# Template: Post-Incident Reflection

Learn, adapt, and strengthen your digital foundations after an incident

|  |  |  |  |
| --- | --- | --- | --- |
| **Doc ID** | LS-TEM-0004 | **Owner** | Bryan Chetcuti |
| **Version** | V1.0 | **Status** | Approved |
| **Confidentiality** | Public | **Last Updated** | 2025-10-30 |
| **Approver** | Bryan Chetcuti | **Next Review** | 2026-06-30 |

## Change Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Author** | **Change** | **Version** |
| 2025-10-30 | Bryan Chetcuti | Approved | V1.0 |

# Template: Post-Incident Reflection

***Tip for Use:*** *After resolving any disruption - big or small* when something went wrong, almost went wrong, or exposed a gap in your digital trust practices - *take 15 minutes to capture what happened, what worked, and what could improve. Sharing these reflections helps build organisational resilience and transparency over time.*

## Basic Details

|  |  |
| --- | --- |
| **Incident title**  (A short, descriptive title) | e.g. “Email sent to wrong recipient” |
| **Date of incident** |  |
| **Date completed** |  |
| **Completed by**  (Name and role of person recording the reflection) |  |
| **Reviewed by**  (Optional - manager, peer, or governance lead) |  |

## What Happened

* Describe the event in plain language.
* Avoid blame - just explain the facts.

Example: “A member’s contact details were accidentally included in an internal report that was shared externally.”

## Impact

Outline who or what was affected.

* Individuals,
* Systems,
* Operations,
* Reputation or trust

If none apply, note that too - “No direct impact identified.”

## Immediate Response

List what actions were taken once the issue was noticed.

Example: “The report was recalled, and recipients were asked to delete it. The correct version was shared within an hour.”

## Root Cause (Why It Happened)

Describe the underlying reason, not just the trigger.

* Was a control missing?
* Was a process unclear?
* Was a tool or training gap involved?

## Learnings & Improvements

Capture what can be done differently next time.

* Add or adjust a process.
* Update documentation or training.
* Strengthen review steps or access control.

## Follow-Up Actions

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Responsible** | **Due Date** | **Status** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Reflection

* How did the team respond overall?
* What went well?
* What could be improved about the response process itself?

## Communication & Transparency

* Was anyone outside the team informed (customers, partners, the public)?
* How was the message framed to maintain trust?