themselves contained in a TVA system of records through TVA's Privacy Act/Freedom of Information Act (FOIA) Procedures.

Internal and External Sharing

14. Explain how the information in the system is limited to the uses specified in the notices discussed above.

The information in this system is limited to the designated Administrators.

15. With which (if any) internal TVA systems is the information shared?

PSIM IPSecurity

16. With which (if any) organizations external to TVA is information shared?

None.

17. Does the system have any associated websites/applications including an external TVA website or third-party owned or managed website or application (e.g., Facebook, YouTube, Twitter, Flicker, etc.)?

○ Yes ◉ No

SECURITY

18. What privacy orientation or training is provided to authorized users of the system or individuals with access to the system?

[redacted]

19. Has a FIPS 199 determination been made?

[redacted]

20. What is the FIPS 199 determination? Check one for each.

[redacted]

21. What types of technical safeguards are in place to protect the information?

[redacted]

22. What types of physical safeguards exist to protect the information?

[redacted]

23. What types of administrative safeguards exist to protect the information?

[redacted]

24. What monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate usage?

All monitoring, recording, and auditing safeguards are in place by TVA Cybersecurity.

25. Discuss any other potential privacy risks to the information within the system and safeguards that are in place to mitigate those risks.

None.

Please submit completed form to: **TVA Privacy Office**
privacy@tva.gov