POST INCIDENT RESPONSE ASSESSMENT (EVENT)

This report must be provided to the parties listed in Section 4 within 30 calendar days of filing the initial Incident Report.

The Privacy Incident Response Assessment (PIRA) contains pre-decisional, confidential information, including internal risk assessments, and constitutes internal memoranda exempt from the Freedom of Information Act, W. Va. Code 29-B-1 et seq. The PIRA and the information contained herein shall only be disclosed to the extent necessary in the deliberative process or as required by law.

SECTION 1 – INCIDENT REPORT INFORMATION

SPO Tracking Number**:**

Date of initial incident report:

Department:

Bureau/Division:

Agency/Office:

Name (of person who reported the incident):

Phone Number:

Email:

Department Privacy Officer:

Agency Privacy Officer (if applicable):

1.1 How was incident reported?

□ Office of Technology Online Security & Privacy Incident Reporting System

□ Other (Please specify below):

1.2 Was this incident reported to law enforcement?

If yes, attach a copy of the report. If the report is not available, identify the law enforcement agencies to which a report was made. (Mark all that apply.) ○ Yes ○ No

□	Local (Municipal or County)	Enter date of report here:	
□	State Police	Enter date of report here:	
□	Federal	Enter date of report here:	

Provide the ID number of report, identify the law enforcement agency below.

SECTION 2 – INCIDENT INFORMATION

2.1 Date incident occurred or began:

2.2 Date incident ended (if applicable):

2.3 Date range for incident if specific dates are unknown:

2.4 Date incident was detected:

2.5 Physical location of incident:

2.6 How was the incident or suspected incident discovered?

2.7 If a privacy complaint was filed by an individual who alleges their PII was inappropriately accessed or disclosed, did the complainant receive a response from the department?

○	N/A (No privacy complaint was made)
○	Yes
○	No (Please explain):

⚠ Attention: Event Classification or Incident Withdraw Determination

Events do not involve an unauthorized disclosure of PII, nor a possibility of an unauthorized disclosure, and must be documented below in Questions 2.8 - 2.10.

Question 2.11 is used to withdraw an incident. All withdraws must receive prior approval in writing from the State Privacy Office.

Event Classification - Answer Questions 2.8 – 2.10.

2.8 Encryption status:

1. Does this incident involve an email that was sent *unencrypted* outside of the wv.gov network, or otherwise against to policy?	-Select-
2. **Non-HIPAA only:** Was the data containing Personally Identifiable Information (PII) encrypted[1], rendering the data elements unusable, unreadable or indecipherable?	-Select-
3. **HIPAA only:** Was the data containing Protected Health Information (PHI) encrypted per NIST standards or an encryption process equally effective to the NIST standard?[1,2]	-Select-

Notes:

- [1]Encrypted, in this context, means there is a low probability of assigning meaning without the use of a confidential process or key, and that process or key is not available to any unauthorized person in possession of the PII
- [2] To determine if the encryption meets the NIST standards, (*See,* https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html).

2.9 Classification determination when encryption is not a relevant to the incident:

1. Was PII accessible by an unauthorized individual?	-Select-
2. Was PII disclosed to an unauthorized individual?	-Select-
3. Was PII used, modified, or destroyed in an unauthorized manner?	-Select-

If the answer to *each* of the questions in 2.9 is “No”, this incident *could* be classified as an event; however, the incident must also be fully resolved.

2.10 For incidents where encryption status is not a factor, describe the following:

1. Circumstances, including other controls, that kept the data containing PII from unauthorized access, disclosure or use (e.g. returned fully sealed, never unopened envelope; pseudonymization); and
2. How the incident was fully resolved.

2.11 Withdraw Documentation: Have you received approval to withdraw this incident from the State Privacy Office? If so, click the "Yes" box, select the appropriate reason for the withdraw, and describe fully in the text box below. □ Yes

○	1. The individual whose PII was involved is responsible for causing the incident.
○	2. An external organization outside the State of West Virginia is responsible for the incident[1]
○	3. The reported incident was determined not to be privacy or security related, or was otherwise errantly reported.[2]
○	4. The reported incident only involved publicly available business information, such as disclosure of a FEIN, with no unauthorized disclosure of any PII?
○	5. Other

Notes:

- Incidents that are **not** eligible for withdraw include:
  - Vendors or third-parties, where there is the possibility of a contractual or legal responsibility for the incident to the State; or
  - Any educational organization, whether it is a county board of education or institution of higher education, and is covered by cyber-insurance through BRIM.
- [1]An example would be having a non-SOWV entity disclosing unrequested PII to an unauthorized state workforce member.

- [2] Examples include requests for technical help that should have been submitted to the service desk, power or phone outages that have no security or privacy implications, or phishing attempts that should have been reported to otphishing@wv.gov.
- A description of the circumstances that support the reason for the withdraw of the incident ***must be*** provided in the text box below.

Describe the circumstances that support withdraw here:

SECTION 3 – INCIDENT OUTCOME

3.1 What measures have been, or will be, implemented to prevent this type of incident from reoccurring? (Mark all that apply):

□ Additional Training
□ Departmental Policy or Procedure Change – Security
□ Departmental Policy or Procedure Change – Privacy
□ System Change
□ Improved Monitoring
□ Physical Security Change
□ Other (Please specify):

3.2 Has the Departmental Privacy Officer determined that the incident is fully resolved, and either qualifies as an event, or to be withdrawn? If yes, check box, initial, read instructions.

Yes □ **DPO Initials: ________________**

SECTION 4 – Filing Instructions for PIRA Submissions

1. PIRA must be kept in fillable pdf format.
2. Submit by email according to the following:
   a. Subject line format**: PIRA for Incident <insert SPO#>**
   b. Send to:
      i. State Privacy Office
         1. david.c.dyer@wv.gov
         2. maryann.escarda@wv.gov
         3. chad.a.bodmer@wv.gov
      ii. WVOT Cyber Security Office – cso@wv.gov
      iii. Cabinet Secretary
      iv. Others as applicable
3. If you are submitting a draft for pre-submission review, please add **"Draft"** to the beginning of the subject line.