# Legal / Compliance – Breach Disclosure Checklist

**Purpose:**  
To guide Legal teams in identifying whether a data or system security incident meets the threshold for disclosure under organisational policy, legal obligations, or insurer requirements. This checklist ensures timely, accurate, and compliant handling of potential breaches.

## When to Use This Checklist

* A security incident has affected operations, data, systems, or third-party assets
* Legal has been alerted to anomalies or external attention (e.g. media inquiry, insurer request)
* Unauthorised access, loss of control, or data/system integrity compromise is suspected

## Step 1: Confirm Potential Breach Indicators

Tick all that apply:

* Unauthorised access attempt or credential misuse detected
* Suspicious cron job, file modification, or system persistence mechanism found
* Customer, shipment, or system data was manipulated or misrouted
* Communications or dashboards displayed false or manipulated information
* External party alerted or notified the organisation first
* Insurance contact or regulator has formally inquired about status

If **two or more indicators are present**, initiate **Step 2**.

## Step 2: Assess Disclosure Requirements

* **Internal Policy** – Does this meet internal breach notification thresholds?
* **Regulatory Duty** – Are we legally obligated to notify any regulatory body?
* **Contractual Obligation** – Do any active agreements require disclosure (e.g. vendors, insurers)?
* **Reputational Risk** – Would failure to disclose damage stakeholder trust?

Document basis for each answer using:

* Legal Risk Escalation Flowchart
* Insurance Communications Template
* Breach Policy Register (if applicable)

If **any requirement is met**, proceed to **Step 3**.

## Step 3: Prepare Disclosure Packet

* Draft breach summary (use: Breach Notification Template)
* Attach validated timeline/log artefacts from Technical and Coordinator
* Confirm insurer contact procedure (see Insurance Comms Template)
* Cross-check any draft statement with Media/Executive
* Classify incident per Risk Register (e.g. Class B, Class A)
* Identify named spokesperson and legal point of contact

## Step 4: Submit and Record

* Send formal notification via approved channels (email or form submission)
* Archive all communication threads related to the breach
* Ensure incident is tagged for legal review during post-incident debrief
* If regulator or insurer response is pending, assign owner to track response timeframe

## Additional Notes

* Do not delay disclosure solely for reputational reasons if legal/contractual thresholds are met
* Always label preliminary findings as “subject to verification”
* If unsure, escalate using Legal Risk Escalation Flowchart for joint Executive review

**Owner:** Legal / Compliance Lead  
**Reference:** LEG-01  
**Version:** 1.0  
**Approved by:** Risk & Legal Steering Group