STANDARD OPERATING GUIDE

# D4H INCIDENT RECORDS MANAGEMENT

Document Number: 08.06.2

20 August 2026

Document Handling Note: **UNRESTRICTED**

Authority: Ohio Revised Code Chapter 5502; Clinton County Emergency Operations Plan (EOP); National Incident Management System (NIMS); Applicable County Resolutions and Policies.

Prepared by: **Clinton County Emergency Management Agency**

## 1. Purpose

The purpose of this Standard Operating Guide (SOG) is to establish a common, repeatable process for creating, maintaining, preserving, and closing incident records managed through D4H Incident Manager and the Clinton County EMA network drive.

During active operations, D4H serves as the authoritative operational record for incident information, including the Situation Report, Log of Events, status boards, forms, maps, attachments, resource requests, and other products created or maintained during the incident.

After operations terminate, required D4H records will be exported, printed, or otherwise saved and consolidated with supporting documents maintained on the network drive. The completed network-drive incident folder becomes the permanent incident record and the primary source package for after-action reporting, operational review, records retention, continuity, and future planning.

This SOG applies to all incidents created in D4H, including monitoring operations, emergency responses, planned events, exercises, Emergency Operations Center activations, recovery activities, and other coordination operations. It is intended to support consistent documentation, situational awareness, decision-making, accountability, continuity of operations, and preservation of Clinton County EMA institutional records.

# 2. Scope

This SOG applies to all incidents created and managed through D4H Incident Manager by Clinton County EMA, including:

- Monitoring and enhanced-monitoring operations
- Emergency and disaster responses
- Severe weather operations
- Hazardous materials incidents
- Infrastructure and utility disruptions
- Planned events
- Training exercises
- Emergency Operations Center activations
- Recovery operations
- Other incidents or coordination activities requiring an organized operational record

This guidance applies to the full incident-record lifecycle, including incident creation, naming, use of D4H templates, creation of the matching network-drive folder, collection and organization of supporting documents, maintenance of the Situation Report and Log of Events, preservation of formal communications, export of D4H products, incident closeout, and preparation of the source package for after-action reporting.

This SOG applies to Clinton County EMA personnel and any other personnel assigned responsibility for creating, entering, updating, reviewing, exporting, printing, organizing, or preserving incident information under the direction of the EMA Director.

D4H is flexible and may be configured differently based on the incident. Not every incident will require the same status boards, forms, maps, task boards, resource requests, attachments, or supporting folders. Additional products may be created as operational needs develop. However, every incident will meet the minimum documentation and closeout requirements established by this SOG.

This SOG does not establish user-account creation procedures, individual access permissions, security roles, board-level access, Static Link controls, or other system-security settings. Those subjects are addressed separately under:

- 08.06.1: SOG – D4H User Account Setup and Maintenance
- 08.06.3: SOG – D4H Security and Access Controls.

# 3. Authority

Clinton County EMA will manage incident information using the following principles:

- D4H is the operational record during active operations. Significant actions, decisions, impacts, status changes, resource activity, and coordination information will be documented in D4H as close to the time of occurrence as practical.
- The network drive is the permanent record location after termination. Required D4H records will be exported, printed, or otherwise saved and consolidated with supporting documents in the matching network-drive incident folder.

- Every incident will meet a minimum documentation standard. At a minimum, each incident will include complete incident details, a Situation Report, a chronological Log of Events, applicable attachments or links, a final status or termination entry, and required closeout exports.
- Documentation will remain scalable. Status boards, forms, maps, task boards, resource requests, attachments, and other products may be created, modified, or added as operational needs develop.
- Incident names and folders will match. The D4H incident and network-drive incident folder will use the same date and short incident name to support identification, filing, and future retrieval.
- Folder organization will remain familiar across incident types. Common folder numbers and functions will remain consistent across templates. A folder may be omitted when it does not apply, but an established folder number will not be reassigned to a different function.
- Original source records will be preserved. Documents received from another organization will be retained as originally received. Annotated, converted, reformatted, or working copies will be saved separately and clearly identified.
- Formal incident communications will be retained. Formal emails, written direction, official requests, reports, briefings, public information products, resource commitments, and other formal communications will be saved as part of the incident record when available.
- Informal communications will be retained when operationally significant. Text messages, informal emails, telephone notes, or similar communications will be documented or saved when they contain a significant decision, direction, impact report, resource commitment, safety concern, status change, or other information needed to understand the response.
- Changing conditions will be preserved. Situation Report snapshots will be saved before material updates so the record shows how conditions, impacts, priorities, and courses of action changed during the incident.
- Continuity copies will be maintained. The Log of Events will be printed at the end of each operational shift. When printing is unavailable, an electronic continuity copy will be exported and saved offline until a paper copy can be produced.
- Restricted records will be separated. Sensitive, protected, or potentially exempt information will be maintained under 99 - Restricted Records and reviewed according to its content and applicable legal authority.
- The record will support later review. Incident documentation should allow a person who was not present to understand what occurred, what decisions were made, why actions were selected, what impacts developed, and how operations ended.



# 4. Mission Statement

## 4.1. EMA Director.

The Clinton County EMA Director has overall responsibility for D4H incident records management and the permanent network-drive incident file.

The EMA Director will:

- Authorize the creation of D4H incidents or designate personnel permitted to create them.
- Confirm the incident name, date, and applicable D4H template.
- Ensure a matching network-drive incident folder is created using the appropriate hazard or incident template.
- Determine the minimum and additional D4H products needed for the incident.
- Establish documentation expectations for assigned personnel.
- Ensure significant actions, decisions, impacts, resource activity, and status changes are documented.

- Review the Situation Report, Log of Events, status boards, forms, maps, attachments, and other records as needed.
- Ensure Situation Report snapshots and shift-end Log of Events copies are preserved.
- Identify missing, incomplete, conflicting, or unsupported incident information.
- Contact participating organizations to request reports, forms, photographs, emails, logs, or other records needed to complete the incident file.
- Approve incident termination and record closeout.
- Verify that required D4H products have been exported, printed, or otherwise saved to the network drive.
- Confirm restricted records are appropriately separated.
- Determine when the permanent incident record is sufficiently complete to begin the After-Action Report process.

Other personnel may perform individual records-management tasks, but final responsibility remains with the EMA Director.

# 4.2. Designated EMA Personnel

Personnel designated by the EMA Director may create incidents, enter information, update products, organize files, produce exports, or support incident closeout.

Assigned personnel will:
- Follow the naming, documentation, and folder standards established by this SOG.
- Enter information accurately and as close to the time of occurrence as practical.
- Use factual, neutral, and concise wording.
- Identify the source of information when it is not based on direct observation.
- Preserve original source documents.
- Save formal incident communications when available.
- Notify the EMA Director of significant information gaps, conflicting reports, sensitive records, or technical problems.
- Complete assigned export, printing, filing, and closeout tasks.
- Avoid deleting or substantially altering incident information without authorization.

## 4.3. Other D4H Users and Incident Contributors

Local-government personnel, partner organizations, stakeholder representatives, mutual-aid personnel, and other authorized users may contribute information based on their assigned duties and approved access.

Incident contributors are expected to:
- Enter only information related to their organization, assigned function, or operational responsibility.
- Clearly identify significant actions, impacts, requests, decisions, and status changes.
- Avoid speculation, unsupported conclusions, personal opinions, or unnecessary personal information.
- Correct known errors promptly or notify EMA when they cannot make the correction.
- Provide supporting records to EMA when requested.
- Preserve records created outside D4H that are necessary to understand their organization's involvement.

User permissions, board access, read or write authority, Static Links, and security controls are governed separately under 08.06.3: SOG – D4H Security and Access Controls.

# 5. Incident Creation and Naming

## 5.1. Authority to Create an Incident

D4H incidents may be created only by the EMA Director or personnel specifically designated by the EMA Director to perform that function.

Local-government personnel, partner organizations, stakeholder representatives, and other D4H users will request incident creation through Clinton County EMA. Access to D4H does not independently authorize a user to create an incident.

## 5.2. When to Create an Incident

A D4H incident should be created when an activity requires an organized operational record. This may include:

- Monitoring or enhanced monitoring
- Multi-agency coordination
- Significant or changing impacts
- Public alerts or coordinated public information
- Resource requests or mission tracking
- Situation reporting
- Emergency Operations Center activity
- Planned-event coordination
- Exercise documentation
- Recovery coordination
- Other activities directed by the EMA Director

An incident may be created before impacts occur when forecast conditions, planned activities, or developing threats require organized monitoring and documentation.

Duplicate incidents should be avoided. Information related to the same event should remain within the existing incident unless the EMA Director determines that a separate incident record is operationally or administratively necessary.

## 5.3. Incident Naming Standard

Incident names should be operationally useful, neutral, and no more specific than necessary to identify and retrieve the record. Names should avoid unnecessarily identifying specific persons, businesses, substances, alleged conduct, legal matters, or sensitive circumstances when a broader title will adequately distinguish the incident. Detailed information will be maintained within the incident description, Situation Report, Log of Events, and supporting records rather than the incident title.

Incident names should not be written as public headlines or attempt to summarize the entire event.

The D4H incident name will use the following format:

- YYYYMMDD <u>General Location or Area</u> + <u>Broad Response Type</u>

Examples include:

- 20260710 Sabina Spill Response
- 20260710 Sabina Spill Response
- 20220811 LE Operations - Smith and Van Tress Road
- 20220305 Dutch Creek Spill Response

The incident name should be:

- Brief and specific
- Written in plain language
- Sufficient to distinguish it from other incidents
- Consistent with terminology used in public information and operational records when practical
- Free of unnecessary personal information or sensitive details

The D4H-assigned incident reference number will remain part of the D4H record but is not required in the network-drive folder name.

## 5.4. Network-Drive Incident Folder

When a D4H incident is created, a matching network-drive incident folder will also be created.

The person creating the folder will:

1. Select the template that most closely matches the primary incident type.
2. Copy and paste the complete template folder.
3. Rename the copied folder to exactly match the D4H incident name.
4. Confirm that the folder was created in the correct active-response location.
5. Remove no standard folders merely because they are not immediately needed unless the selected template was intentionally designed without them.

Available templates may include:

- zz-Active Aggressor Template-zz
- zz-Dam Failure (Class I) Template-zz
- zz-HazMat Template-zz
- zz-Power Outage Template-zz
- zz-Wx Template-zz

Additional templates may be developed as recurring operational needs are identified.

## 5.5. Template Selection and Modification

Template selection will be based on the primary incident type. When an incident includes multiple hazards or cascading impacts, the template that best supports the main operational need should be selected.

Folders or subfolders may be added as conditions develop. Established folder numbers and functions will not be reassigned. Intentional numbering gaps are acceptable when a particular folder does not normally apply to that incident type.

The incident folder structure should remain familiar across Natural Disasters, Technological Disasters, and Human-Caused Disasters while allowing hazard-specific information to be organized where it is most useful.

# 6. Minimum D4H Incident Record

Every incident created in D4H will maintain a minimum operational record. The amount of detail may be scaled to the incident, but the required elements will not be omitted solely because the incident is short, produces limited impacts, or does not require Emergency Operations Center activation.

## 6.1. Incident Details

The incident record will include accurate basic information, including:

- Incident name
- Incident type
- Start date and time
- Location or area affected
- Incident status
- Responsible or coordinating organization
- Brief incident description
- Applicable D4H template
- Other identifying information required by the system

Incident details will be updated when the scope, location, operational status, or nature of the incident materially changes.

## 6.2. Situation Report

Every incident will include a Situation Report or equivalent Situation page that provides the current operational picture.

The Situation Report should identify, as applicable:

- What occurred or may occur
- Areas or jurisdictions affected
- Known and potential impacts
- Current Community Lifeline status
- Significant operational actions
- Public information issued
- Resource or coordination needs
- Current priorities
- Expected duration or next operational period
- Conditions requiring continued monitoring
- Current incident status

The Situation Report is a current-status product and should be updated as conditions change. It is not intended to reproduce the complete Log of Events.

## 6.3. Log of Events

Every incident will include a chronological Log of Events.

The log will document significant:

- Initial reports and notifications
- Monitoring actions
- Decisions and courses of action
- Status and impact changes
- Resource requests and commitments
- Partner coordination
- Public alerts and information releases
- Safety concerns
- Significant communications
- Operational milestones
- Stabilization actions
- Demobilization and termination actions

Entries should be factual, concise, and entered as close to the time of occurrence as practical. When information is received from another organization or source, the entry should identify the source.

The log should not be filled with repetitive status checks, routine acknowledgments, or minor administrative activity unless that information is necessary to understand the incident.

## 6.4. Attachments and Links

Applicable supporting information will be attached to or linked from the D4H incident when doing so supports operational access, situational awareness, coordination, or decision-making.

Supporting information may include:

- Briefings
- Maps
- Reports
- Photographs
- Public information products
- Weather information
- Utility status information
- Partner documents
- Forms
- Resource information
- Technical references
- Relevant network-drive locations
- Approved external links

D4H attachments do not replace the requirement to preserve permanent records on the network drive after termination.

## 6.5. Additional D4H Products

Additional D4H products may be created as operational needs develop, including:

- Status boards
- Forms
- Maps
- Task boards
- Resource requests
- Assignment tracking
- Damage-assessment products
- Public-information products
- Stakeholder reporting tools
- Other incident-specific pages or displays

Not every incident requires every available D4H function. Products should be created when they improve coordination, accountability, situational awareness, decision-making, or records preservation.

## 6.6. Final Status and Termination Entry

Every incident will include a final Log of Events entry documenting termination or transition to another phase.

The final entry should identify:

- Date and time operations terminated or transitioned
- Final known incident status
- Remaining monitoring or follow-up requirements
- Outstanding resource, documentation, or coordination issues
- Responsibility for unresolved actions
- Direction for incident-record closeout

The D4H incident status will be updated to reflect termination, closure, or the appropriate continuing operational condition.

# 7. Network-Drive Incident Folder Management

The network-drive incident folder supports document organization during active operations and becomes the permanent incident record after D4H closeout.

The network drive does not replace required D4H documentation during the response. Significant actions, decisions, impacts, and status changes will continue to be entered in D4H even when supporting documents are saved on the network drive.

## 7.1. Incident Folder Location

Active incident folders will be maintained in the designated EMA response-records location.

The response directory may include:

- Annual folders containing completed incidents from previous years
- Current active or recently completed incident folders
- Individual hazard or incident templates located at the bottom of the directory using the zz- naming convention

Examples include:

- 2023 Responses
- 2024 Responses
- 2025 Responses
- 20260710 Sabina Spill Response
- 20260721 Enhanced Risk Severe Wx
- zz-Active Aggressor Template-zz
- zz-Dam Failure (Class I) Template-zz
- zz-HazMat Template-zz
- zz-Power Outage Template-zz
- zz-Wx Template-zz

At the appropriate archive point, completed incident folders may be moved into the applicable annual response folder.

## 7.2. Standard Folder Numbering

Approved incident templates will use a consistent folder-numbering system so common records are stored in familiar locations.

The following rules apply:

- A folder number will retain the same general function across all templates.
- A folder may be omitted when it does not normally apply to that incident type.
- An omitted folder may create an intentional gap in the numbering sequence.
- An established folder number will not be reassigned to an unrelated function.
- Additional subfolders may be created as operational needs develop.
- Folder names should remain short, direct, and understandable without additional explanation.

The following folders will retain the same number and function when used:

- 10 - Closeout and AAR
- 99 - Restricted Records

Hazard-specific folders may differ between Natural Disaster, Technological Disaster, and Human-Caused Disaster templates.

## 7.3. Use During Active Operations

Supporting documents should be saved to the network-drive incident folder as they are received or produced when practical.

- These records may include:
- External briefings
- Weather or technical information
- Public alerts
- Public information products
- Partner reports
- Maps
- Photographs and videos
- Utility status information
- Damage reports
- Resource documents
- Formal correspondence
- Forms and spreadsheets
- Other supporting operational records

Files should be placed in the folder that best represents their primary operational purpose. Duplicate copies should be avoided unless duplication is necessary for continuity, distribution, or records protection.

## 7.4. File Naming

Files should be named so their date, source, and purpose can be understood without opening them.

Time-sensitive operational products should generally use:
- YYYYMMDD_HHMM Source - Description

Examples:
- 20260721_0830 NWS ILN - Weather Briefing.pdf
- 20260721_1246 D4H - SITREP 01.pdf
- 20260721_1600 AES - Clinton County Outage Map.png
- 20260721_2110 EMA - Final CCEA Alert.pdf

When the exact time is unknown or unnecessary, the time may be omitted.

## 7.5. Draft and Final Products

EMA-created documents that undergo review may use (Draft) and (Final) to show document status.

Examples:
- (Draft) 20260710 Sabina Spill After-Action Report.docx
- (Final) 20260710 Sabina Spill After-Action Report.pdf

(Draft) and (Final) should normally be used for reports, plans, releases, summaries, and other products that have a defined review or approval process.

Routine exports, screenshots, received briefings, photographs, and partner documents should normally retain a date-, time-, and source-based filename rather than being labeled as draft or final.

### 7.6. Permanent Reference Materials

Standing guidance, blank forms, training material, technical manuals, FEMA or Ohio EMA reference documents, and other reusable material should be maintained in an appropriate permanent reference library rather than copied into every incident template.

A reference document should be copied into the incident folder only when:

- It was specifically used during the incident;
- It was issued or distributed as part of the response;
- It was completed or modified for the incident;
- It supports a significant decision or course of action; or
- Its preservation is necessary to understand the incident record.

## 8. Situation Report and Log Preservation

The D4H Situation Report and Log of Events are the primary records used to document changing conditions, significant actions, decisions, and operational progress during an incident. Both records will be preserved in a manner that supports continuity, closeout, and later after-action review.

### 8.1. Situation Report Maintenance

The D4H Situation Report will reflect the current operational picture and will be updated as conditions materially change.

Material changes may include:

- Changes in incident scope or affected area
- New or worsening impacts
- Community Lifeline status changes
- Significant protective actions
- Changes in operational priorities
- Major resource needs or commitments
- Public information actions
- Stabilization or restoration progress
- Transition, demobilization, or termination decisions

The Situation Report is subject to revision as D4H forms, operational needs, and reporting practices change. This SOG establishes the requirement to maintain and preserve the record but does not permanently prescribe specific Situation Report fields.

### 8.2. Situation Report Snapshots

Before making a material update to the D4H Situation Report, the existing version will be exported or otherwise saved as a snapshot.

Situation Report snapshots preserve:

- Conditions known at a specific point in time
- The basis for operational decisions

- Changes in priorities or courses of action
- The complexity and progression of the incident
- Information that may later be replaced or summarized
- Context needed to fill gaps during after-action review

Minor spelling, formatting, or administrative corrections do not require a new snapshot.

## 8.3. Situation Report File Naming and Storage

Situation Report snapshots will be saved in the designated network-drive folder using a chronological filename.

Example:

```
02 - Situation Reports and Briefings
 └── SITREP Snapshots
```

Recommended file naming:

- YYYYMMDD_HHMM D4H - SITREP Number.pdf

Examples:

- 20260721_0900 D4H - SITREP 01.pdf
- 20260721_1500 D4H - SITREP 02.pdf
- 20260721_2110 D4H - SITREP Final.pdf

The final Situation Report will be clearly identified during closeout.

## 8.4. Shift-End Log of Events Copy

At the end of each operational shift, the complete D4H Log of Events will be printed and placed in the central incident records file.

This requirement provides an offline continuity record in the event of:

- D4H disruption
- Internet failure
- Electrical-power loss
- Equipment failure
- Cyber incident
- Loss of access to the network drive
- Relocation of EOC operations
- Other significant technology disruption

For an incident that begins and terminates within one operational shift, the final Log of Events printout satisfies this requirement.

## 8.5. Printing Unavailable

Clinton County EMA does not maintain a permanently equipped EOC. EOC operations may be established at an identified location using deployable equipment and position support kits.

When a printer, electrical power, or suitable workspace is unavailable at shift change:

1. Export the complete Log of Events to PDF.
2. Save the PDF to the network-drive incident folder when access is available.

3. Save an offline copy to an authorized encrypted USB drive or other approved local storage when available.
4. Print the Log of Events and place it in the central incident records file as soon as printing becomes available.

The inability to print immediately does not remove the requirement to preserve the shift-end record.

### 8.6. Central Incident Records File

Printed Log of Events copies and other required paper records will be maintained in one central incident records binder or file controlled by Clinton County EMA.

Printed operational records will not be distributed among individual EOC Position Support Kits as the official record. Position kits may contain reference materials, checklists, administrative supplies, and continuity resources, but the central incident file will remain the controlled paper record for the incident.

## 9. Communications and Source Records

Incident communications and source documents will be preserved when they document significant operational information, decisions, coordination, impacts, or actions.

### 9.1. Formal Communications

For purposes of this SOG, formal communications include official written direction, reports, requests, notifications, approvals, commitments, and information products transmitted through established organizational channels.

Formal incident communications will be retained when available. Examples include:

- Official direction or approval
- Written requests for assistance
- Resource requests and commitments
- Situation reports and briefings
- Reports from participating organizations
- Public alerts and public information products
- Government or utility status reports
- Formal notifications
- Written demobilization or termination direction
- Other correspondence necessary to document the incident

Every reasonable attempt should be made to save important emails as PDF files showing:

- Sender
- Recipients
- Date and time
- Subject
- Complete message content

Email attachments will be saved separately in their original format when practical.

### 9.2. Informal Communications

Informal communications do not require routine preservation unless they contain operationally significant information.

An informal email, text message, telephone note, chat message, or similar communication should be documented or retained when it includes:

- A decision or course of action
- Operational direction
- A resource request or commitment
- A significant impact or status change
- A safety concern
- A report requiring follow-up
- Information necessary to understand why an action was taken
- A documentation gap or unanswered request
- Other information needed to complete the incident record

Operationally significant informal communications may be:

- Summarized in the D4H Log of Events;
- Saved as a screenshot;
- Converted to PDF;
- Documented through a memorandum or telephone record; or
- Preserved through another practical method.

Routine acknowledgments, scheduling messages, duplicate notifications, and courtesy communications do not require preservation unless they provide necessary context.

## 9.3. Original Source Documents

Documents received from another organization will be preserved as originally received.

The original file will not be overwritten, edited, reformatted, annotated, or replaced. Any working, annotated, converted, redacted, or revised copy will be saved separately and clearly identified.

This requirement applies to:

- Partner reports
- Briefings
- Maps
- Spreadsheets
- Photographs and videos
- Utility information
- Technical reports
- Submitted forms
- Email attachments
- Weather products
- Other supporting records

## 9.4. Source Identification

When practical, filenames or supporting documentation should identify:

- Date and time received or created
- Source organization
- Document purpose
- Applicable version
- Whether the file is an original, working, redacted, draft, or final copy

When information is entered into D4H from another source, the Log of Events or applicable product should identify the source sufficiently to support later verification.

# 10. Restricted Records

Incident files may include information that requires limited access, review before release, redaction, or withholding under applicable state or federal law.

## 10.1. Restricted Records Folder

Applicable incident templates will include:

- 99 - Restricted Records

Recommended subfolders include:

```
99 - Restricted Records
├── 01 - Security and Infrastructure (R.C. 149.433)
├── 02 - Medical and Personal Information
├── 03 - Law Enforcement Sensitive
├── 04 - Legal and Other Protected Records
└── 05 - Release Review and Redacted Copies
```

Additional subfolders may be created when necessary.

## 10.2. Records Requiring Separation

Records should be placed under 99 - Restricted Records when they contain or may contain:

- Security procedures or access information
- Detailed critical-infrastructure information
- Infrastructure vulnerabilities
- Protected medical information
- Unnecessary personally identifiable information
- Law-enforcement-sensitive information
- Detailed tactical information
- Attorney-client or attorney work-product material
- Cybersecurity information
- Trade secrets
- Information protected by another state or federal law
- Other information requiring restricted handling or release review

## 10.3. Legal Status

Placement of a record within the Restricted Records folder does not independently establish that the record is exempt from public disclosure.

The content of the record and applicable legal authority determine whether the record:

- May be released;
- Requires redaction;
- Requires legal review;
- Must be withheld; or
- May be released only to specified persons.

Not all restricted records qualify under R.C. 149.433. Records involving medical, personal, law-enforcement, legal, or other protected information may be governed by different legal authority.

Questions regarding disclosure, redaction, or withholding should be coordinated with the County's designated records official or legal counsel.

### 10.4. Parent Incident Folder

The parent incident folder will not normally be labeled FOUO or restricted merely because it contains a restricted-records subfolder.

The standard incident name will remain:

- YYYYMMDD Short Incident Name

Restricted records will be separated under Folder 99. Administrative handling labels do not independently create an exemption from public disclosure.

When nearly the entire incident file requires restricted handling, the EMA Director may apply an appropriate administrative handling designation after reviewing the nature of the records and applicable authority.

### 10.5. Release Review

Restricted records will be excluded from routine unrestricted source packages, broad stakeholder access, and public-release packages.

Redacted or releasable copies may be maintained under:

```
99 - Restricted Records
└── 05 - Release Review and Redacted Copies
```

The original record will be preserved separately.

## 11. Incident Termination and D4H Closeout

Operational termination and records closeout are related but separate actions. An incident may terminate operationally while records collection, export, organization, and after-action preparation continue.

### 11.1. Termination

The EMA Director will determine when EMA monitoring, response, coordination, or recovery operations terminate or transition to another phase.

Before changing the incident to a closed or terminated status, the record should identify:

- Final known conditions
- Final operational status
- Remaining monitoring requirements
- Outstanding assignments
- Unresolved resource issues
- Required follow-up actions
- Organizations responsible for continuing work
- Date and time of termination or transition

A final Log of Events entry will document the termination or transition.

## 11.2. Closeout Responsibility

The EMA Director is responsible for the completion and verification of incident-record closeout.

This responsibility includes:

- Confirming final D4H entries
- Reviewing the final Situation Report
- Reviewing the complete Log of Events
- Confirming the incident status
- Exporting required D4H products
- Consolidating records on the network drive
- Verifying folder and file organization
- Identifying missing or incomplete records
- Contacting participating organizations for documentation
- Separating restricted records
- Confirming the source package is ready for after-action review
- Other personnel may assist, but final responsibility remains with the EMA Director.

## 11.3. Required D4H Exports

The following D4H records will be exported, printed, or otherwise saved when used:

- Incident overview or incident details
- Final Situation Report
- Complete Log of Events
- Final versions of status boards
- Submitted forms and reports
- Maps or map exports
- Resource requests
- Task or assignment records
- D4H attachments not already preserved elsewhere
- Final termination or closeout entry
- Other operational products needed to understand the incident

Blank forms, unused boards, inactive products, and empty pages do not need to be exported solely to document that they were available.

## 11.4. Final Situation Report and Log

The final Situation Report will be clearly identified and saved under the applicable incident folder.

The final Log of Events will be:

- Exported to PDF;
- Saved to the network-drive incident folder;
- Printed for the central incident records file when practical; and
- Preserved with earlier shift-end copies.

## 11.5. Missing Records

The EMA Director will identify significant missing records and make reasonable attempts to obtain them from participating organizations.

Requests may include:

- Partner reports
- Incident logs
- Photographs
- Forms
- Emails

- Resource documentation
- Technical reports
- Maps
- Public information products
- Other records necessary to understand the organization's involvement

A missing record that cannot be obtained should be documented as a source limitation when it materially affects the incident record or After-Action Report.

# 12. Permanent Network-Drive Incident Record

After required D4H information has been exported and supporting records have been consolidated, the network-drive incident folder becomes the permanent incident record.

## 12.1. Permanent Record Contents

The permanent incident record should contain, as applicable:

- Final D4H exports
- Situation Report snapshots
- Shift-end and final Log of Events copies
- Formal communications
- Partner reports
- Maps
- Photographs and videos
- Public alerts and information products
- Resource records
- Damage-assessment records
- Weather or technical information
- Forms and spreadsheets
- Restricted records
- Final After-Action Report
- Other records necessary to document the incident



## 12.2. Working and Final Files

Draft, working, and final files may be preserved when they document a meaningful review, decision, or change.

Unnecessary duplicates, temporary downloads, blank forms, and files with no operational or administrative value should be removed during closeout.

Original source files will not be deleted merely because a converted, summarized, or final version exists.

## 12.3. Annual Archive

Completed incident folders may remain in the active-response directory until records closeout and after-action requirements are completed.

At the appropriate archive point, the folder will be moved into the applicable annual response folder.

Example:

```
2026 Responses
└── 20260710 Sabina Spill Response
```

Moving an incident into the annual folder indicates that active records work is complete. It does not authorize destruction of the record.

### 12.4. D4H Record Retention

Closing and exporting an incident does not authorize deletion of the incident from D4H.

D4H records will be retained or disposed of only under approved system-administration procedures, applicable records-retention schedules, and direction from the EMA Director.

## 13. After-Action Report Source Package

The permanent incident folder will serve as the primary source package for development of the After-Action Report.

### 13.1. Readiness for After-Action Review

Before beginning the After-Action Report process, the EMA Director will confirm that the available record is sufficiently complete to support review.

The source package should include, as applicable:

- Final D4H Log of Events
- Final Situation Report
- Earlier Situation Report snapshots
- Incident overview
- Relevant status boards
- Forms
- Maps
- Alerts
- Public information products
- Partner reports
- Formal communications
- Resource records
- Photographs
- Technical products
- Other records needed to understand the incident

After-action work should not be delayed solely because every possible record is unavailable. Significant missing information will be identified as a source limitation.

### 13.2. Use of the AAR Builder

The current EMA AAR Builder Prompt may be used after the record has been consolidated and reviewed.

The AAR process should:

- Review the permanent incident record;
- Identify the sources used;
- Identify missing or conflicting information;
- Preserve significant actions and impacts;
- Evaluate sustained practices and observations;
- Avoid unsupported conclusions;
- Protect restricted information; and
- Produce the final After-Action Report for the incident file.

The AAR Builder Prompt should be reviewed following completion of this SOG to ensure its records-location and source-loading instructions match the D4H-to-network-drive lifecycle established here.

### 13.3. Final After-Action Report

The final approved After-Action Report will be saved under:

- 10 - Closeout and AAR

Recommended filenames include:

- (Draft) YYYYMMDD Incident Name After-Action Report.docx
- (Final) YYYYMMDD Incident Name After-Action Report.pdf

Supporting working material may be retained when it documents a significant review, correction, or decision.

## 14. Continuity and Technology Disruption

Clinton County EMA maintains identified EOC locations but does not maintain a permanently equipped EOC awaiting activation. EOC operations may be established using deployable equipment, communications systems, position support kits, printed references, and incident-specific materials.

### 14.1. Offline Record Continuity

Incident records will be protected against the possible loss of:

- D4H access
- Internet service
- Network-drive access
- Electrical power
- Printing capability
- Computer equipment
- Primary EOC workspace
- Other technology resources

Continuity measures include:

- Shift-end Log of Events copies
- Situation Report snapshots
- Network-drive storage
- Approved offline electronic storage
- Printed central incident records
- Preservation of original source documents
- Paper fallback methods when needed
- 14.2. Portable Printing Capability

A portable laser printer should be maintained for deployable EOC operations when available.

The printer and supporting equipment should:

- Be suitable for operational use;
- Be stored in a protective transport case;
- Be capable of deployment to identified EOC locations;
- Include required cables, toner, paper, and power accessories; and
- Be maintained in a ready condition.

Until the portable printer is procured and available, the electronic fallback process in Section 8.5 will be used.

### 14.3. EOC Position Support Kits

Each designated EOC functional position may be assigned an EOC Position Support Kit maintained in a labeled position bin.

Position Support Kits may contain:
- Position checklists
- Plans and reference materials
- Administrative supplies
- Pens, markers, and highlighters
- Notepads and scratch paper
- Clipboards
- Stapler and related supplies
- Tabletop position nameplate
- Approved electronic continuity resources
- Other position-specific material

The kits support rapid establishment of a deployable EOC but do not replace the central incident records file.

### 14.4. Offline Electronic Storage

EMA intends to maintain approved USB hard drives or similar portable storage devices for EOC continuity when available.

Portable storage used for incident records should be:
- Authorized by the EMA Director;
- Encrypted when practical;
- Clearly labeled;
- Assigned and tracked;
- Protected from unauthorized access;
- Updated through an established process; and
- Stored in the designated EOC Position Support Kit or other approved location.

Security, access, custody, and encryption requirements will be addressed under 08.06.3: SOG – D4H Security and Access Controls and applicable technology procedures.

## 15. Records Quality Control

Incident records will be reviewed for accuracy, completeness, usefulness, and proper handling before final closeout.

### 15.1. Documentation Standards

Incident documentation should be:

- Factual
- Concise
- Neutral
- Time-stamped when practical
- Supported by an identified source
- Written as close to the activity as practical
- Sufficient for a person not present to understand the event
- Free of unsupported conclusions or unnecessary opinion

### 15.2. Closeout Review

The EMA Director or designated reviewer should confirm:

- The D4H incident name and folder name match.
- Incident details are complete.
- The Situation Report reflects the final status.
- Required Situation Report snapshots were preserved.
- The Log of Events is complete and chronological.
- Shift-end continuity copies were preserved.
- Significant formal communications were saved.
- Original source files were preserved.
- Required D4H products were exported.
- Relevant photographs, maps, reports, and attachments are present.
- Restricted records are separated.
- Missing or conflicting records are identified.
- Draft and final products are clearly labeled.
- Unnecessary duplicates and temporary files are removed.
- The source package is ready for after-action review.

### 15.3. Corrections

Known errors should be corrected when the system and user permissions allow.

Corrections should not conceal the original record or create a misleading sequence. When a material correction cannot be made directly, a clarifying Log of Events entry or supporting memorandum should document:

- The incorrect or incomplete information;
- The corrected information;
- The source of the correction; and
- The date and person making the clarification.

## 16. Incident Records Closeout Sequence

The following sequence provides the basic closeout process:

1. Confirm operational termination or transition.
2. Enter the final Log of Events entry.

3. Update the D4H incident status.
4. Complete and save the final Situation Report.
5. Export the complete Log of Events.
6. Export all used status boards, forms, maps, resource requests, task records, and other required D4H products.
7. Print the final Log of Events and other required paper records when practical.
8. Save all exports to the matching network-drive incident folder.
9. Obtain significant missing documentation from participating organizations.
10. Preserve original source records and separate working copies.
11. Move restricted records under 99 - Restricted Records.
12. Review filenames, folder placement, drafts, final products, and duplicates.
13. Confirm that the permanent record is sufficiently complete.
14. Use the AAR Builder to develop the After-Action Report.
15. Save the final AAR under 10 - Closeout and AAR.
16. Move the completed incident folder into the applicable annual response folder.

# 17. Reference Documents

- This SOG should be used with the following documents and resources:
- 08.06: SOG – D4H Incident Manager Procedures
- 08.06.1: SOG – D4H User Account Setup and Maintenance
- 08.06.3: SOG – D4H Security and Access Controls
- 08.11: SOG – EMA Equipment and Technology Management
- Clinton County Emergency Operations Plan
- Applicable Clinton County records-retention schedules and policies
- EMA AAR Builder Prompt
- D4H Incident Management and Operations Center Help Center: https://help.d4h.com/collection/1-d4h-incident-management-operations-center

# 18. Review and Maintenance

This SOG should be reviewed annually or following:
- A significant incident;
- A major D4H system change;
- A network-drive or records-management change;
- A continuity or technology failure;
- Adoption of new EOC equipment;
- Revision of the Situation Report;
- Revision of the AAR Builder;
- Changes to applicable law or records-retention requirements; or
- Identification of a significant documentation gap.

The EMA Director is responsible for:
- Coordinating reviews and revisions;

- Maintaining version control;
- Confirming continued operational usefulness;
- Updating folder and file standards;
- Reviewing D4H closeout requirements;
- Coordinating legal or records review when necessary; and
- Ensuring related SOGs remain consistent.

Minor administrative corrections may be completed as needed. Significant procedural changes will be documented in the Record of Changes.

# RECORD OF CHANGES

This section documents significant revisions, updates, and modifications made to this document to support version control, operational continuity, and historical reference. Minor formatting, spelling, or administrative corrections that do not affect operational content may not be individually tracked.

Changes are recorded in chronological order and should include the date of revision, affected section(s), a brief summary of the update, and the individual or agency responsible for the change.

This document should be reviewed periodically and updated as operational requirements, authorities, procedures, or organizational structures change.

| Version | Date | Section(s) Updated | Summary of Changes | Updated By |
|---|---|---|---|---|
| 0.1 | 22 Jul 2026 | Initial Development | Began development of the D4H incident-records concept, including D4H documentation, supporting network-drive folders, and permanent incident-record requirements. | T. Breckel, EMA |
| 0.2 | 27 Jul 2026 | Purpose, Scope, and Records Lifecycle | Established application to all D4H incidents and defined D4H as the authoritative record during active operations and the network drive as the permanent record after termination. | T. Breckel, EMA |
| 0.3 | 31 Jul 2026 | Incident Creation, Naming, and Folder Templates | Established incident-creation authority, matching D4H and network-drive naming, hazard-specific template folders, common folder numbering, and chronological annual archiving. | T. Breckel, EMA |
| 0.4 | 3 Aug 2026 | Minimum Record, SITREP, Log Preservation, and Responsibilities | Established minimum D4H record requirements, Situation Report snapshots, shift-end Log of Events printing, continuity fallback procedures, and EMA Director closeout responsibility. | T. Breckel, EMA |
| 0.5 | 7 Aug 2026 | Communications, Source Records, and Restricted Records | Added formal and informal communications requirements, email-to-PDF preservation, original-source protection, restricted-record separation, and release-review guidance. | T. Breckel, EMA |
| 0.6 | 10 Aug 2026 | Incident Termination, D4H Exports, and Permanent Record | Added termination and closeout procedures, required D4H exports, missing-record follow-up, permanent network-drive record requirements, and annual archiving. | T. Breckel, EMA |
| 0.7 | 13 Aug 2026 | AAR Source Package and Continuity | Integrated the AAR Builder process, deployable EOC records support, portable printing | T. Breckel, EMA |

| Version | Date | Section(s) Updated | Summary of Changes | Updated By |
|---|---|---|---|---|
| | | | capability, EOC Position Support Kits, and planned offline storage. | |
| 0.8 | 15 Aug 2026 | Quality Control, Closeout Sequence, and References | Added records-quality standards, correction procedures, final closeout review, quick closeout sequence, references, and document-maintenance requirements. | T. Breckel, EMA |
| 1.0 | 17 Aug 2026 | All Sections | Completed full review and finalized the D4H Incident Records Management SOG for implementation. | T. Breckel, EMA |