INCIDENT RESPONSE EVENT CHECKLIST

INCIDENT MANAGEMENT ACTION STEPS	RESPONSIBLE INDIVIDUAL(S)	STATUS	DATE OF COMPLETION
1. Has the incident been reported through WV Office of Technology (WVOT) website? If no, you must file incident at: https://apps.wv.gov/ot/ir/Default.aspx. Additional information can be found at: http://www.privacy.wv.gov/incidentresponse **NOTE:** Along with the WVOT, the State Privacy Office (SPO) and Board of Risk and Insurance Management (BRIM) simultaneously receive notification of the incident. If the incident report reveals that the Unauthorized Disclosure is most likely a breach that will involve cyber insurance, BRIM will initiate a conference call with the DPO/APO, SPO and WVOT.			
2. Review initial report: ○ When did it happen ○ Who discovered it ○ Who reported it ○ To whom was it reported ○ What was stolen or compromised ○ Was data encrypted ○ What systems affected ○ What devices/data are missing ○ Has data loss been stopped			
3. Notify Department leaders.			
4. For any Unauthorized Disclosure that involves IT systems, 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 individual responsible to resolve.			

INCIDENT RESPONSE EVENT CHECKLIST

INCIDENT MANAGEMENT ACTION STEPS	RESPONSIBLE INDIVIDUAL(S)	STATUS	DATE OF COMPLETION
5. Activate your Department Incident Response Team (IRT). This may also involve external members.			
6. If the incident is a result of criminal activity notify law enforcement or confirm that law enforcement has been notified.			
7. Investigate Incident ○ Interview and document ○ Who else knows about it ○ Inventory disclosed elements ○ Determine individuals affected, and place of residence ○ Potential impact on other organizations ○ Potential impact to other systems			
8. Recover Data Elements Disclosed ○ Request that recipient of disclosed SPI either return (if hard copy) or delete (if electronic copy) ○ Request that recipient not share the information with anyone else ○ If already shared w/others, obtain a list of those individuals ○ Request that those individuals either return (if hard copy) or delete (if electronic copy) ○ Obtain a signed, legal binding document from all of the recipients noting they will not disclose the documents or use the SPI maliciously or for personal gain.			
9. If Payment Card Industry (PCI) data is exposed, notify appropriate financial institutions in accordance with PCI Data Security Standards (DSS).			

INCIDENT RESPONSE EVENT CHECKLIST

INCIDENT MANAGEMENT ACTION STEPS	RESPONSIBLE INDIVIDUAL(S)	STATUS	DATE OF COMPLETION
10. HIPAA Only: If PHI is exposed, then compliance with both HIPAA and W. Va. Code § 46A-2A-101 is required. Refer to Response to Unauthorized Disclosures Appendix.			
11. Complete Risk of Compromise Assessment (ROCA).			
12. Determine if individual notification is required. **NOTE:** Individual notification may be delayed if a law enforcement agency advises that notification would impede an investigation or security. Obtain this request in writing for the file.			
13. If notification is required or optional: ○ Get approval from BRIM prior to notification. ○ Prepare a list of affected individuals. ○ Draft notification letter. ○ Print and mail letters when authorized. ○ Determine how questions from affected individuals will be managed. ○ Develop a notification for Department workforce members. ○ Develop a standby statement for media. ○ Designate a Department leader who will deliver messages and obtain media training if necessary. ○ Create FAQ's to support the communication program.			
14. If a call center is authorized: ○ Obtain a toll-free number and train personnel on messages. ○ Track response, update FAQs, and provide call center training as needed.			

INCIDENT RESPONSE EVENT CHECKLIST

INCIDENT MANAGEMENT ACTION STEPS	RESPONSIBLE INDIVIDUAL(S)	STATUS	DATE OF COMPLETION
15. In consultation with legal counsel and/or the cyber insurance breach coach, identify applicable laws and determine any risks associated with violations of the laws.			
16. Conduct a post incident review to determine what steps can be taken to prevent reoccurrence. ○ Document and distribute analysis of the underlying incident and the response to your IRT. ○ Determine if additional specific controls or improvements to the Privacy Program, including additional training are necessary. ○ Complete the Post Incident Response Assessment (PIRA) within 30 calendar days of the Incident Report. Submit the completed report along with the ROCA to the SPO, CIO, BRIM and your Department Cabinet Secretary.			