# Legal / Compliance – Post-Breach Reform Guidance

**Purpose:**  
To provide structured guidance on how to assess, prioritise, and implement policy, process, or control improvements following a confirmed breach or major incident. This document ensures that lessons are translated into meaningful change and that stakeholders are engaged in continuous improvement.

## When to Use

* A breach or critical incident has occurred and been formally closed
* The debrief or review phase has commenced
* Legal, risk, or audit stakeholders have requested forward-looking reform

## Step 1: Conduct Post-Breach Review

* Convene a cross-role debrief involving Legal, Technical, Executive, Ops, Media, and Incident Coordination
* Review:
  + What went wrong and why
  + What worked well
  + What decisions were constrained by unclear policy or outdated procedures
* Use outputs from:
  + Incident logs
  + Final executive summary
  + Inject tracking tables or system reports

## Step 2: Identify Reform Areas

Categorise all lessons into the following:

* **Policy Gaps**  
  E.g. outdated escalation criteria, missing legal thresholds
* **Process Failures or Bottlenecks**  
  E.g. delayed logging, unclear comms approvals
* **Control Weaknesses**  
  E.g. lack of alerts, weak detection, poor isolation protocols
* **Training & Awareness**  
  E.g. misunderstanding of role responsibilities, lack of scenario exposure
* **Technology Limitations**  
  E.g. inaccessible logs, missing dashboards, system overload

## Step 3: Recommend and Document Reforms

For each item identified:

* Describe the issue
* Recommend a policy, process, or control change
* Assign an owner (legal, tech, executive sponsor, etc.)
* Define a delivery timeframe and accountability checkpoint
* Log in the “Post-Breach Reform Register”

## Step 4: Engage Key Stakeholders

* Present draft reform plan to Executive team
* Engage legal advisers if reforms affect regulatory obligations
* If third-party or insurer pressure is involved, prepare external-facing summary
* Link any policy reforms to compliance calendar or audit schedule

## Step 5: Monitor Reform Progress

* Track progress of each action via formal register
* Schedule quarterly check-ins until all items resolved or adopted
* Confirm final closure with the Executive and Risk Owner
* Archive reform actions with audit trail

## Outputs:

* Reform Summary Document
* Post-Breach Reform Register (template or system entry)
* Updated Policy Binder (with version control)

**Owner:** Legal / Compliance Lead  
**Reference:** LEG-04  
**Version:** 1.0  
**Approved by:** Risk & Legal Steering Group