Data breach response procedure

SOP TEMPLATE

Check this template against your local regulations and your own policies before you use it.

SOP no.		Version		Effective date	
Owner		Approver		Review date	

Purpose

To make sure every suspected data breach is reported, contained and assessed quickly, that the people affected and the regulator are told when the law requires it, and that the cause is fixed.

Scope

Any loss, theft, unauthorised access to or disclosure of personal information the business holds, about customers, staff or anyone else, on paper or in any system, including systems run for us by suppliers.

Responsibilities

Role	Responsibility
All staff and contractors	Report a suspected breach to the breach lead straight away, and help contain it.
Breach lead (often the privacy officer or a senior manager)	Leads the response, assesses the risk, decides on notification and keeps the record.
Owner or senior manager	Approves notifications, deals with the regulator and the media, and approves fixes.
IT support or the system supplier	Contains technical breaches, preserves evidence and helps work out what was accessed.

Definitions

Data breach: When personal information is lost, or accessed or disclosed without permission, whether by mistake, theft or an attack.

Eligible or notifiable breach: A breach that the privacy law you're under says must be reported, usually because it's likely to cause serious harm.

What you need

- The data breach register
- Contact details for IT support, your insurer and your privacy regulator

Procedure

1. **Report it straight away**

   Anyone who suspects a breach tells the breach lead at once, even if they're not sure, with what happened, when and what data may be involved.

   > **Caution:** Don't wait until you're certain. Many privacy laws count the deadline from when the business became aware.

2. **Contain it**

   Stop the breach getting worse, such as recalling the email, asking the recipient to delete it, changing passwords, or disconnecting an infected device.

   - Keep evidence; don't wipe devices or delete logs
   - Tell IT support or the supplier if a system is involved

3. **Record it**

   Open a line in the data breach register with what's known so far, and keep it updated as you learn more.

4. **Assess the risk of harm**

   Work out what data, how many people and how sensitive it is, who may have it, and how likely it is to cause harm such as fraud, identity theft or distress.

5. **Decide who must be told**

   Using the privacy law that applies to you, decide whether the regulator and the people affected must be notified, and record the decision and why.

   > **Caution:** Deadlines differ by law and country. Check the rule that applies to you and note the deadline in the register.

6. **Notify**

   Tell the regulator and the people affected as the law requires, saying what happened, what data was involved and what they should do. Tell your insurer and, for theft or fraud, the police or bank.

7. **Fix the cause**

   Find out why it happened and add actions to the corrective action register, such as training, a system setting or a change to the procedure.

8. **Review and close**

   Once actions are done, review the response with the owner, record what was learned and close the breach in the register.

Records

- The data breach register, including breaches you decided not to report and why.
- Copies of notifications and correspondence with the regulator.
- Evidence gathered and the risk assessment.

Related documents

- Privacy policy
- Data breach response flowchart
- Corrective and preventive action procedure
- Information security policy

Revision history

Version	Date	What changed	Approved by