

Specimen — illustrative example

Pemberton Home Goods is a fictional organisation. This document comes from the scenario described on [riskwoven.com/examples](https://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.

# Security Incident Response Procedure

Pemberton Home Goods

|                   |                                       |                        |                         |
|-------------------|---------------------------------------|------------------------|-------------------------|
| Document type     | procedure                             | Version                | 1.0 Draft               |
| Owner             | Director of Digital                   | Customer decision role | Chief Operating Officer |
| Effective date    | Upon customer release                 | Review cycle           | Annual                  |
| Framework basis   | RiskWoven AI practical best practices |                        |                         |
| Jurisdiction      | Canada and the United States          |                        |                         |
| Prepared for      | Pemberton Home Goods                  | Industry               | Retail                  |
| 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 tells Pemberton Home Goods staff exactly what to do when a security incident occurs. It covers detection, triage, containment, investigation, recovery, and the post-incident

review. Following it protects customers, loyalty members, and employees whose information Pemberton holds, keeps the Shopify Plus storefront and point-of-sale estate running, and meets Pemberton's obligations under applicable Canadian and United States privacy and security law.

## 2. Scope

This procedure applies to every Pemberton Home Goods employee, contractor, and third-party service provider who operates, supports, or accesses Pemberton systems or information. It covers all systems and information assets, including the Shopify Plus storefront and customer accounts, the personalisation platform, the order management and fulfilment systems, the loyalty database, and the point-of-sale estate in stores.

This procedure does not duplicate the Privacy Breach Response Procedure or the AI Incident Response Procedure. Where an incident involves personal information, the Incident Lead must engage the Privacy Breach Response Procedure in parallel. Where an incident involves an AI system, the Incident Lead must engage the AI Incident Response Procedure in parallel. This procedure governs the security response; those procedures govern their respective specialist tracks.

## 3. Definitions

**Event.** Any observable occurrence on a Pemberton system or network. Most events are routine. An event becomes an incident when it meets the criteria in Section 5.

**Incident.** A confirmed or strongly suspected event that has caused, or could cause, harm to Pemberton systems, information, customers, or operations. An incident triggers this procedure.

**Severity.** The classification assigned to an incident based on its business, data, safety, legal, and service impacts. Severity determines response speed and escalation path. The four levels are defined in Section 5.

**Containment.** The actions taken to stop an incident from spreading or causing further harm, while preserving evidence and keeping critical business services running to the extent possible.

**Evidence.** Any record, log, file, screenshot, device, or other artefact that documents what happened, when, and how. Evidence must be preserved in a way that maintains its integrity and supports any subsequent investigation or legal proceeding.

**Breach.** An incident that results in the unauthorised access to, disclosure of, loss of, or destruction of personal information or other sensitive Pemberton data. A breach triggers notification assessment under Section 9 and, where personal information is involved, the Privacy Breach Response Procedure.

## 4. Roles and Responsibilities

**Any Pemberton staff member or contractor.** Reports a suspected event immediately through the channels in Section 6. Does not attempt to investigate or remediate without instruction from the IT Manager.

**IT Manager (Incident Lead).** Receives all reports, makes the initial severity classification, leads the technical response, assigns tasks to the response team, maintains the incident record, and escalates as required. Holds on-call responsibility for the storefront outside office hours.

**Director of Digital (Document Owner).** Owns this procedure. Authorises customer communications during an incident. Reviews this procedure annually and after any Critical incident.

**Chief Operating Officer.** Receives executive escalation for all Critical and High incidents. Makes decisions on business continuity, public communications, and regulatory notification. Acts as the final decision-maker on containment actions that affect trading operations.

**Finance Director.** Receives immediate notification of any incident touching the payment path or involving fraud. Leads the payment-specific response track in coordination with the Incident Lead.

**Privacy Officer.** Assesses whether an incident constitutes a breach of personal information. Leads the privacy notification track in parallel with the security response, using the Privacy Breach Response Procedure.

**Merchandising Manager.** Participates in post-incident review. Reviews this procedure annually alongside the Director of Digital.

**Third-party service providers.** Must report suspected incidents affecting Pemberton systems or data to the IT Manager immediately, in accordance with their contractual obligations and the Third-Party Risk Management Policy.

## 5. Severity Classification

The IT Manager assigns severity at first triage and may revise it as the incident develops. Severity is based on the combined business, data, safety, legal, and service impact at the time of classification.

**Critical.** Any of the following: confirmed or suspected exposure of customer, loyalty member, or employee personal information; a compromise of any system in the payment path; a pricing error published at scale across the storefront. Response targets for Critical incidents are an organisational parameter that Pemberton must set and record in the Incident Response Targets document maintained by the IT Manager. Starting-point recommendations, which are not derived from any cited control, are: acknowledge within 15 minutes of report receipt; escalate to the Chief Operating Officer within 30 minutes; correct a published-pricing error or hold the storefront within 1 hour.

**High.** Any of the following: a storefront outage during a peak trading period; the personalisation platform displaying one customer's data to another customer. Response targets are an organisational parameter that Pemberton must set and record in the Incident Response Targets document. A starting-point recommendation, not derived from any cited control, is 30 minutes from report receipt for acknowledgement.

**Medium.** A degraded recommendation or personalisation service that does not expose personal data and does not prevent customers from completing purchases. Response targets are an organisational parameter that Pemberton must set and record in the Incident Response Targets document. A starting-point recommendation, not derived from any cited control, is 2 hours from report receipt for acknowledgement.

**Low.** An isolated content error on the storefront or in marketing material that does not affect personal data, payment systems, or trading availability. Response targets are an organisational parameter that Pemberton must set and record in the Incident Response Targets document. A starting-point recommendation, not derived from any cited control, is next business day for acknowledgement.

The IT Manager records the severity classification, the factors considered, and the time of classification in the incident record at the point of triage.

## 6. Reporting Channels

Pemberton must maintain at least two monitored reporting channels: one for staff and one for external parties. The specific channel details — email addresses, phone numbers, ticketing system links — are maintained by the IT Manager and published in the internal staff directory and on the supplier portal.

Every report received through any channel must be logged immediately with:

- the date and time the report was received;
- the channel through which it arrived;
- the name and role of the person who made the report, or a description of the source if anonymous;
- a verbatim or close summary of what was reported.

This log entry is the first record in the incident record. It must not be altered after creation; corrections are added as a new dated entry.

The IT Manager is responsible for ensuring both channels are monitored continuously. Outside office hours (Monday to Friday 08:00 to 18:00 Eastern), on-call cover for the storefront must be able to receive and act on a Critical report within the acknowledgement target set by Pemberton for Critical incidents.

## 7. Step-by-Step Response

The steps below are numbered. Each step names the role responsible. Steps run in sequence unless a step explicitly permits parallel action.

### Phase 1: Detection and Initial Report

Step 1 — Any staff member or contractor.

On observing or suspecting a security event, report it immediately through the designated reporting channel. Do not attempt to investigate, remediate, or discuss the event outside the reporting channel. Preserve any evidence you can access without altering it — for example, take a screenshot rather than closing a window.

Step 2 — IT Manager.

On receiving the report, log it as required by Section 6. Assign a unique incident reference number. Acknowledge receipt to the reporter within the target for the suspected severity level.

### Phase 2: Triage and Classification

Step 3 — IT Manager.

Assess the report against the severity criteria in Section 5. Consider business impact, data impact, safety impact, legal exposure, and service impact. Assign an initial severity level. Record the classification and the reasoning in the incident record.

Step 4 — IT Manager.

If the initial severity is Critical or High, notify the Chief Operating Officer immediately by phone. Do not wait for full investigation before escalating.

Step 5 — IT Manager.

If the incident touches the payment path or involves suspected fraud at any severity level, notify the Finance Director immediately by phone.

Step 6 — IT Manager.

If the incident may involve personal information of customers, loyalty members, or employees, notify the Privacy Officer immediately. The Privacy Officer opens a parallel track under the Privacy Breach Response Procedure.

Step 7 — IT Manager.

If the incident involves an AI system, notify the Director of Digital and open a parallel track

under the AI Incident Response Procedure.

### Phase 3: Evidence Preservation

Step 8 — IT Manager.

Before taking any containment action, preserve evidence. Actions to take:

- Capture system logs, access logs, and error logs in their current state. Export to a write-protected location.
- Take timestamped screenshots of any relevant system state.
- Record the chain of custody: who collected each item, when, and where it is stored.
- Do not power off affected systems unless the Chief Operating Officer directs it and the risk of further harm outweighs the loss of volatile evidence.

Step 9 — IT Manager.

Record every evidence item in the incident record with: item description, collection time, collector name, and storage location. This record is the chain of custody log.

### Phase 4: Containment

Step 10 — IT Manager, with Chief Operating Officer decision on actions affecting trading.

Contain the incident to stop further harm. Containment actions depend on the incident type and may include:

- Isolating affected systems from the network while keeping unaffected systems running.
- Revoking or suspending compromised credentials.
- Blocking a malicious IP address or traffic pattern.
- Taking a storefront feature offline if it is the source of harm — for example, holding the storefront to correct a published-pricing error within the Critical acknowledgement target.
- Engaging the relevant third-party provider to isolate their component.

For any containment action that will affect storefront availability or customer-facing services, the IT Manager must obtain the Chief Operating Officer's decision before acting, unless the delay would cause immediate and material additional harm. If the IT Manager acts without that decision, they must notify the Chief Operating Officer immediately after acting and record the reason for not waiting.

Step 11 — IT Manager.

Record each containment action in the incident record: action taken, time, person who took it, and the business service impact of the action.

### Phase 5: Investigation

**Step 12 — IT Manager.**

Conduct or direct the technical investigation. Determine:

- What happened and how.
- Which systems and data were affected.
- The timeline of the incident from first indicator to containment.
- Whether personal information was accessed, disclosed, or lost.
- Whether the payment path was compromised.
- The root cause.

**Step 13 — IT Manager.**

Document findings in the incident record as they emerge. Do not wait until the investigation is complete to record findings; record them in real time.

**Step 14 — Privacy Officer (parallel, if personal information is involved).**

Assess whether the incident constitutes a breach as defined in Section 3. Report the assessment to the Chief Operating Officer and the IT Manager. Proceed under the Privacy Breach Response Procedure for notification decisions.

**Phase 6: Notification Assessment****Step 15 — Chief Operating Officer, with Privacy Officer and Finance Director as required.**

Assess notification duties. Consider:

- Regulatory notification obligations under applicable Canadian and United States privacy and security law. The Privacy Officer leads this assessment for personal information. Pemberton's legal advisers must be engaged for any Critical incident involving personal data or payment systems.
- Payment card network notification obligations. The Finance Director leads this assessment.
- Customer notification. The Director of Digital leads drafting; the Chief Operating Officer decides whether and when to notify.
- Staff notification where their personal information is involved.
- Third-party notification where a supplier or partner is affected or needs to act.

**Step 16 — Director of Digital.**

Draft any customer-facing communication. The Chief Operating Officer reviews and decides on release. The IT Manager confirms the communication is technically accurate before release.

**Step 17 — IT Manager.**

Record all notification decisions in the incident record: what was decided, who decided it, when, and the reason.

## Phase 7: Recovery

Step 18 — IT Manager.

Before restoring any affected system to production, confirm:

- The root cause has been identified.
- The vulnerability or weakness that enabled the incident has been addressed or a compensating control is in place.
- Evidence has been preserved and the chain of custody is complete.
- The Chief Operating Officer has confirmed the decision to restore.

Step 19 — IT Manager.

Restore systems in a controlled sequence. Monitor restored systems closely for a period set by Pemberton and recorded in the Incident Response Targets document. Pemberton has not yet set this monitoring period; 24 hours post-restoration is offered as a starting-point recommendation and is not derived from any cited control.

Step 20 — IT Manager.

Record the restoration time, the steps taken, and the monitoring outcome in the incident record.

## Phase 8: Incident Closure

Step 21 — IT Manager.

Declare the incident closed when: systems are restored, monitoring shows no recurrence, all immediate notification obligations have been met, and the incident record is complete. Record the closure time.

Step 22 — IT Manager.

Notify the Chief Operating Officer and the Director of Digital that the incident is closed. Provide a summary of the incident, the actions taken, and the open post-incident actions.

## 8. Post-Incident Review

Step 23 — Director of Digital (convenes); IT Manager, Chief Operating Officer, Privacy Officer, Finance Director (as relevant), Merchandising Manager.

Convene a post-incident review within a period set by Pemberton and recorded in the incident record. Pemberton has not yet set this period; 10 business days from incident closure is offered as a starting-point recommendation for Critical and High incidents, and 20 business days for Medium and Low incidents; these are not derived from any cited control.

Step 24 — IT Manager.

Prepare a post-incident report covering:

- Incident timeline.
- Root cause.
- Effectiveness of detection, containment, and recovery.
- Evidence of any control failure.
- Actions taken and their outcomes.
- Proposed corrective actions, each with a named owner and a completion date.

Step 25 — Director of Digital.

Present the post-incident report to the review participants. Record the discussion, decisions, and agreed corrective actions in the review record.

Step 26 — IT Manager.

Track each corrective action to completion. Record completion in the incident record. Report overdue corrective actions to the Director of Digital and the Chief Operating Officer on a cycle set by Pemberton; monthly is offered as a starting-point recommendation and is not derived from any cited control.

Step 27 — Director of Digital.

If the review identifies a gap in this procedure, initiate an unscheduled review of this document. Do not wait for the annual review cycle.

## 9. Metrics

The IT Manager collects and reports the following metrics to the Director of Digital on a cycle set by Pemberton; quarterly is offered as a starting-point recommendation and is not derived from any cited control.

- **Time to acknowledge.** The elapsed time from report receipt to the IT Manager's acknowledgement, measured per incident and averaged across the reporting period. Reported separately for each severity level.
- **Time to contain.** The elapsed time from incident declaration to confirmed containment, measured per incident and averaged across the reporting period. Reported separately for each severity level.
- **Post-incident actions closed on time.** The number and percentage of corrective actions completed by their agreed due date in the reporting period.

- **Post-incident reviews completed on time.** The number and percentage of required post-incident reviews convened within the target period in the reporting period.
- **Exceptions past expiry.** The number of documented exceptions to this procedure or to related security controls that have passed their expiry date without renewal or closure.
- **Material control failures and overdue corrective actions.** The number of incidents in the reporting period that revealed a material control failure, and the number of corrective actions from any incident that are overdue at the time of reporting.

The Director of Digital presents these metrics to the Chief Operating Officer as part of the regular governance reporting cycle.

## 10. Evidence and Records

The IT Manager maintains an incident record for every incident from the moment of first report to closure and beyond. The incident record must contain at minimum:

- the unique incident reference number;
- the date and time of first report and the reporting channel;
- the reporter's name and role;
- the initial and any revised severity classification with reasoning;
- all escalation notifications with times and recipients;
- the chain of custody log for all evidence items;
- a chronological log of all decisions and actions with times and responsible persons;
- all notification decisions and their rationale;
- the closure declaration with time;
- the post-incident report and review record;
- the corrective action register with owners, due dates, and completion dates.

Incident records must be retained for a period set by Pemberton and consistent with the Records Retention and Disposal Policy. Pemberton has not yet set this retention period in the context of this procedure; the IT Manager must confirm the applicable period with the Director of Digital and the Privacy Officer before this procedure takes effect, taking into account applicable Canadian and United States legal requirements.

Access to incident records is restricted to the roles named in Section 4 and to any person the Chief Operating Officer specifically authorises. The IT Manager reviews access to the incident record store on a cycle set by Pemberton; annually is offered as a starting-point recommendation and is not derived from any cited control.

## 11. Relationship to Other Documents

This procedure operates within the framework set by the Information Security Policy. It does not restate the mandates in that policy.

Where an incident involves personal information, the Privacy Breach Response Procedure runs in parallel. The IT Manager and the Privacy Officer coordinate to avoid conflicting actions.

Where an incident involves an AI system, the AI Incident Response Procedure runs in parallel. The IT Manager and the Director of Digital coordinate the two tracks.

Where an incident threatens business continuity, the Business Continuity Policy governs the continuity response. The Chief Operating Officer coordinates between this procedure and the continuity response.

Data classification decisions during an incident follow the Data Classification and Handling Standard.

Third-party involvement in an incident is governed by the Third-Party Risk Management Policy and, where a third-party AI system is involved, the Third-Party AI Review Procedure.

Password resets and credential actions during an incident follow the Password and Authentication Standard.

System restoration actions follow the Patch Management Procedure where patching is part of the recovery.

## 12. Document Control

**Document owner:** Director of Digital.

**Review authority:** Chief Operating Officer.

**Review cycle:** Annual, and after every Critical incident, and after any post-incident review that identifies a gap in this procedure.

**Review record:** The Director of Digital maintains a review record showing the date of each review, the reviewer, the changes made, and the version number.

This procedure takes effect on the date it is recorded as reviewed by the Chief Operating Officer. The Director of Digital communicates changes to all staff and contractors in scope within a period set by Pemberton; 10 business days from the review record date is offered as a starting-point recommendation and is not derived from any cited control.

## Owner review items

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

| Type | Detail                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Where                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| gap  | Pemberton has not specified response targets for Critical, High, Medium, and Low severity incidents. The procedure marks all four sets of targets as organisational parameters that must be set and recorded in the Incident Response Targets document maintained by the IT Manager. Starting-point recommendations are provided in Section 5 for each level but are not derived from any cited control.                                                                                                                                                                                                                 | Section 5 — Severity Classification                                    |
| gap  | Pemberton has not specified the post-restoration monitoring period. The procedure marks this as an organisational parameter with a starting-point recommendation of 24 hours. The IT Manager must set and record this value.                                                                                                                                                                                                                                                                                                                                                                                             | Section 7, Step 19 — Recovery                                          |
| gap  | Pemberton has not specified the post-incident review convening period. The procedure marks this as an organisational parameter with starting-point recommendations of 10 business days for Critical and High and 20 business days for Medium and Low. The Director of Digital must set and record these values.                                                                                                                                                                                                                                                                                                          | Section 8, Step 23 — Post-Incident Review                              |
| gap  | Pemberton has not specified the retention period for incident records in the context of this procedure. The procedure directs the IT Manager to confirm the applicable period with the Director of Digital and the Privacy Officer, consistent with the Records Retention and Disposal Policy and applicable law. This must be resolved before the procedure takes effect. Legal advisers should confirm the applicable Canadian and United States requirements — candidates include PIPEDA, applicable provincial privacy legislation, and relevant US state privacy laws — but Pemberton's legal team must determine w | Section 10 — Evidence and Records                                      |
| gap  | Pemberton has not specified the physical locations of its stores or offices beyond 'Canada and the United States'. The jurisdiction of specific stores affects which privacy and breach notification laws apply to incidents at those locations. Pemberton's legal advisers should map store and office locations to the applicable regulatory regimes before this procedure takes effect.                                                                                                                                                                                                                               | Section 9 — Notification Assessment; Section 10 — Evidence and Records |
| gap  | The specific reporting channel details — email addresses, phone numbers, ticketing system links — are not supplied. The procedure directs the IT Manager to maintain and publish these. They must be in place and tested before the procedure takes effect.                                                                                                                                                                                                                                                                                                                                                              | Section 6 — Reporting Channels                                         |
| gap  | The metrics reporting cycle is marked as an organisational parameter with a starting-point recommendation of quarterly. The Director of Digital must set and record this cycle.                                                                                                                                                                                                                                                                                                                                                                                                                                          | Section 9 — Metrics                                                    |
| gap  | The corrective action overdue reporting cycle is marked as an organisational parameter with a starting-point recommendation of monthly. The IT Manager must set and record this cycle.                                                                                                                                                                                                                                                                                                                                                                                                                                   | Section 8, Step 26 — Post-Incident Review                              |
| gap  | The procedure references the Incident Response Targets document as the location where response targets for all severity levels and the post-restoration monitoring period                                                                                                                                                                                                                                                                                                                                                                                                                                                | Section 5 — Severity Classification                                    |

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                             |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
|     | will be recorded. Pemberton must create and maintain this document. It does not currently appear in the existing document inventory.                                                                                                                                                                                                                                                                                                                                           |                                                                             |
| gap | The customer answers name the Merchandising Manager as a reviewer of this procedure. The Merchandising Manager's operational connection to security incident response is not explained. The procedure includes the Merchandising Manager in the post-incident review and annual document review, which is consistent with the stated role. If the Merchandising Manager's involvement is intended to be broader, Pemberton should clarify and the procedure should be updated. | Section 4 — Roles and Responsibilities;<br>Section 8 — Post-Incident Review |
| gap | The procedure does not cover the scenario where the IT Manager is themselves the subject of or implicated in an incident. Pemberton should designate a named alternate Incident Lead for that scenario. The information supplied does not supply a name for this role.                                                                                                                                                                                                         | Section 4 — Roles and Responsibilities                                      |

## Information the organization must supply

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

- Response targets (acknowledgement and containment) for Critical, High, Medium, and Low severity incidents. Record these in the Incident Response Targets document maintained by the IT Manager.
- The post-restoration monitoring period following system recovery. Record this in the Incident Response Targets document.
- The post-incident review convening period for each severity level. Record these in the Incident Response Targets document.
- The retention period for incident records, confirmed by legal advisers against applicable Canadian and United States privacy and security law requirements. Record this in the Records Retention and Disposal Policy or as a schedule to it.
- The specific reporting channel details: email address, phone number, and ticketing system link for staff reporting; equivalent channels for external and third-party reporting. Publish these in the internal staff directory and supplier portal before the procedure takes effect.
- The metrics reporting cycle (the period on which the IT Manager reports metrics to the Director of Digital).
- The corrective action overdue reporting cycle (the period on which the IT Manager reports overdue corrective actions to the Director of Digital and Chief Operating Officer).
- The staff and contractor communication period following a procedure update.

- The access review cycle for the incident record store.
- A named alternate Incident Lead to act when the IT Manager is unavailable or implicated in an incident.
- A mapping of store and office locations to applicable Canadian and United States regulatory regimes, confirmed by legal advisers, to support notification assessment during incidents.
- Creation of the Incident Response Targets document referenced in Section 5, to hold the response targets for all severity levels and the post-restoration monitoring period.

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.

SPECIMEN