

West Virginia Executive Branch
**Privacy Impact Assessment (PIA)
Instructions**



FILING INFORMATION

After completing the PIA, submit a fillable copy by e-mail to the following:

- Lori Tarr - Assistant Chief Privacy Officer, State Privacy Office lori.l.tarr@wv.gov
- Mary Ann Escarda - Administrative Assistant, State Privacy Office maryann.escarda@wv.gov
- Cyber Security Office, WV Office of Technology cso@wv.gov
- Procurement Officer
- Department Privacy Officer
- Security Officer (when applicable)
- Agency Privacy Officer (when applicable)

Once the PIA is received by the State Privacy Office, an email acknowledging its receipt will be sent to the submitter and designated contact staff, along with additional information about the review process, and a newly assigned subject line. This subject line should be used in all future emails.

PIA INFORMATION

- The PIA consists of seven sections.
 1. General Information
 2. Privacy Threshold Analysis
 3. Data Classification
 4. Data Collection, Use and Storage
 5. Data Disclosure (Sharing)
 6. Administrative, Physical and Technical Controls
 7. Appendix A of the Software as a Service (SaaS) Addendum
- First complete Sections 1. General Information, and 2. Privacy Threshold Analysis (PTA). If you do not need to complete Sections 3-7, certify the (PTA) at question 31, and submit per instructions above.
- **Save your work on a regular basis. Links may take you out of the document.**
- Look for the action items. These are tips that may be revealed, depending on the answer, that will point to relevant privacy and security policies. For your convenience, links to privacy and security policies, are provided here:
 - State Privacy Policies (SPO): [Privacy Policies](#)
 - Office of Technology Policies (WVOT): [Security Policies](#)

1. GENERAL INFORMATION

Contact Information: Please provide the names of the departmental and agency privacy officers, the procurement officer and other individuals involved in this project. Below is a link to lists of privacy officers and procurement officers.

Departmental and Agency Privacy Officers: [Privacy Officer Contact List](#)

Procurement Officer: [Procurement Officer List](#)

Privacy Impact Assessment (PIA)

Instructions

1. GENERAL INFORMATION (CONTINUED)

Removable Media - Questions 1, 4 -7: In Question 1, fully describe the purpose for which the removable media will be used. If the removable media is for an external hard drive for data storage, explain why alternative storage is not appropriate.

Confirm in Question 4 if this PIA is for the purchase of removable media.

See the following definitions for removable media types for Question 5:

- **Memory Cards include:** CF cards, SD cards
- **External Hard Drives:** HDD, SDD
- **Optical Discs:** CDs, DVDs, Blu-ray discs
- **USB Flash Drives:** thumb drives, jump drives, key drives

2. PRIVACY THRESHOLD ANALYSIS

Section 2 is the Privacy Threshold Analysis. The information supplied on this page determines if the rest of the file needs to be completed. If there is no Personally Identifiable Information (PII) that will be collected, used, maintained or disclosed by this project or purchase then answer Question 8, certify the PTA in Question 31 and submit as instructed.

3. DATA CLASSIFICATION

- **Data Classification - Question 11:** Select the highest level of data classification for the data associated with this project or purchase. There are three classifications: Public, Sensitive and Restricted. Restricted data is the highest level and requires the greatest amount of controls for safeguarding collection, access, usage and disclosure. Data classifications are important and must reflect the sensitivity of the data collected. A link is provided to review the classifications per policy.
- **Data Classification - Question 11 and 12:** If the answer to Question 11 is Sensitive or Restricted, answer "No" to Question 12 and skip Questions 13-16 and proceed to Section 4.
- **Software-as-a-Service Addendum, Appendix A - Questions 12-16:** These questions relate to projects with a third-party vendor hosting applications in the cloud through internet access. The input for questions 13-16 are linked to Section 7 (Appendix A of the SaaS Addendum). This document is required for all SaaS projects that will process non-public information. All non-public data is defined, and referenced, as restricted data in the SaaS Addendum.

West Virginia Executive Branch
Privacy Impact Assessment (PIA)

4. DATA COLLECTION, USE AND STORAGE

- Questions 12 & 13: These relate to the legal authority for the project. It is important to know the legal basis and parameters for collecting, using, maintaining and disclosing PII in order to adhere to the Minimum Necessary and Limited Use Policy (No. WVEB-P104).

5. DATA DISCLOSURE (SHARING)

- Question 21: Per Policy No. WVEB-P106, transmission of Sensitive Personal Information must only be transmitted using secured and/or encrypted methods of transmission approved by the Cyber Security Office.
- Question 23: For projects with vendors that collect PII, PHI (covered under HIPAA) or host applications in the Cloud, please pay close attention to this question and the footnotes.

6. ADMINISTRATIVE, PHYSICAL AND TECHNICAL CONTROLS

- Question 31: If there is concern that additional risk mitigation is needed for this project, you should review it with your Privacy and/or Security Officers to determine what additional actions should be taken. The Cyber Security Office may also be of assistance.
- Question 33: Asks you to confirm you are ready to finalize the PIA and that the information provided is true, correct and complete to the best of your knowledge and belief.

7. APPENDIX A OF THE SOFTWARE AS A SERVICE ADDENDUM

- Section 7 relates to projects that involve a vendor that will host applications in the cloud, which requires the Software as a Service Addendum (SaaS) to be included in the contract. Section 7., Appendix A, provides the output for Questions 1 - 6 of Appendix A of the SaaS Addendum. Questions 1 - 4 are completed automatically, with links to information provided in Section 3 - Data Classification. This page should be provided to the procurement officer involved in the contract process.

West Virginia Executive Branch
Privacy Impact Assessment (PIA)

Section 1: General Information

PROJECT CONTACT INFORMATION

Name: Email:

Role/Title:

Project Manager (if applicable):

PROJECT INFORMATION

Department (cabinet level):

Division, Bureau, Office or Agency:

Project Name:

Project Start Date (mm/dd/yy):

WV Office of Technology Number:
(if available)

OFFICER CONTACTS

Privacy Officer - Department:

Privacy Officer - Agency:

Security Officer - Department:

Procurement Officer:

Procurement Officer List: [Procurement Officer List](#)

1. Purchase or Project Description (e.g. to track direct hire benefits; to process financial transactions; provide project specific reports. If this is for the purchase of removable please carefully, read instructions on page 2.

West Virginia Executive Branch
Privacy Impact Assessment (PIA)

2. Project Designation: Identify the designation of this project/system. (Select only one from the dropdown menu: Major Application, Minor Application, General Support System, Purchase of Removable Media, Other)

Specify Other here:

3. If the answer to Question 2 is "Major Application" provide the type of major application. (Select only one from the dropdown menu: New Information System, Existing Information System, Significantly Modified System, New Electronic Collection of Information, Existing Electronic Collection)

4. Is this a purchase of removable storage media?

If not, proceed to question 8.

5. What type of removable storage media?

6. Will the removable media be used for long-term data storage?

7. Will the removable media be password protected and encrypted?

Section 2: Privacy Threshold Analysis

8. Is Personally Identifiable Information (PII) being collected, used, maintained or disclosed with this purchase or project?

NOTES:

- DEFINITION: PII is all information that identifies, or can be used to identify, locate, or contact an individual. See Question 10 below for list of PII types. This list is not exhaustive.
- Only answer "No" if this project or purchase will not have any data privacy issues.
- **If the answer to Question 8 is "No" then STOP. Do not complete Questions 6 – 30. Certify Question 31 and submit as directed.**

9. Does the collection of this information require a Privacy Notice Statement? (Select answer from dropdown box.)

West Virginia Executive Branch
Privacy Impact Assessment (PIA)

10. What PII will be collected, used maintained or disclosed? (Checkmark all that apply.)

<input type="checkbox"/>	Biometric Identifier (facial recognition, fingerprint, voiceprint, retinal scan)
<input type="checkbox"/>	Certificate / License Number (Non-Driver's License Numbers)
<input type="checkbox"/>	Child Information
<input type="checkbox"/>	Citizenship
<input type="checkbox"/>	Consumer Reporting Agency
<input type="checkbox"/>	Criminal Information
<input type="checkbox"/>	Date of Birth
<input type="checkbox"/>	Disability Information
<input type="checkbox"/>	Driver's License Numbers
<input type="checkbox"/>	Education Information
<input type="checkbox"/>	Employment Information (Name, Address, Phone, Fax, IP Address, Email)
<input type="checkbox"/>	Emergency Contact
<input type="checkbox"/>	Financial Account Information (Checking, Savings, PINs, Credit or Debit Card Numbers)
<input type="checkbox"/>	First and Last Name
<input type="checkbox"/>	Gender
<input type="checkbox"/>	Health Information (HIPAA Covered)
<input type="checkbox"/>	Health Information (Non-HIPAA Covered)
<input type="checkbox"/>	Home Street Address
<input type="checkbox"/>	Individual Taxpayer Identification Number
<input type="checkbox"/>	Law Enforcement
<input type="checkbox"/>	Legal Documents
<input type="checkbox"/>	Maiden Name (Individual)
<input type="checkbox"/>	Maiden Name (Mother's)
<input type="checkbox"/>	Marital Status
<input type="checkbox"/>	Other ID Number
<input type="checkbox"/>	Other Names
<input type="checkbox"/>	Passport Number
<input type="checkbox"/>	Payment Card Information (Debit / Credit Card)
<input type="checkbox"/>	Personal Email Address
<input type="checkbox"/>	Personal Fax Number
<input type="checkbox"/>	Personal Internet Protocol (IP) Address
<input type="checkbox"/>	Phone - Home
<input type="checkbox"/>	Phone - Mobile (Personal only)
<input type="checkbox"/>	Place of Birth
<input type="checkbox"/>	Race / Ethnicity
<input type="checkbox"/>	Social Security Number (Full)
<input type="checkbox"/>	Social Security Number (Last 4 digits)
<input type="checkbox"/>	Spouse Information
<input type="checkbox"/>	Student Identification Card Number
<input type="checkbox"/>	Tax Information (Federal)
<input type="checkbox"/>	Tax Information (State)
<input type="checkbox"/>	Vehicle Identification Number (including license plate)
<input type="checkbox"/>	Visual Media (Photograph or Video)
<input type="checkbox"/>	Other-Describe here: <input style="width: 150px; height: 15px;" type="text"/>

West Virginia Executive Branch
Privacy Impact Assessment (PIA)

Section 3: Data Classification

11. What is the highest data classification level of the PII related to this project or purchase? If uncertain, see WVOT Data Classification Policy No. PO1006.

12. Will restricted or sensitive data be processed by a vendor, also known as a service provider?

13. Does the restricted information include personal information, such as

- First name, or first initial, and last name; linked with,
 - Government issued identification numbers (e.g. SSN, Driver's License, State ID); or
 - Financial account information, including account number with access code?
- Protected Health Information (PHI)?
- Payment Card Information (PCI) (e.g. credit or debit card data)?

14. Does the restricted information include non-public data, such as state information protected by law, data not subject to FOIA requests or trademarks?

15. Will your agency allow the service provider to store its data in another country outside the U.S. that has privacy laws that are equally strong or stronger?

NOTE: Section 7. Appendix A, provides you with information for Questions 1 - 5 of the Procurement Officer's Report for Appendix A of the Software as a Service Addendum.

West Virginia Executive Branch
Privacy Impact Assessment (PIA)

Section 4: Data Collection, Use & Storage

16. Do you have legal authority to collect this information?
 (Select answer from dropdown box.)

17. What of the following provides you with legal authority to collect this information?
 (Check all that apply.)

	Affordable Care Act
	Children's Online Privacy Protection Act
	Drivers Privacy Protection Act
	Fair Credit Reporting Act
	Family Education Rights and Privacy Act
	Freedom of Information Act (FOIA)
	Gramm-Leach-Bliley Act
	Health Information Technology for Economic and Clinical Health Act (HITECH)
	Health Insurance Portability and Accountability Act of 1996 (HIPAA)
	Maxwell Governmental Access to Financial Records Act
	Omnibus Reconciliation Act of 1990
	Privacy Act of 1974
	Records Management and Preservation of Essential Records Act
	Tax Reform Act of 1976
	Uniform Electronic Transactions Act
	Uniform Motor Vehicle Records Disclosure Act
	Federal Law
	<u>Enter Federal law common name, or legal citation here:</u>
	State Law
	<u>Enter State law common name, or legal citation here:</u>
	Other - Describe here: <input style="width: 500px; height: 20px;" type="text"/>

18. Which of the following describes how the information will be stored at the point of collection?
 (Select only one from the dropdown menu: Electronic only, Combination of electronic / paper, paper only.)

West Virginia Executive Branch
Privacy Impact Assessment (PIA)

19. From whom is the information being collected? (Check all that apply.)

<input type="checkbox"/>	Citizens (including minors)
<input type="checkbox"/>	Employees / Contractors
<input type="checkbox"/>	Websites
<input type="checkbox"/>	Other Sources

20. Where will the information be stored? (Check all that apply.)

<input type="checkbox"/>	On-site, locally (within physical location of the owning department/agency)
<input type="checkbox"/>	Office of Technology Data Center
<input type="checkbox"/>	Third-Party Data Center (vendor data center/storage location, cloud)
<input type="checkbox"/>	Identify vendor, data location here:
<input type="checkbox"/>	Other (please identify)
<input type="checkbox"/>	Identify other location here:

Section 5: Data Disclosure (Sharing)

21. How will the information be transmitted?

(Select only one from the dropdown menu: Electronic only, Combination of electronic/paper, Paper only or Other.)

22. Will the information be secured (i.e. encrypted) in transit?

(Select answer from dropdown box.)

23. With whom will the information be shared? (Check all that apply.)

<input type="checkbox"/>	Within the organization
<input type="checkbox"/>	Other State Agencies
<input type="checkbox"/>	Federal Government Agencies
<input type="checkbox"/>	Local Government Agencies
<input type="checkbox"/>	Contractors
<input type="checkbox"/>	Citizens
<input type="checkbox"/>	Other
<input type="checkbox"/>	N/A

West Virginia Executive Branch
Privacy Impact Assessment (PIA)

24. If your project involves a vendor, which agreements are needed? (Check all that apply.)

	Memorandum of Understanding
	Vendor Contract
	Privacy, Security and Confidentiality Contract Term ¹
	Business Associate Addendum ²
	Software as a Service Addendum ³
	Other
	N/A

1. For use when the vendor will process your Personally Identifiable Information (PII). This term is located in the Agency and Purchasing Master Terms and Conditions.
2. For use when your agency is a HIPAA covered entity, or business associate, and the vendor will process your Protected Health Information (PHI).
3. For use when the vendor will host applications in the cloud that are accessed using the internet.

25. Are there procedures or policies in place that give individuals the opportunity, ability or right to:

	Decline providing information?
	Gain access to their own information to verify accuracy?
	Update or correct their PII?
	N/A

Section 6: Administrative, Physical and Technical Controls

26. Are there controls in place to ensure that access to PII is restricted to only those individuals who need the PII to perform their official duties?
 (Select answer from dropdown box.)

27. Are there controls in place to ensure files are backed up?
 (Select answer from dropdown box.)

28. What controls are in place to ensure files are backed up?

West Virginia Executive Branch
Privacy Impact Assessment (PIA)

29. Are there physical controls in place to ensure the files are secure?
(Select answer from dropdown box)

30. Which of the following physical controls are in place?

<input type="checkbox"/>	Biometrics
<input type="checkbox"/>	Cipher Door Locks
<input type="checkbox"/>	Door Keys
<input type="checkbox"/>	Security Guards
<input type="checkbox"/>	Identification Badges
<input type="checkbox"/>	Key Cards
<input type="checkbox"/>	Locked Cabinet
<input type="checkbox"/>	Security Camera
<input type="checkbox"/>	Other
<input type="checkbox"/>	Specify other here:

31. Is there an incident response plan in place?

32. Is additional risk mitigation needed?

33. Is there a data retention policy in place for this data?

34. If there is any additional information you would like to provide, please do so here?

35. If you are ready to submit your finalized PIA (or PTA), certify the following: Do you certify that the information contained in this document is true, correct and complete to the best of your knowledge and belief?

West Virginia Executive Branch
Privacy Impact Assessment (PIA)

NOTE: This Appendix is only for projects that require the Software-as-a-Service Addendum.

**Section 7: Procurement Officer Report
for
Appendix A of the Software as a Service Addendum**

Agency/public jurisdiction's required information - Questions 1 - 6

1. Will restricted information be processed by the service provider?

2. If yes to #1, does the restricted information include personal data?

3. If yes to #1, does the restricted information include non-public data?

4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?

5. Provide the name and email address of the Department Privacy Officer.

Name:

Email:

6. Provide the name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact (if available):

Name:

Email:

Phone: