Notifiable Data Breach: A Three-Day Response Plan

Description

A business should contain the incident immediately, preserve evidence and assess whether the breach is notifiable. Once it determines that notification is required, the PDPC says it must notify as soon as practicable and no later than three calendar days; affected individuals may also need prompt notice.

Start with the decision table

Situation	Decision signal
Systems are still being accessed	Contain and preserve evidence before routine recovery
Breach may cause significant harm	Assess individual-notification and PDPC thresholds urgently
Scale may be significant	Count affected individuals using a reproducible method
Facts are incomplete at notification deadline	Notify with known facts and update rather than wait silently
Vendor system caused the breach	The organisation still needs ownership and coordination

Start two clocks

Operational response begins at detection; the legal notification deadline follows the determination that the breach is notifiable. Record detection, containment, assessment and determination timestamps separately.

Contain without destroying evidence

CSA incident-response checklist supports isolating affected systems, preserving logs, resetting compromised credentials and coordinating recovery. Do not wipe or rebuild before investigators capture

what is needed.

Test both notifiability routes

PDPC breach notification guidance explains significant-harm and significant-scale considerations. Document data types, protection, recipients, likely misuse, affected count and mitigating steps.

Notify with disciplined uncertainty

State what is confirmed, what remains under investigation and when an update will follow. Avoid unsupported reassurance, but do not delay a required notice while seeking perfect facts.

Protect affected people

Give specific actionsâ??password reset, card monitoring or scam vigilanceâ??only where the exposure supports them. Align legal, security, customer service and leadership on one fact register.

Worked application

A three-day board can use four columns: time, fact, evidence and decision. At hour two, â??public link disabledâ?? is an action; â??files downloaded by unknown partyâ?? remains unconfirmed until logs support it. This separation prevents a hypothesis from becoming a public claim.

Action checklist

1. Open an incident log with exact timestamps
2. Contain affected systems and credentials
3. Preserve logs, devices and vendor evidence
4. Map data types and affected people
5. Document the notifiability decision
6. Notify PDPC and individuals where required
7. Issue updates and complete post-incident actions

Keep a decision record another person can audit

The reader task is specific: contain harm, reach a defensible notifiability decision and notify on time. Create a short file showing the controlling fact, when it was checked, the evidence retained and who owns the next action. A changed date, amount, person, address, service screen or eligibility result can alter the outcome even when the broad rule stays the same.

#	Control	Evidence	Failure signal
1	Open an incident log with exact timestamps	Authority readback	Starting the record hours later

#	Control	Evidence	Failure signal
2	Contain affected systems and credentials	Dated statement or screen	Wiping systems before imaging
3	Preserve logs, devices and vendor evidence	Calculation inputs	Treating vendor ownership as a defence
4	Map data types and affected people	Written approval	Waiting for certainty beyond the deadline
5	Document the notifiability decision	Receipt or reference	Sending generic advice unrelated to the exposed data
6	Notify PDPC and individuals where required	Photo or versioned document	Starting the record hours later
7	Issue updates and complete post-incident actions	Outcome check	Wiping systems before imaging

The two original tools in this guideâ??a timestamped three-day incident board and a claim-to-log verification registerâ??do different jobs. The first structures the choice; the second tests it against a concrete case. Neither should be copied into another case without refreshing every input and recording the extraction date.

What the primary sources establish

Source	Claim used	Freshness control
PDPC breach notification guidance	Notifiability tests, assessment and three-calendar-day notification timeline.	Checked 2026-07-18; re-open before acting
CSA incident-response checklist	Containment, evidence preservation, recovery and communications controls.	Checked 2026-07-18; re-open before acting

These sources are linked beside the claims they support. If a live service, formal notice, contract or officerâ??s written response differs from a general page, keep both and ask which newer fact or rule produces the difference. Do not choose the more convenient answer without resolving that conflict.

For adjacent questions, continue with our key employment terms checklist and company-secretary deadline guide. Each serves a separate next-step intent.

Run a final verification before committing

Start with the first decision signal in the table: **Systems are still being accessed**. Confirm whether the present facts really support â??contain and preserve evidence before routine recoveryâ?•. Then test the opposite edge caseâ??**Vendor system caused the breach**â??because that is where an apparently simple plan can fail. Write the answer in plain language and attach the dated evidence; do not leave an unspoken assumption in a spreadsheet cell.

Next, ask another adult or colleague to reproduce the worked application without seeing the result. Give that person only the source links and inputs. If the answer changes, identify whether the difference

comes from arithmetic, definition, timing or judgement. Recalculate using the live figure, retain both versions and state why the later one controls. This check is especially important when the choice depends on PDPC breach notification guidance and CSA incident-response checklist.

Finally, rehearse the first three actionsâ??open an incident log with exact timestamps; contain affected systems and credentials; preserve logs, devices and vendor evidenceâ??and set a stop point before any payment, filing, booking, upload or irreversible instruction. The stop point is reached if a required approval is absent, a source has changed, the named person cannot confirm the facts, or the downside in â??starting the record hours laterâ?• is still possible. This makes the guide usable under pressure and gives the next person enough context to continue without guessing.

Errors that change the outcome

- Starting the record hours later
- Wiping systems before imaging
- Treating vendor ownership as a defence
- Waiting for certainty beyond the deadline
- Sending generic advice unrelated to the exposed data

Keep the dated authority pages, calculation inputs, confirmations and advice used for the decision. This article applies public information to a general fact pattern and does not determine an individual application, contract, tax position, medical need or legal dispute. Recheck the primary source immediately before acting.

Questions readers ask

When does the three-day limit apply?

After the organisation determines the breach is notifiable, according to PDPC guidance.

Can notification be updated?

Where facts remain incomplete, provide known information and follow the PDPC process for updates.

Does containment replace notification?

No. Operational containment and statutory notification are separate duties.

Date Created
19/07/2026
Author
claratan