INCIDENT MANAGEMENT PROCEDURE

1. **Ensure that incident was reported through the WVOT website**
2. **Review initial incident report**

   What happened? When did it happen? When was it discovered? Who discovered and/or reported it? Was data encrypted? What systems were affected? Has data loss been stopped?

3. **Notify department leaders**
4. **For IT issues, ensure that appropriate IT personnel are contacted**

   Close security gaps ● Isolate affected systems ● Terminate processes that expose PII, etc.

5. **Activate department Incident Response Team**
6. **In the case of theft, notify law enforcement**
7. **Investigate the event**

   Interview witnesses and/or affected parties and document in writing ● Determine if anyone else has knowledge of the event ● List data elements disclosed ● Determine affected individuals and place of residence ● Determine potential impact on other organizations or systems.

8. **Recover data elements exposed**

   Request that recipient of disclosed information either return documents (hard copy), or delete (electronic copy). Get signed affidavit stating the information was returned/deleted and will not be used or disclosed further.

   If already disclosed to others, follow instructions above for each individual who saw or accessed the information.

9. **If applicable, follow special rules for HIPAA, Payment Care Industry data or Federal Tax Information**
10. **Complete the Risk of Harm Assessment (ROHA) to determine whether**

    The incident is a breach ● Individual notification is required, including setting up a call center ● A stand-by media statement should be developed.

11. **Complete investigation, remediate, and take all required action, including submission of Post Incident Response Assessment (PIRA) within 30 days of the incident report**

IMPORTANT CONTACT INFORMATION

Sallie Milam, Chief Privacy Officer	smilam@hcawv.org
Lori Tarr, Assistant Chief Privacy Officer	ltarr@hcawv.org
Sue Haga, Administrative Secretary	shaga@hcawv.org
Phone: 304-558-7000	Website: www.privacy.wv.gov

INCIDENT MANAGEMENT PROCEDURE

1. **Ensure that incident was reported through the WVOT website**
2. **Review initial incident report**

   What happened? When did it happen? When was it discovered? Who discovered and/or reported it? Was data encrypted? What systems were affected? Has data loss been stopped?

3. **Notify department leaders**
4. **For IT issues, ensure that appropriate IT personnel are contacted**

   Close security gaps ● Isolate affected systems ● Terminate processes that expose PII, etc.

5. **Activate department Incident Response Team**
6. **In the case of theft, notify law enforcement**
7. **Investigate the event**

   Interview witnesses and/or affected parties and document in writing ● Determine if anyone else has knowledge of the event ● List data elements disclosed ● Determine affected individuals and place of residence ● Determine potential impact on other organizations or systems.

8. **Recover data elements exposed**

   Request that recipient of disclosed information either return documents (hard copy), or delete (electronic copy). Get signed affidavit stating the information was returned/deleted and will not be used or disclosed further.

   If already disclosed to others, follow instructions above for each individual who saw or accessed the information.

9. **If applicable, follow special rules for HIPAA, Payment Care Industry data or Federal Tax Information**
10. **Complete the Risk of Harm Assessment (ROHA) to determine whether**

    The incident is a breach ● Individual notification is required, including setting up a call center ● A stand-by media statement should be developed.

11. **Complete investigation, remediate, and take all required action, including submission of Post Incident Response Assessment (PIRA) within 30 days of the incident report**

IMPORTANT CONTACT INFORMATION

Sallie Milam, Chief Privacy Officer	smilam@hcawv.org
Lori Tarr, Assistant Chief Privacy Officer	ltarr@hcawv.org
Sue Haga, Administrative Secretary	shaga@hcawv.org
Phone: 304-558-7000	Website: www.privacy.wv.gov

SUBMITTING AN INCIDENT FORM

Any event that involves misuse of computing resources or is disruptive to normal system or data processing operations is an incident. Examples include, but are not limited to:

- Data theft, accidental disclosure;
- Unauthorized modification or deletion of data;
- Theft, loss, or damage of IT assets;
- Denial of service (DoS) attack;
- Misuse of services;
- Overt threats;
- Loss of power or connectivity to a critical system;
- Unauthorized or malicious software;
- Multiple failed login attempts;
- Unauthorized changes to hardware, software, or configuration; and Reports of unusual system behavior.

STEP 1.
SUBMIT A FORM

Report any observation of attempted security or privacy violations at apps.wv.gov/ot/ir or go to WVOT's website and click "Report Incident." Email incidents@wv.gov if form unavailable.

STEP 2.
CALL IF CRITICAL

If the incident is CRITICAL OR ON-GOING, call the Service Desk after submitting the form. No details on the incident should be provided, just provide contact information and incident severity level.

STEP 3.
WAIT

During business hours, you will be contacted as soon as possible by a member of the WVOT Security Team or State Privacy Office. Response times will be based on severity.

STEP 4.
THANK YOU

We appreciate the time you take to report incidents. Please anticipate follow-up questions from either WVOT of the Privacy Office.

IMPORT CONTACT INFORMATION

Reporting Form:	https://apps.wv.gov/ot/ir
Service Desk Phone:	304.558.9966, 877.558.9966
Incident Email:	Incident@wv.gov
Cyber Security Office:	CSO@wv.gov
Website:	technology.wv.gov

West Virginia OFFICE OF TECHNOLOGY

SUBMITTING AN INCIDENT FORM

Any event that involves misuse of computing resources or is disruptive to normal system or data processing operations is an incident. Examples include, but are not limited to:

- Data theft, accidental disclosure;
- Unauthorized modification or deletion of data;
- Theft, loss, or damage of IT assets;
- Denial of service (DoS) attack;
- Misuse of services;
- Overt threats;
- Loss of power or connectivity to a critical system;
- Unauthorized or malicious software;
- Multiple failed login attempts;
- Unauthorized changes to hardware, software, or configuration; and Reports of unusual system behavior.

STEP 1.
SUBMIT A FORM

Report any observation of attempted security or privacy violations at apps.wv.gov/ot/ir or go to WVOT's website and click "Report Incident." Email incidents@wv.gov if form unavailable.

STEP 2.
CALL IF CRITICAL

If the incident is CRITICAL OR ON-GOING, call the Service Desk after submitting the form. No details on the incident should be provided, just provide contact information and incident severity level.

STEP 3.
WAIT

During business hours, you will be contacted as soon as possible by a member of the WVOT Security Team or State Privacy Office. Response times will be based on severity.

STEP 4.
THANK YOU

We appreciate the time you take to report incidents. Please anticipate follow-up questions from either WVOT of the Privacy Office.

IMPORT CONTACT INFORMATION

Reporting Form:	https://apps.wv.gov/ot/ir
Service Desk Phone:	304.558.9966, 877.558.9966
Incident Email:	Incident@wv.gov
Cyber Security Office:	CSO@wv.gov
Website:	technology.wv.gov

West Virginia OFFICE OF TECHNOLOGY