State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Procedure - OP-30 – Incident Reporting and Response

Revised: February 10, 2025

1.0 PURPOSE

Confidential information, as well as the technology used to maintain it, is a vital State of West Virginia government asset. Those who control or use this information are responsible for its care, custody, and protection.

This procedure outlines types of security breaches and disclosures, the roles and responsibilities of employees and management re: incident reporting, handling, testing, and response requirements.

2.0 SCOPE

This policy applies to all authorized system users who utilize State-provided systems and equipment. This includes all WV Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and Office of Shared Administration (OSA) employees, business associates, contractors, and/or consultants.

3.0 PROCEDURE

3.1 When faced with a security incident or an unauthorized disclosure, whether real or perceived, the DH, DHF, DoHS and the OSA must be able to respond by protecting its own information and assist in the protection of the information of others who might be affected by the incident.

3.2 Unauthorized access to the State-provided network and/or disclosure of sensitive personally identifiable information (PII), and restricted protected health information (PHI), Federal Tax Information (FTI), Payment Card Industry (PCI) data, and/or Social Security Administration (SSA) data could result in high risk, immense vulnerability to its systems, and financial penalties to the State. Examples include, but are not limited to the following:

- Loss or theft of a device with legally protected information;

- Employee theft of confidential and/or sensitive information;
- Accidental or unintentional transmission of sensitive and restricted PII, PHI, SSA data PCI data, or FTI to the wrong individual (e.g. a file being emailed to the wrong recipient);
- Discovery of unauthorized access to systems containing sensitive and restricted PII, SSA data, PCI data, or FTI; or
- Transmission of sensitive and restricted PII, PHI, SSA data PCI data, or FTI to an unauthorized vendor or agency.

3.3 All system users, whether Agency employees or contractors, are expected to be aware of federal and state policies, procedures, and guidelines related to incident reporting and the use of sensitive and restricted PHI, PII, SSA data, PCI data, and FTI. These policies and guidelines must be followed in order to effectively safeguard confidential information and to ensure the security and integrity of the information contained within the State network.

3.4 Reporting Security and Privacy Incidents/Unauthorized Disclosures

3.4.1 As specified by WV State Code and Executive Branch Information Security and Privacy policies all DH, DHF, DoHS and the OSA employees, contractors, and users of State systems must report suspected or detected information security breaches or unauthorized disclosures immediately, or no longer than 15 minutes, after discovery.

3.4.2 Because the Agencies and contractors are supported by WVOT systems and networks, all security incidents and/or unauthorized disclosures must be reported concurrently to WVOT and OMIS. Users must access the WVOT Online Computer Security and Privacy Incident Reporting System (https://wv.accessgov.com/technology/Forms/Page/incident-reporting/incident-reporting/0) and complete an Incident Report Form, and then contact OMIS at OSAincident@wv.gov (using the subject line “INCIDENT”). If the suspected incident or disclosure is thought to be critical or ongoing,

employees should call the WVOT Service Desk at 304-558-9966. All reports must include the following information:

- Contact Information (Name, Phone Number, Agency, Cell/Pager)
- Physical Location of Incident (include building number, room number, etc.)
- Date and Time Incident Occurred
- Is the Incident still ongoing? (yes/no)
- Physical Location of Incident (include building number, room number, etc)
- Date and Time Incident Occurred
- Enter a brief summary of the reported incident. If known, enter what you think has or is happening. Examples of incidents include, but are not limited to:
    - Lost or stolen laptop computers or other portable devices
    - Lost or stolen media that contains sensitive data
    - Rampant computer virus infections within the State network
    - Loss of system or network functionality
    - A disaster scenario or act of terrorism
    - A prolonged power outage
    - A compromised (hacked) computer or server
    - A defaced Web page
    - An information security policy violation
- Briefly describe the impact of the reported incident. If known, include the number of affected critical systems, computers, networks, users and/or agencies.

3.4.3 If the incident involves either a suspected or known incident or unauthorized disclosure of sensitive and restricted PHI, PII, FTI, PCI data, or SSA data, the OMIS Information Security Officer (ISO) will also notify the following entities: the IRS, the SSA, and the Centers for Medicare and Medicaid Services (CMS).

3.4.4 The OMIS ISO must report to CMS all potential or confirmed security incidents or data breaches within one (1) hour of discovery. Upon receiving notice of the incident report, the OMIS ISO must notify the following entities:

3.4.4.1 Any event warranting a disconnect from the system-to-system connection to CMS and/or the Federal Services Data Hub (FDSH) must be reported by immediately calling the CMS IT Service Desk at either 1-800-562-1963 or 1-410-786-2580, or by emailing CMS_IT_Service_Desk@cms.hhs.gov. CMS will work with the Agency for the duration of the incident and notify any affected federal agencies.

3.4.4.2 The ISO must then notify the SSA regional office contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the ISO is unable to notify either of these contacts within the one (1) hour timeframe, he/she must report the incident to the SSA National Network Service Center (NNSC) at 877-697-4889 (select “security and PII reporting” from the options list). If the ISO cannot reach the SSA contacts or the NNSC, he/she will contact the SSA’s Office of Information Security, Security Operations Center (SOC) at 1-866-718-6425. The ISO will use a PII Loss Reporting Worksheet to gather and organize information about the incident and will provide to SSA timely updates as any additional information about the loss of PII becomes available.

3.4.5 If the incident involves a possible improper inspection or disclosure of FTI, including breaches and incidents, by a state employee, a contractor, or any other person, the individual making the observation or receiving information must perform the following steps:

3.4.5.1 Contact the OMIS ISO, who must then contact the IRS Office of Safeguards immediately, but no later than 24 hours, at safeguardreports@irs.gov. The ISO must outline for the IRS the specifics of the incident or breach known at the time into a data incident report, including but not limited to the following:

- Point of contact information for the incident (include name, name of Department, email address, phone and cell numbers);
- Date and time the incident occurred (mm/dd/yy and hh:mm:ss am/pm), if known;
- Date and time the incident was discovered (mm/dd/yy and hh:mm:ss am/pm);
- How the incident/breach was discovered;
- A brief summary of the reported incident (i.e., Description of the incident/breach and the data involved, including specific data elements, if known);
- Potential number of FTI records involved; if unknown, provide a range if possible
- Physical location of incident (include street address, building number, room number, etc.);
- IT involved (e.g., laptop, server, mainframe)
- Does the incident involve unauthorized access or disclosure by an agency employee? (Y/N)
- If a criminal indictment is not pursued, will a disciplinary or adverse action be proposed against the agency employee involved in this unauthorized access or disclosure? (Y/N)

3.4.5.2 After reporting the incident or breach, the OMIS ISO must immediately conduct an internal investigation to determine if FTI was involved.

3.4.5.3 Reports must be sent electronically and encrypted via IRS-approved encryption techniques as outlined in Publication 1075, Section 2.E.3, Encryption Requirements. Use the term "data incident report" in the subject line of the email. FTI must not be included in the data incident report.

3.4.5.4 Even if all information is not available, the OMIS ISO must immediately notify the IRS of the suspected or known incident or breach. Additional information must be provided to the Office of Safeguards as soon as it is available.

3.4.5.5 The Office of Safeguards will coordinate with the Departments regarding appropriate follow-up actions required to be taken to ensure continued protection of FTI. Once the incident has been addressed, the OMIS must conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance.

3.4.5.6 As required by the Taxpayer First Act (TFA) 3002 and Internal Revenue Code (IRC) 7431, the Departments must provide written notification to any taxpayer whose FTI was subject to unauthorized access or disclosure when a disciplinary or adverse action is proposed against a Department employee responsible. The written notification must include the date of the unauthorized inspection or disclosure and the rights of the taxpayer.

3.4.5.7 The Departments must confirm to the Office of Safeguards when the required written notification to the taxpayer is completed and

of any pending media releases, including sharing a draft of the release, prior to distribution.

3.4.6 The OMIS ISO will notify the OMIS Chief Information Officer (CIO) of all information security incidents as defined in the WVOT Incident Management Plan (WVOT-PL1007), and other incidents as defined in this procedure.

3.4.7 The OMIS CIO will notify the DH, DHF, DoHS and the OSA Cabinet Secretaries and others, as appropriate.

3.4.8 Incident investigations will begin immediately upon receipt of reporting and will be conducted in concurrence with notification to regulatory agencies, as required.

3.4.9 The OMIS ISO will collaborate and cooperate with federal, state, and local authorities, and with WVOT to implement an incident management plan and to expedite mitigation strategies.

3.4.10 When necessary, designated individuals within OMIS will work with the DH, DHF, DoHS and the OSA Privacy Office and/or the WVOT to classify the disclosure; recover lost or stolen sensitive and restricted PII, FTI, SSA data, PCI data, or PHI; determine whether it is necessary to notify impacted individuals; and activate the appropriate response team. More detailed information is outlined in Section 4.5 of the West Virginia State Privacy Office policy WVEB-P101.1.

3.5 Incident Response Training

3.5.1 The OMIS Quality and Compliance team is responsible for providing Incident Response training to information system users consistent with their assigned roles and responsibilities.

3.5.2 Training is provided to all DH, DHF, DoHS and the OSA employees upon hire and on an annual basis thereafter. Instruction materials include federal guidelines, Executive Branch and OMIS policies, and online training.

3.5.3 Employees must receive Incident Response training within 30 days prior to assuming an incident response role or responsibility or acquiring system access, as required by information system changes, and annually thereafter.

3.5.4 Incident response training must be reviewed and/or updated on an annual basis and following major business and systems change impacting the FTI environment.

3.6 Incident Response Testing

3.6.1 OMIS will collaborate with WVOT, contractors, and other stakeholders as necessary to test the effectiveness of the incident response capability annually using tabletop exercises.

3.6.2 IT personnel involved in the Incident Response testing process must use qualitative and quantitative data from testing to:

a. Determine the effectiveness of incident response processes;

b. Continuously improve incident response processes; and

c. Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format. (For more information, see OMIS IM-01 - Incident Management Plan.)

3.7 Incident Response Notification

3.7.1 The Departments must provide written notification to a taxpayer whose FTI was subject to unauthorized access or disclosure when a disciplinary

or adverse action is proposed against the Department employee responsible.

3.7.2 The required written notification to the taxpayer must include the date of the unauthorized inspection or disclosure and the rights of the taxpayer under IRC § 7431.

3.7.3 The Departments must confirm to the Office of Safeguards when the required written notification to the taxpayer is completed. In addition, the Departments must inform the Office of Safeguards of any pending media releases, including sharing a draft of the release, prior to distribution.

3.8 Incident Handling

3.8.1 The OMIS will coordinate with WVOT and applicable contractors to implement an incident handling capability across the Departments. The incident handling process will include preparation, detection and analysis, containment, eradication, and recovery and must be consistent with the Incident Response Plan. The entities must also do the following:

3.8.1.1 Coordinate incident handling activities with contingency planning activities;

3.8.1.2 Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

3.8.1.3 Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the Departments. (For more information, see IM-01- Incident Management Plan.)

3.9 Incident Response Plan

3.9.1 OMIS must develop an Incident Response Plan and complete the following steps:

3.9.1.1 Distribute copies of the incident response plan to authorized incident response personnel and agency personnel with access to FTI;

3.9.1.2 Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

3.9.1.3 Communicate incident response plan changes to authorized incident response personnel and Department personnel with access to FTI;

3.9.1.4 Protect the incident response plan from unauthorized disclosure and modification.

3.10 Information Spillage Response

3.10.1 OMIS will coordinate with WVOT and applicable contractors to respond to information spills by doing the following:

3.10.1.1 Assigning designated incident response agency personnel with responsibility for responding to information spills;

3.10.1.2 Identifying the specific information involved in the system contamination;

3.10.1.3 Alerting designated agency officials of the information spill using a method of communication not associated with the spill;

3.10.1.4 Isolating the contaminated system or system component;

3.10.1.5 Eradicating the information from the contaminated system or component;

3.10.1.6 Identifying other systems or system components that may have been subsequently contaminated; and

3.10.1.7 Performing the following additional actions: Report incident information to the appropriate special agent-in-charge and the IRS Office of Safeguards.

3.11 Incident Response policies and procedures will be updated every three (3) years or when a significant change occurs.

3.12 All Agency employees must read and sign the *Policy/Procedure Acknowledgement*, which is located on the last page of this document.

4.0 VIOLATIONS

Violation of this procedure will subject an individual to disciplinary action up to and including dismissal. Depending on the circumstances surrounding the incident, policy violations could result in prosecution under state and federal statutes.

5.0 DEFINITIONS

5.1 **Breach** – Any situation for other than authorized purposes to have access or potential access to sensitive or restricted information, whether physical or electronic.

5.2 **Disclosure** - The release, transfer, provision of, access to, or divulging in any other manner information outside the Department holding the information. Disclosures can be authorized or unauthorized. There are two possible types of Unauthorized Disclosures.

5.3 **Employee** – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of this procedure, the term "employee" will include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined to be subject to this procedure. This definition does not create any additional rights or duties.

5.4 **Federal Tax Information (FTI)** – According to the IRS Publication 1075, FTI is defined as any return or return information received from the IRS or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information.

5.5 **Incident** - Any event that involves misuse of computing resources, compromises data, or is disruptive to normal system or data processing operations.

5.6 **Information Spillage** - Instances where classified or controlled unclassified information (e.g., FTI) is inadvertently placed on systems that are not authorized to process such information. Such information spills occur when information that is initially thought to be of lower sensitivity is transmitted to a system and then subsequently determined to be of higher sensitivity.

5.7 **Office of Management Information Services (OMIS) -** This office reports directly to the DH, DHF, DoHS and the OSA Cabinet Secretaries and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the Departments.

5.8 **Payment Card Industry Data Security Standard (PCI DSS)** – A proprietary information security standard for organizations that handle branded credit cards from the major card schemes.

5.9 **Personally Identifiable Information (PII)** – All information that identifies, or can be used to identify, locate, or contact (or impersonate) a particular individual.

Personally identifiable information is contained in both public and non-public records. Examples may include but are not limited to a specific individual's: first name (or initial) and last name (current or former); geographical address, electronic address (including an e-mail address); telephone number or fax number dedicated to contacting the individual at their physical place of residence; social security number; credit and debit card numbers; financial records, including loan accounts and payment history; consumer report information; mother's maiden name; biometric identifiers, including but not limited to, fingerprints; facial recognition and iris scans; driver identification number; full face image; birth date; birth or adoption certificate number; physical description; genetic information; medical, disability or employment records, including salary information; computer information, including information collected through an Internet cookie; criminal history, etc. When connected with one or more of the items of information specified above, PII includes any other information concerning an individual, that if disclosed, identifies or can be used to identify a specific individual physically or electronically.

5.10 **Privacy Officer** - An individual responsible for implementing privacy policies and procedures of a Department, leading the Department's privacy program and ensuring that the Department complies with its stated procedures.

5.11 **Protected Health Information (PHI)** – With regard to HIPAA covered entities, individually identifiable health information, including demographic information, whether oral or recorded in any form or medium, that relates to the individual's health, health care services and supplies, or payment for services or supplies, ***and*** which identifies the individual or could reasonably be used to identify the individual. This includes information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual including but not limited to preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care as well as counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the structure or function of the

body; or the past, present or future payment for the provision of health care to an individual; *and* includes identity information, such as social security number or driver's license number, even if the name is not included, such that the health information is linked to the individual. Protected health information does not include the following:

- Records covered by the Family Educational Right and Privacy Act.
- Employment records held by the entity in its role as employer (though use and dissemination of these records may be subject to other federal and state laws such as the Family and Medical Leave Act and West Virginia Workers' Compensation).

5.12 **Sensitive PII** - Those elements of PII that must receive heightened protection due to legal or policy requirements. Examples of Sensitive PII include, but are not limited to the following:

- Social Security numbers
- Credit card numbers
- Health and medical data
- Driver license numbers
- Individual financial account numbers

5.13 **Social Security Administration (SSA) Data** – Data received and accessed from the SSA for purposes of administering federally funded and state administered programs [i.e., Medicaid, Supplemental Nutrition Assistance Program (SNAP), and State Health Insurance Programs], which determines individual eligibility, citizenship status, and social security number verifications, etc.

5.14 **Unauthorized External Disclosure** – Occurs when PII, FTI, PCI data, SSA data, or PHI is exposed or potentially exposed to any person(s) outside of the Executive Branch.

5.15 **Unauthorized Internal Disclosure** – Occurs when PII, FTI, PCI data, SSA data, or PHI is exposed or potentially exposed to any person(s) within the Executive Branch.

5.16 **West Virginia Office of Technology (WVOT)** - The division of the Department of Administration established by WV Code § 5A-6-4a*, et. seq.,* which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services and reviewing information technology contracts.

6.0 REFERENCES/RELATED MATERIAL

This procedure applies to all relevant federal and state statutes pertaining to breaches of the security of protected, electronic data. These statutes include, but are not limited to the following:

6.1 26 U.S. Code § 7431 - *Civil damages for unauthorized inspection or disclosure of returns and return information*

6.2 Internal Revenue Service (IRS) Publication 1075

6.3 WV Code §46-2A-101 *et seq*. – *The West Virginia Consumer Credit and Protection Act*, "Breach of Security of Consumer Information"

6.4 *Health Insurance Portability and Accountability Act (HIPPA)* of 1996 as amended by the *American Recovery and Reinvestment Act* (ARRA) of 2009 (the HITECH Act)

6.5 OMIS Policy 0512 – *Information Security Policy*

6.6 WVEB-P101.1 – West Virginia Executive Branch Procedure: *Response to Unauthorized Disclosures* (http://www.privacy.wv.gov/incidentresponse/Pages/default.aspx)

6.7 WVOT PO1006 – *Data Classification*

6.8 WVOT-PL1007 – *Incident Management Plan*

6.9 OMIS Procedure - IM-01 - Incident Management Plan

6.10 Social Security Administration Information Exchange Agreement and the *Electronic Information Exchange Security Requirements and Procedures, for State and Local Agencies Exchanging Electronic Information with the Social Security Administration,* (also known as Technical System Security Requirements - TSSR), Document Classification: Sensitive

6.11 Centers for Medicare and Medicaid Service (CMS), Computer Matching Agreement (CMA) for State-based Administering Agencies and the Interconnecting Security Agreement (ISA)

7.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	10/12/2016	Approved by CIO
Version 1.1	02/14/2017	Revised CMS Contact Information
Version 1.2	09/17/2018	Annual Review and formatting revisions
Version 1.3	03/10/2020	Annual Review and formatting revisions

State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Procedure - OP-30 – Incident Reporting and Response

Revised: February 10, 2025

Version 1.4	03/25/2021	Annual Review
Version 1.5	11/17/2021	Revised SSA Reporting Information
Version 1.6	02/01/2022	Converted document from Word to Google Docs; Updated formatting; Annual Review
Version 1.7	02/07/2023	Annual Review; updated policy links
Version 1.8	08/25/2023	Updated 3.4.5 - per IRS, removed requirement to contact TIGTA
Version 1.9	02/12/2024	Annual Update - changed “DHHR” to “Departments of Health, Health Facilities, Human Services, and Office of Shared Administration”, updated links, overall review of content, revised language throughout
Version 2.0	07/01/2024	As the result of IRS security assessment, revised and/or added language in Sections 3.4, 3.4.5, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 5.0

State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Procedure - OP-30 – Incident Reporting and Response

Revised: February 10, 2025

Version 2.0.1	11.15.2024	Updated incident email address - from DHHRincident@wv.gov to osaincident@wv.gov Revised Departments' acronyms throughout document
Version 2.1	02/10/2025	Annual review and update - revised format