Tennessee Valley Authority
Privacy Impact Assessment (PIA)

TVA Account Portal (TAP)

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 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 09/15/2025

Responsible TVA Business Unit T&I

Name of System TVA Account Portal (TAP)

System Owner Details

Name [redacted]

Title [redacted]

Phone [redacted]

Email [redacted]

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

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

	Name	Signature	Date
System Owner	[redacted]	[redacted]	[redacted]
Senior Privacy Program Manager	Chris Marsalis	Chris Marsalis (E-Signature)	09/16/2025

SYSTEM OVERVIEW

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

This will be a vendor developed software inside the BTP tool designed to facilitate the payment of TVA invoices by external customers (LPCs, Direct Served Customers, & non-power customers). It will replace 2 homegrown applications and will reside in the cloud with the S4/Hana application and feed data directly to it.

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 How is the information collected? *Customers provide their banking information, S4 provides the billing information.*

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)	*Invoice information for their billing information.*
☒ 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.

Number of people impacted?

○ 1 - 999 ○ 1,000 - 4,999 ◉ 5,000 - 19,999 ○ 20,000 - 99,999 ○ 100,000 or more

Privacy Notice and Transparency

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

Tennessee Valley Authority Act of 1933, 16 U.S.C. 831-831ee; Executive Order 10577; Executive Order 10450; Executive Order 11478; Executive Order 11222; Equal Employment Opportunity Act of 1972, Public Law 92-261, 86 Stat. 103; Veterans' Preference Act of 1944, 58 Stat. 387, as amended; various sections of title 5 of the United States Code related to employment by TVA.

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-2-Personnel Files*

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

PIA's, SORN's, Privacy Act Statement

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

There is a mandatory consent box when they enable their payment information regarding specific uses or sharing of their information.

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?

1 year for messages. Other data is not maintained in TAP - it is maintained in S/4 but viewable in TAP.

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:

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

The customer would be notified that their information is inaccurate and they would be responsible to correct it.

Access and Redress

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

The customer would be notified that their information is inaccurate and they would be responsible to correct it.

Internal and External Sharing

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

The system is limited to the users and admins of the system.

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

[redacted]

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

Please describe and provide link: *TAP.TVA.GOV*

i. Does the website or application allow individuals to submit comments, feedback or messages?

(●) Yes
( ) Yes, but the feature will be turned off
( ) No

ii. Does the website or application allow individuals to submit comments, feedback or messages?

( ) Yes, but TVA does not have access to any system information.
( ) Yes, TVA has access to the collected information, but only single-session technologies are used.
(●) Yes, TVA has access to the collected information, and multi-session technologies are used.
( ) 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