INCIDENT RESPONSE CHECKLIST

For your internal use only. Do not include this when filing the Post Incident Response Assessment.

Privacy Incident Management Action Steps:

STEP1: Report incident (if not already reported) through the WVOT Online Computer Security and Privacy Incident Reporting System (Incident Report Portal), which is found:

a. WVOT > https://appengine.egov.com/apps/wv/ot/ir
b. State Privacy Office > https://privacy.wv.gov/incidentresponse/Pages/default.aspx (along with additional information on incident response)

NOTE: The report is sent to the Cybersecurity Office (CSO) at WVOT, the State Privacy Office (SPO) and Board of Risk and Insurance Management (BRIM). If the incident report reveals that the Unauthorized Disclosure is most likely a breach that will involve cyber insurance, someone at the SPO or CSO will initiate a conference call with the departmental privacy officer.

Responsible Individual(s):	
Date Completed:	

Notes:

STEP 2: Review initial report (if not already received). Note the following:

- When did it happen?
- How was it discovered?
- Who discovered it?
- Who reported it?
- To whom was it reported?
- What device was stolen/lost?
- What data was stolen/lost?
- What systems are affected?
- What organizations are affected?
- Was data encrypted?
- Has data loss been stopped?

Responsible Individual(s):	
Date Completed:	

Notes:

STEP 3: Notify department/agency leaders (if appropriate). Note: It may be helpful to pre-determine, with leadership, which type of incident that leaders are notified of. For example, cabinet secretaries certainly are not interested in being notified of a lost cell phone. However, if the incident involves a cyber attack on the operations, they should be notified immediately.

Responsible Individual(s):	
Date Completed:	

INCIDENT RESPONSE CHECKLIST

Notes:

STEP 4: For an unauthorized disclosure that involves an IT system, contact appropriate IT personnel to:

- Close security gaps;
- Isolate affected systems;
- Terminate any processes that expose PII;
- Other Issues identified? If so, identify and assign an individual the responsibility to resolve.

****IMPORTANT NOTE**: Care must be taken not to destroy forensic evidence. If there are any questions about this, please contact the CSO: Phone: 304-957-8107 or 304-558-9966; email CSO@wv.gov

Responsible Individual(s):	
Date Completed:	

Notes:

STEP 5: Activate your Department Incident Response Team (IRT). This may also involve external members.

Responsible Individual(s):	
Date Completed:	

Notes:

STEP 6: If the incident is a result of criminal activity notify law enforcement or confirm that law enforcement has been notified.

Responsible Individual(s):	
Date Completed:	
Law Enforcement Agency:	
Contact Name:	
Report Number:	

INCIDENT RESPONSE CHECKLIST

Notes:

STEP 7: Investigate Incident:

Document everything (suggested questions and information to obtain):

- Determine who needs to be interviewed
- Identify the unauthorized recipients
- What did the unauthorized recipients do with the PII?
- Confirm the types of PII disclosed?
- How did the incident happen?
- What has been done to stop further disclosure?
- Determine data governing regulations, policy.
- Determine if sensitive non-PII was disclosed. (e.g. Benefits received, health, financial and employment status, etc.)
- Determine individuals affected, and place of residence
- Determine impact on other organizations.
- Determine impact on other systems.

Responsible Individual(s):			
Date Completed:			
Individual(s) Interviewed:		Date:	
Individual(s) Interviewed:		Date:	
Individual(s) Interviewed:		Date:	

Notes:

INCIDENT RESPONSE CHECKLIST

STEP 8: **Incident Mitigation -** Secure the disclosed PII:

- Request the data be returned (hard copy) or picked up by authorized individual if appropriate.
- Request the data be destroyed thoroughly if it is not appropriate to have it returned. Provide guidance regarding shredding and other methods.
- Request the data be thoroughly deleted (electronic) including in trash and delete boxes.
- Obtain an agreement of destruction, non-disclosure, and use.
    - Should be signed affidavit(s) from unauthorized recipient(s) that data was destroyed, deleted, not further disclosed, will not be disclosed in the future, and/or will not be used for personal gain or malicious purposes.
    - Consider if the affidavit should be witnessed or notarized. This may depend on regulations, internal policies, and circumstances of the incident.
- In the case of a cybersecurity incident, work with IT personnel, leadership, WVOT, BRIM/SPO, and the state breach coach to determine forensic and remediation requirements.

Responsible Individual(s):	
Date Completed:	

Notes:

STEP 9: **Determine risk and notification requirements –**

- Does the incident include Payment Card Information (PCI)? Confirm compliance with PCI-DSS (Data Security Standards). Notify financial institutions as required by PCI-DSS, and notify BRIM.
- Does the incident include Federal Tax Information (FTI)? Comply with notification requirements by the IRS. NOTE: FTI has a specific definition by the IRS. See: https://www.irs.gov/privacy-disclosure/safeguarding-federal-tax-information-fti-in-aca-printed-notices
- Does the incident include HIPAA covered Protected Health Information? If PHI is exposed, then compliance with both HIPAA and W. Va. Code § 46A-2A-101 is required.
- Complete the Risk Assessment in Section 3 of the Post Incident Response Assessment (PIRA).
- Unless otherwise regulated by law, **prior to notifying affected individual(s) of an unauthorized disclosure, a determination must be made in conjunction with the SPO, BRIM and the state breach coach, as to the appropriateness of a notification.** **This includes notification requirements covered by the HIPAA and HITECH Acts.**

Responsible Individual(s):	
Date Completed:	

INCIDENT RESPONSE CHECKLIST

Notes:

STEP 10: Notification Processes –

- Prepare a list of affected individuals, including:
  - Addresses
  - Number of adults and minors
- Work with the breach coach to:
  - Draft the notification letter (this should be approved by leadership)
  - Print and mail notification letters (if sent using internal resources)
  - Determine communication plan. This may include:
    - Communications with departmental or agency workforce members
    - Communications with state leadership
    - Communications with media
      - Standby statements
      - Designated individuals for press statements
      - Media training
    - FAQs to support the communication plan
    - Communications with notified/affected individuals. This may include:
      - Call center
      - Call tracking reports
      - Follow-up
      - Updated FAQs.

Responsible Individual(s):	
Date Completed:	

Notes:

INCIDENT RESPONSE CHECKLIST

STEP 11: Incident Wrap-up and Closure –

- Conduct a post-incident review and analysis to determine what steps can be taken to prevent a reoccurrence. This may include:
  - Improved physical and technical controls
  - Revised policies and procedures
  - Additional training
- Document and distribute analysis of the underlying incident and the response to your IRT, if appropriate.
- Complete the Post Incident Response Assessment (PIRA). This is due within 30 calendar days of the incident report, unless additional time is required for complex investigations, forensic reviews or remediation.
- Submit the completed PIRA per instructions SPO, CISO, BRIM and your Department Cabinet Secretary.
- Save important incident documents, such as incident reports, investigation notes and the PIRA in a secure location. Keep for six years.

Responsible Individual(s):	
Date Completed:	

Notes: