One page breach response plan

What to do in the first hour, the first day and within 72 hours of a personal data breach, with a breach log to record decisions.

A personal data breach is any security incident that leads to personal data being lost, destroyed, changed, disclosed or accessed without authority. Under the NDPA, a breach likely to result in a risk to people must be reported to the NDPC within 72 hours of becoming aware of it.

Response team

Role	Name	Phone
Breach lead		
Data protection officer		
IT or security lead		
Communications lead		
Senior manager		

In the first hour: contain

1. Report the incident to the breach lead immediately. Do not investigate alone.
2. Stop the leak: disconnect affected devices, reset passwords, recall emails, revoke access.
3. Preserve evidence. Do not delete logs, emails or files.
4. Start the breach log below and record every decision with the time.

In the first day: assess

1. What data is involved, how much, and about whom?
2. Is any of it sensitive, or about children?
3. What could happen to the people affected: fraud, discrimination, distress, physical harm?
4. Is the data encrypted or otherwise unusable to others?
5. Decide the risk level: low, medium or high.

Within 72 hours: notify

- If the breach is likely to result in a risk to people, notify the NDPC with what happened, the data involved, likely consequences and the measures taken.
- If the risk to people is high, tell the affected individuals in clear language, with steps they can take to protect themselves.
- If information is still incomplete, notify on time and send updates later.

Afterwards: learn

Hold a short review within two weeks. What failed, what worked, and what will change? Update policies, training and controls.

Breach log

Date and time	What happened or was decided	By whom

General guidance only, not legal advice. Adapt it to your organisation. © 2026 EDAN Development & Consulting Ltd.