

AI Incident Log

The Operator's Manual for Artificial Intelligence

Template Kit — Document 4 of 6

IMPORTANT — BEFORE YOU USE THESE TEMPLATES

These templates are starting points for organizations without existing AI governance. They are not legal documents and are not a substitute for qualified legal counsel. Review and adapt them to your specific jurisdiction, industry, and situation before use. Do not implement any policy, form, or checklist from this kit without professional review. The Operator's Manual for Artificial Intelligence makes no representations as to their completeness, accuracy, or fitness for any particular purpose.

Complete one record per incident. File a new record for each separate event. Do not combine multiple incidents in a single record. Retain completed records for a minimum of [enter period, e.g., 2 years] and store them in a location accessible to the Policy Owner and legal/compliance team.

An incident includes: accidental exposure of sensitive data to an AI tool, AI output that caused or could have caused harm, automated AI actions taken without proper review, a policy violation, an unexpected AI behavior affecting a real system or person, or any other AI-related event that required or should have required a response.

Incident Information

Field	Entry
Incident ID	[Use format: AI-YYYY-NNN, e.g., AI-2026-001]
Date of Incident	
Date Reported	
Time of Incident (if known)	
Reported By (Name and Title)	
Department / Team	
AI Tool or System Involved	
Vendor and Product Version (if known)	

What Happened

Describe the incident as factually as possible. State what occurred, not why it occurred or who is at fault. Include what the AI was asked to do, what it produced or did, and how the incident was discovered.

Description of Incident

--

Risk Assessment

Field	Entry
Risk Level (Low / Medium / High / Critical / Prohibited)	
Risk Ladder Category That Applies	
Was Sensitive Data Involved? (Yes / No / Unknown)	
If Yes — Data Type(s) Involved	
Was Data Exposed to the Vendor? (Yes / No / Unknown)	
Estimated Number of Records Affected	
Were Any Real-World Actions Taken Automatically? (Yes / No)	
If Yes — Describe the Actions	

Immediate Response

Record the actions taken immediately after the incident was identified. Include who took each action and when.

Action Taken	Taken By	Date / Time

Resolution

Field	Entry
Is the Incident Resolved? (Yes / No / Ongoing)	

Field	Entry
Date Resolved (if applicable)	
Root Cause (if determined)	
Corrective Action Taken or Planned	
Was a Policy or Process Change Required? (Yes / No)	
If Yes — Describe the Change	
Was Legal, Compliance, or HR Notified? (Yes / No / N/A)	
Was the AI Vendor Notified? (Yes / No / N/A)	
Was a Regulatory Authority Notified? (Yes / No / N/A)	

Follow-Up Required

	Required Action	Done
☐	Policy update required — assign to: _____	
☐	Training required — assign to: _____	
☐	Vendor review required — assign to: _____	
☐	Technical control change required — assign to: _____	
☐	Legal review required — assign to: _____	
☐	Regulatory notification required — deadline: _____	
☐	Insurance notification required — assign to: _____	

Approval and Filing

Record Completed By	Date
Reviewed By (Manager)	Date
Approved By (Policy Owner)	Date
Filed In	Retention Date