

Specimen — illustrative example

Halden Precision Manufacturing is a fictional organisation. This document comes from the scenario described on riskwoven.com/examples, and is not an assessment of any real entity. It is advisory output to support your own decisions: not legal advice, not a certification, and not an audit.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

AI Incident Response Procedure

Halden Precision Manufacturing

Document type	procedure	Version	1.0 Draft
Owner	Plant Operations Manager	Customer decision role	Chief Operating Officer
Effective date	Upon customer release	Review cycle	Annual
Framework basis	RiskWoven AI practical best practices		
Jurisdiction	Ontario, Canada		
Prepared for	Halden Precision Manufacturing	Industry	Precision manufacturing
Organization size	101-500	Locations	Not specified

Advisory draft for accountable-owner and professional review. Validate legal, regulatory, contractual, technical and operational requirements before customer release. This is not legal advice, a certification, or a compliance determination.

1. Purpose

This procedure establishes the ordered steps Halden Precision Manufacturing follows to respond to AI incidents affecting its vision-based defect detection and predictive maintenance

systems. It covers receiving and triaging reports, containing harm, identifying affected outputs and decisions, correcting or reversing those decisions where feasible, assessing notification duties, validating remediation, and capturing lessons learned.

2. Scope

This procedure applies to all AI incidents involving:

- The vision models on the production line that flag surface defects and dimensional deviation.
- The predictive maintenance model that forecasts bearing and spindle failure from vibration data.

It covers harmful outputs, data exposure, misuse, model drift, and control failures affecting these systems. It does not replace the Security Incident Response Procedure or the Privacy Breach Response Procedure; where an AI incident also constitutes a security incident or privacy breach, both procedures run in parallel with this one.

3. Definitions

AI incident: Any event where an AI system produces a harmful output, exposes data contrary to policy, is used outside its permitted purpose, drifts from validated performance, or experiences a control failure that could affect the reliability of its outputs.

Harmful output: An AI system output that causes or could cause personnel safety risk, a defect escape reaching a customer, damage to equipment, loss of confidential customer part geometry, or a decision that violates the prohibition on assessing operator performance.

Model drift: A change in an AI model's accuracy, precision, recall, or output distribution compared to its validated baseline, whether caused by changes in input data, operating conditions, or model degradation.

Affected decision: Any production, quality, or maintenance decision that relied on an AI output during the period the incident was active and undetected.

Containment: The act of pausing, restricting, or isolating an AI system to prevent further harm while investigation and remediation proceed.

4. Roles and Responsibilities

Incident Lead (Plant Operations Manager): Owns this procedure, coordinates the response, makes containment decisions, and maintains the incident record.

Executive Decision-Maker (Chief Operating Officer): Reviews the incident record for Critical and High severity incidents, decides on extended containment or system restoration, and reviews lessons learned.

Quality Manager: Assesses whether a defect escape may have reached a customer, determines customer notification requirements, and reviews corrective actions.

Controls Engineer: Executes technical containment, investigates root cause, implements remediation, and validates system restoration.

Health and Safety Coordinator: Assesses any personnel safety implications and determines whether safety reporting obligations apply.

Chief Executive Officer: Sole authority for external communications beyond customer quality notifications.

Any employee: Reports suspected AI incidents through the channels in Section 5.

5. Receive and Triage Reports

Step 5.1 – Any employee: Report a suspected AI incident immediately to the shift supervisor or directly to the Plant Operations Manager. Reports may be made verbally, by email, or through the plant's incident reporting system.

Step 5.2 – Shift Supervisor (if first contact): Record the report with the time received, the system involved, the nature of the suspected issue, and the reporter's name. Notify the Plant Operations Manager within a target time set by Halden Precision Manufacturing for any report involving personnel safety, a suspected defect escape, or loss of the plant network; 15 minutes is a recommended starting point.

Step 5.3 – Plant Operations Manager: Acknowledge the report. For Critical severity, acknowledge within 15 minutes of receipt. For High, Medium, and Low severity, acknowledge within a target time set by Halden Precision Manufacturing and recorded in the AI Risk Management Standard; one hour is a recommended starting point for High severity and is not derived from a cited control.

Step 5.4 – Plant Operations Manager: Assign a severity level using the following criteria:

- Critical: Personnel safety affected, defect escape reaching a customer, or loss of the plant network.
- High: Line stoppage beyond 4 hours, or model failure allowing defective parts through undetected.
- Medium: Single-cell fault with production continuing.
- Low: Contained fault with no production impact.

Step 5.5 – Plant Operations Manager: Open an incident record. Record the incident identifier, date and time reported, reporter, system affected, initial severity, and initial description. The incident record is the single source of truth for all subsequent steps.

6. Contain the Incident

Step 6.1 – Plant Operations Manager: Determine whether continued operation of the AI system could increase harm. If yes, proceed to Step 6.2. If no, proceed to Section 7.

Step 6.2 – Plant Operations Manager: Decide on the containment action:

- Pause: Stop the AI system entirely; manual inspection or maintenance planning takes over.
- Restrict: Limit the AI system to a subset of lines, cells, or functions.
- Isolate: Disconnect the AI system from downstream integrations while allowing continued data collection for investigation.

Step 6.3 – Controls Engineer: Execute the containment action. Record the action taken, the time executed, and the systems or lines affected in the incident record.

Step 6.4 – Plant Operations Manager: For Critical severity, escalate to the Chief Operating Officer within 30 minutes of the initial report. For High severity, escalate within a target time set by Halden Precision Manufacturing; two hours is a recommended starting point and is not derived from a cited control.

Step 6.5 – Plant Operations Manager: Notify the Quality Manager immediately if the incident involves the vision defect detection system and a defect escape is suspected.

Step 6.6 – Plant Operations Manager: Notify the Health and Safety Coordinator immediately if the incident involves any personnel safety risk.

7. Identify Affected Scope

Step 7.1 – Controls Engineer: Determine the incident window—the period from when the incident began (or is reasonably estimated to have begun) to when containment was executed.

Step 7.2 – Controls Engineer: Identify affected outputs. For the vision defect detection system, this includes all accept and reject decisions during the incident window. For the predictive maintenance model, this includes all failure predictions and non-predictions during the incident window.

Step 7.3 – Controls Engineer: Identify affected data. Determine whether any data was exposed, corrupted, or transmitted contrary to policy. For customer part geometry, confirm whether any data left the plant network.

Step 7.4 – Quality Manager: Identify affected decisions. Cross-reference the affected outputs against:

- Parts accepted and shipped during the incident window.
- Parts scrapped based on AI rejection during the incident window.
- Maintenance actions taken or deferred based on predictions during the incident window.

Step 7.5 – Plant Operations Manager: Identify affected integrations and suppliers. Determine whether any AI outputs were transmitted to downstream systems, customer portals, or third-party maintenance providers during the incident window.

Step 7.6 – Plant Operations Manager: Identify affected people. For these systems, no personal data is processed; confirm this remains true for the incident. If personal data was involved contrary to policy, invoke the Privacy Breach Response Procedure in parallel.

Step 7.7 – Plant Operations Manager: Record all findings in the incident record.

8. Correct or Reverse Affected Decisions

Step 8.1 – Quality Manager: For the vision defect detection system, determine which accepted parts shipped during the incident window require customer notification or recall assessment. A suspected defect escape triggers customer notification assessment within a target time set by Halden Precision Manufacturing; 4 hours from identification is a recommended starting point.

Step 8.2 – Quality Manager: For parts scrapped based on AI rejection during the incident window, determine whether re-inspection is feasible and cost-justified. If yes, arrange re-inspection and record results.

Step 8.3 – Plant Operations Manager: For the predictive maintenance model, review all predictions and non-predictions during the incident window with the maintenance planner. Determine whether any maintenance was incorrectly deferred or incorrectly performed.

Step 8.4 – Plant Operations Manager: For incorrectly deferred maintenance, schedule immediate inspection of the affected equipment. For incorrectly performed maintenance, assess whether reversal or additional action is required.

Step 8.5 – Quality Manager: Assess customer notification duties. If a defect escape may have reached a customer, prepare a notification in accordance with customer agreements and quality management requirements. The Chief Executive Officer reviews any external communication before release.

Step 8.6 – Plant Operations Manager: Assess regulatory notification duties. Consult the Health and Safety Coordinator for safety-related incidents. Consult the Human Resources Manager if personal data was involved. Record the assessment and any notifications made in the incident record.

Step 8.7 – Plant Operations Manager: Record all corrective actions, their completion status, and their outcomes in the incident record.

9. Investigate Root Cause

Step 9.1 – Controls Engineer: Collect evidence. Preserve logs, model inputs, model outputs, configuration snapshots, and any telemetry relevant to the incident window. Store evidence in a location accessible for review but protected from modification.

Step 9.2 – Controls Engineer: Analyse the evidence to determine root cause. Categories include:

- Model drift: Change in input data distribution, sensor degradation, or environmental change.
- Data issue: Corrupted, missing, or mislabelled input data.
- Configuration error: Incorrect thresholds, parameters, or integration settings.

- Control failure: Bypass of human review, failure of sampling checks, or access control breach.
- Misuse: Use of the system outside its permitted purpose, including any use to assess operator performance.
- External factor: Supplier system failure, network issue, or upstream data quality problem.

Step 9.3 – Controls Engineer: Document the root cause, contributing factors, and the evidence supporting the conclusion in the incident record.

Step 9.4 – Plant Operations Manager: If the root cause involves a third-party AI supplier, invoke the Third-Party AI Review Procedure to assess supplier performance and contractual obligations.

10. Remediate and Restore

Step 10.1 – Controls Engineer: Develop a remediation plan addressing the root cause. The plan must specify the actions, responsible parties, and target completion dates.

Step 10.2 – Plant Operations Manager: Review the remediation plan for Critical and High severity incidents with the Chief Operating Officer before execution.

Step 10.3 – Controls Engineer: Execute the remediation plan. Record each action completed and the date of completion in the incident record.

Step 10.4 – Controls Engineer: Validate that the remediation resolves the root cause. Validation must include:

- For model drift: Re-validation against the baseline performance metrics recorded in the AI Risk Management Standard.
- For data issues: Confirmation that input data quality meets documented requirements.
- For configuration errors: Review of configuration against documented standards.
- For control failures: Test of the restored control to confirm it operates as designed.

Step 10.5 – Controls Engineer: Document validation results in the incident record.

Step 10.6 – Plant Operations Manager: Decide on system restoration. For Critical and High severity incidents, the Chief Operating Officer reviews the validation results and decides whether to restore the system to full operation.

Step 10.7 – Controls Engineer: Restore the system to operation. Record the restoration time and any residual restrictions in the incident record.

11. Update Risk Assessment

Step 11.1 – Plant Operations Manager: Within a period set by Halden Precision Manufacturing after incident closure (30 days is offered as a starting point), review the AI Risk Management Standard entry for the affected system.

Step 11.2 – Plant Operations Manager: Determine whether the incident reveals a risk not previously identified, a risk rated too low, or a control rated more effective than it proved to be.

Step 11.3 – Plant Operations Manager: If the risk assessment requires update, revise the entry in the AI Risk Management Standard. Record the change, the rationale, and the incident that prompted it.

Step 11.4 – Plant Operations Manager: If the incident reveals a gap in the AI Acceptable Use Policy, the AI Governance and Accountability Policy, or any related standard, raise the gap with the Chief Operating Officer for inclusion in the next scheduled review of that document.

12. Document Lessons Learned

Step 12.1 – Plant Operations Manager: Within a period set by Halden Precision Manufacturing after incident closure (30 days is offered as a starting point), convene a lessons-learned review for Critical and High severity incidents. Attendees include the Controls Engineer, Quality Manager, and any other parties involved in the response.

Step 12.2 – Plant Operations Manager: Document the following in the lessons-learned record:

- What worked well in the response.
- What delayed detection, containment, or remediation.
- What changes to this procedure, related procedures, or controls would improve future response.
- Any training or awareness needs identified.

Step 12.3 – Plant Operations Manager: Present the lessons-learned record to the Chief Operating Officer for review.

Step 12.4 – Plant Operations Manager: Track any improvement actions arising from the lessons-learned review to completion. Record completion in the incident record.

Step 12.5 – Quality Manager: For incidents involving the vision defect detection system, incorporate relevant lessons into the quality management review cycle.

SPECIMEN

13. Incident Record Retention

Step 13.1 – Plant Operations Manager: Retain the complete incident record, including all evidence, root cause analysis, remediation documentation, validation results, and lessons learned, in accordance with the Records Retention and Disposal Policy.

Step 13.2 – Plant Operations Manager: Ensure the incident record is accessible for audit, regulatory inquiry, and future incident investigation for the retention period specified in the Records Retention and Disposal Policy.

14. Metrics and Reporting

The Plant Operations Manager tracks and reports the following metrics at a frequency set by Halden Precision Manufacturing (quarterly is offered as a starting point):

- AI incidents contained within target: Percentage of incidents where containment was executed within the target time for the assigned severity level.
- Affected decisions reviewed and corrected: Number of affected decisions identified, number reviewed, and number corrected or reversed.
- Percentage of required reviews completed on time: For Critical and High severity incidents, percentage where Chief Operating Officer review occurred within the target window.
- Number of approved exceptions past their expiry date: Count of any temporary containment restrictions or workarounds that remain in place beyond their documented expiry.
- Number of material control failures and overdue corrective actions: Count of incidents classified as control failures, and count of remediation actions past their target completion date.

The Plant Operations Manager reports these metrics to the Chief Operating Officer. The Chief Operating Officer determines whether to include them in broader operational or board reporting.

15. Related Documents

- AI Governance and Accountability Policy

- AI Risk Management Standard
- AI Acceptable Use Policy
- Security Incident Response Procedure
- Privacy Breach Response Procedure
- Third-Party AI Review Procedure
- Third-Party Risk Management Policy
- Data Classification and Handling Standard
- Records Retention and Disposal Policy
- Business Continuity Policy
- Information Security Policy
- Privacy and Personal Information Policy

16. Review and Maintenance

The Plant Operations Manager reviews this procedure annually or following any Critical severity AI incident, whichever is sooner. The Chief Operating Officer reviews proposed changes before they take effect. The Quality Manager is consulted on any changes affecting quality or customer notification processes.

Owner review items

The drafting process identified the following in the supplied answers. Resolve each before customer release.

Type	Detail	Where
gap	The information supplied does not include the text of the AI Risk Management Standard, so this procedure references it by title but cannot confirm the specific baseline performance metrics, risk ratings, or control effectiveness ratings recorded there. Halden Precision Manufacturing must verify that the AI Risk Management Standard contains the entries this procedure assumes.	Sections 10, 11
gap	The information supplied does not include the text of the Records Retention and Disposal Policy, so this procedure defers to it for retention periods without stating a specific duration. Halden Precision Manufacturing must confirm that policy specifies a retention period for AI incident records.	Section 13
gap	The information supplied does not specify acknowledgement targets for High, Medium, and Low severity incidents, nor the escalation notification target for the shift supervisor. This procedure	Section 5, Steps 5.2

	offers one hour and 15 minutes respectively as recommended starting points; Halden Precision Manufacturing must set and document the actual targets.	and 5.3
gap	The information supplied does not specify an escalation target for High severity incidents. This procedure offers two hours as a recommended starting point; Halden Precision Manufacturing must set and document the actual target.	Section 6, Step 6.4
gap	The information supplied does not specify the customer notification assessment target for a suspected defect escape. This procedure offers 4 hours as a recommended starting point; Halden Precision Manufacturing must set and document the actual target.	Section 8, Step 8.1
gap	The information supplied does not specify the timeframe for updating the risk assessment or completing lessons-learned documentation after incident closure. This procedure offers 30 days as a starting point for each; Halden Precision Manufacturing must set and document the actual targets.	Sections 11, 12
gap	The information supplied does not specify the reporting frequency for incident metrics. This procedure offers quarterly as a starting point; Halden Precision Manufacturing must set and document the actual frequency.	Section 14
vague	The customer answers state that privacy requests are answered 'within the period the applicable law requires' but do not identify the specific statute or period. If an AI incident involves personal data contrary to expectation, the Privacy Breach Response Procedure governs notification timelines, but Halden Precision Manufacturing should confirm with legal counsel which privacy legislation applies.	Section 8, Step 8.6

Information the organization must supply

These values were not available from the intake and are required before this document can operate:

- Target time for the shift supervisor to notify the Plant Operations Manager for Critical-trigger reports (15 minutes is a recommended starting point in Step 5.2).
- Acknowledgement targets for High, Medium, and Low severity AI incidents (one hour is a recommended starting point for High severity in Step 5.3).
- Escalation target for High severity AI incidents (two hours is a recommended starting point in Step 6.4).
- Customer notification assessment target for a suspected defect escape (4 hours is a recommended starting point in Step 8.1).
- Timeframe for updating the risk assessment after incident closure (30 days is a recommended starting point in Section 11).

- Timeframe for completing lessons-learned documentation after incident closure (30 days is a recommended starting point in Section 12).
- Reporting frequency for AI incident metrics (quarterly is a recommended starting point in Section 14).
- Confirmation that the AI Risk Management Standard contains baseline performance metrics for each AI system, against which post-incident validation can be performed.
- Confirmation that the Records Retention and Disposal Policy specifies a retention period for AI incident records.
- Confirmation with legal counsel regarding which Ontario or federal privacy legislation applies to employee personal information, in case an AI incident unexpectedly involves such data.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.