PDPA PROGRAMME PACK · B11

Data breach management plan

Fictional organisation, illustrative only, not a client case study. Quillmarrow Supplies Pte. Ltd. (fictional) is invented. All people are shown by role only.

Organisation	Quillmarrow Supplies Pte. Ltd. (fictional)
Document	B11 · Data breach management plan
Version	1.0
Date	30 October 2026 (illustrative)
Prepared by	Alex Lew, reviewer and sign-off
Client approver (role)	Managing Director
Label	Fictional organisation, illustrative only, not a client case study

1. Purpose and when to use this plan

This plan gives Quillmarrow a practical way to recognise, contain, assess, record and respond to a suspected or confirmed personal data breach. It assigns responsibilities, separates the assessment of a breach from the decision to notify, and provides a first-response playbook and draft communications.

Use the plan as soon as there are credible grounds to believe that personal data has been lost, accessed, used, disclosed, copied, changed or destroyed without authorisation, or otherwise compromised. The facts may initially be incomplete. Staff do not need to decide whether an incident is notifiable before reporting it internally.

Examples include:

- A customer spreadsheet shared through an unrestricted link.
- An email or attachment sent to the wrong recipient.
- A lost device or paper file containing staff or customer information.
- Unauthorised access to Fictional ShopCloud, Microsoft 365 or another system.
- A compromised administrator account or suspicious activity reported by Fictional Harbour IT.
- A supplier or delivery partner reporting loss or unauthorised disclosure of Quillmarrow data.
- A ransomware incident, accidental deletion or other event affecting the availability or integrity of personal data.

A security event is not automatically a personal data breach, and a breach is not automatically notifiable. The Head of Operations, as Quillmarrow's appointed Data Protection Officer (DPO), leads the fact-finding and assessment. The Managing Director (MD) owns the notification decision, supported by the DPO and, where appropriate, a Singapore-qualified lawyer.

The response should be proportionate to the information available and the potential effect on individuals. **Do not delay containment or the assessment while waiting for a complete investigation.** Record what is known, what remains uncertain, and when the assessment will next be reviewed.

This plan should be read with the personal data inventory in B3, the access and correction request log in B7, the retention schedule in B8, the vendor checklist in B9, and the incident scenario in B15. Actions should be tracked against the relevant gaps in B2, including G-07, G-09 and G-10.

The plan is for Quillmarrow's response. The reviewer supports Quillmarrow and does not act as its DPO. Questions about legal duties, exceptions or a proposed notification decision should be confirmed with a Singapore-qualified lawyer.

2. The rule in one box

> - A data breach is notifiable if it results in, or is likely to result in, significant harm to affected individuals, or is of a significant scale (affects 500 or more individuals).

> - The organisation must assess whether a breach is notifiable in a reasonable and expeditious manner; PDPC guidance expects the assessment within 30 calendar days of credible grounds to believe a breach occurred.
> - If notifiable, notify the PDPC as soon as practicable and no later than 3 calendar days after assessing that the breach is notifiable.
> - Where significant harm is likely, notify affected individuals as soon as practicable, on or after notifying the PDPC, subject to the exceptions in the Act.
> - A data intermediary processing on Quillmarrow's behalf must notify Quillmarrow without undue delay after it has credible grounds to believe a breach occurred.
> - Keep the assessment (facts, scale, harm) separate from the decision to notify (who decides, when, reasons).
> - Public explanation: https://alexlew.live/faq.html#faq-breach-deadlines

The assessment period is not a reason to wait before acting. If the available facts support an assessment earlier, complete and record it earlier. Keep investigating where needed and review the assessment if material facts change.

The PDPC deadline is counted from the assessment that the breach is notifiable, not from discovery. Record the assessment completion date and time, calculate the deadline, and have a second person check it. Seek advice from a Singapore-qualified lawyer where the deadline, an exception or the facts are uncertain.

3. Breach response team

Quillmarrow should confirm deputies, their availability and a secure contact route before this plan is approved. The deputies below are proposed role assignments, not evidence that an individual has accepted the responsibility.

Role	Response responsibility	Proposed deputy
Head of Operations, appointed DPO	Lead the response; open the incident record; coordinate containment and assessment; advise the MD; maintain the assessment and decision records; coordinate communications.	COO
MD	Own the notification decision and approve the breach management plan and significant external communications. Record the decision and reasons with the DPO.	COO, subject to documented delegation by the MD
IT Manager	Coordinate technical containment, preserve available logs and configurations, identify affected systems, and direct Fictional Harbour IT.	Head of Operations, for coordination only; technical support to be arranged
Fictional Harbour IT, managed service provider	Provide authorised technical support, preserve relevant system evidence, support containment and recovery, and report findings to the IT Manager.	A nominated alternate at Fictional Harbour IT, to be confirmed
Head of Customer Service	Identify customer-facing records and communications; coordinate customer enquiries; provide relevant incident facts and help with notices.	Sales Manager
HR Manager	Coordinate matters involving applicants or employees, relevant records and staff communications, with access limited to those who need it.	Head of Operations
COO	Support resourcing and operational decisions, coordinate business continuity, and act as the proposed deputy where authorised.	MD
External Singapore-qualified lawyer, on call	Advise Quillmarrow on legal questions, notification, individual notices, exceptions and relevant contractual issues.	An alternative Singapore-qualified lawyer appointed by Quillmarrow
External forensic support, on call	Where separately engaged, investigate technical scope, preserve and analyse evidence, and report findings. **Forensic work is not part of this programme.**	An alternative provider appointed by Quillmarrow

The DPO maintains the team contact list separately from this plan. The list should include out-of-hours routes and be accessible if a primary system is unavailable. The IT Manager should agree the escalation route with Fictional Harbour IT; it should not be assumed from the existence of an IT support relationship.

If the DPO is unavailable, the proposed deputy coordinates the response and records the handover. If the MD is unavailable, the COO should act as decision owner only where the MD has documented the delegation. An unavailable decision-maker must not become a reason to postpone containment or fact-finding.

4. The C.A.R.E. sequence

The sequence follows the *PDPC Guide on Managing and Notifying Data Breaches under the PDPA*. Activities can overlap: containment and evidence preservation may continue while the assessment is underway.

Contain

Lead: IT Manager for technical containment, with the relevant operational owner. The DPO coordinates.

1. Record when and how the incident was discovered and who reported it. Give it an incident reference.
2. Stop or limit further exposure where safe to do so. Depending on the incident, this may mean disabling a shared link, restricting an account, isolating a device, recalling a message where possible, or asking a recipient not to use or share the information.
3. Preserve evidence before making changes where practicable. Record the original sharing settings, account details, relevant logs, messages and timestamps. Do not expose additional personal data while collecting evidence.
4. Record each containment action, its owner and time. Distinguish an action attempted from one confirmed effective.
5. If a third party has received information, seek written confirmation of deletion or other containment, without assuming that a confirmation alone proves no further use or disclosure.
6. Escalate to the DPO immediately. Involve the IT Manager, operational owner and Fictional Harbour IT as needed.

Records kept: initial report; incident timeline; evidence register; affected-system and data list; containment actions and confirmation; copies of relevant correspondence. Store these in a restricted incident file.

The IT Manager should record any limitations in the available logs. If logs do not show an access, that is evidence of what those logs recorded, not conclusive proof that no other access occurred.

Assess

Lead: DPO, with the IT Manager and relevant business owner.

1. Establish the facts available: what happened, when, how long exposure lasted, who may have had access and what information was involved.
2. Identify the categories of individuals and data using B3. Count affected individuals where possible; distinguish a verified count, a reasonable estimate and an unknown.
3. Consider the circumstances of the exposure, possible recipients and likely consequences for individuals. Identify whether data in the prescribed classes in the *Personal Data Protection (Notification of Data Breaches) Regulations 2021* is involved.
4. Consider separately whether significant harm results or is likely and whether the incident is of significant scale. Document evidence and uncertainty for both.
5. Record containment status, any data intermediary involved, the assessor and the date and time the assessment is completed.
6. Escalate material uncertainty or legal questions to a Singapore-qualified lawyer. Complete the assessment in a reasonable and expeditious manner; update it if new information changes the picture.

Records kept: assessment form in section 6; data and individual counts or estimates; evidence references; advice obtained; outstanding questions; and a dated assessment of new material facts.

Report

Lead: MD for the notification decision; DPO for coordination. The MD designates who sends any notification.

1. The DPO presents the completed assessment and relevant uncertainty to the MD.
2. The MD and DPO record the notification decision, time and reasons separately from the assessment.
3. If the breach is assessed as notifiable, calculate and independently check the PDPC deadline. Prepare and send the notification as soon as practicable and no later than that deadline.
4. Where significant harm is likely, arrange notice to affected individuals as soon as practicable, on or after notifying the PDPC, subject to the exceptions in the Act. Confirm an exception with a Singapore-qualified lawyer before relying on it.
5. Record who approved and sent each notice, when it was sent, to whom, what it contained and any acknowledgement or delivery evidence.

6. If the decision is not to notify, record the reasons and the trigger for reconsideration. A later change in facts may require a fresh assessment and decision.

Records kept: separate decision record; deadline calculation and check; approved notification content; submission acknowledgement; individual-notice delivery record; legal advice reference; and subsequent updates.

Evaluate

Lead: DPO, supported by the IT Manager and relevant business owners.

1. Review the cause, the effectiveness of containment, the quality of available evidence and the timeliness of decisions.
2. Identify improvements to access controls, training, supplier arrangements, notices, records and this plan.
3. Assign each action an owner, target date, evidence required to close it and a status. Add or update the relevant B2 gap and action tracker.
4. Review whether the data inventory, retention schedule, vendor checklist or request process needs updating.
5. Report material open actions to the COO and MD. Verify completion using evidence rather than closing an action on an assurance alone.

Records kept: post-incident review; action tracker; evidence of completion; approvals; and updates to the relevant pack documents.

5. First 72 hours playbook

The windows below are operational prompts, not permission to wait for the end of a window. They run from discovery for response coordination. The PDPC three-calendar-day clock runs from the assessment that the breach is notifiable, **not from discovery**. The assessment must not be delayed.

Time window	Actions	Owner	Record
0–1 hour	Report the suspected incident to the DPO and IT Manager. Record discovery time and initial facts. Take immediate proportionate containment steps, such as disabling a link or restricting access. Preserve available evidence before changes where practicable.	Person discovering the issue; DPO; IT Manager	Initial report, incident reference, timeline, containment and evidence log
1–4 hours	Establish the systems, data and people potentially affected. Secure relevant logs and communications. Contact the operational owner and Fictional Harbour IT where needed. Ask an unintended recipient to contain and delete information where appropriate. Brief the MD if the potential impact warrants it.	DPO; IT Manager; relevant business owner	Initial scope, evidence register, recipient correspondence, MD briefing
4–24 hours	Continue fact-finding and assess potential harm and scale using section 6. Identify information gaps and obtain legal or specialist support where needed. Complete the assessment sooner if the facts permit. Record containment status and follow-up checks.	DPO, supported by IT Manager and business owner	Assessment form, counts or estimates, advice reference, outstanding questions
24–72 hours	Complete or update the assessment as soon as the facts permit; present it to the MD. Record the separate notification decision. If assessed notifiable, calculate and check the PDPC deadline and prepare or send required notices. Continue containment and record any new facts.	DPO; MD; designated sender	Completed assessment, decision record, checked deadline, notification and delivery evidence where applicable

If the assessment is completed before 24 hours, do not wait for a later window to make or act on the decision. If it cannot yet be completed, record the reason, the outstanding evidence, the person obtaining it and the next review time. The DPO should escalate a stalled assessment to the MD and obtain legal advice where appropriate.

6. Assessment form

The DPO should complete this form using the best available evidence. Mark unknowns as unknown, identify estimates, and link to supporting records. This form records the assessment; it is not the notification decision.

Field	Information to record
Incident reference	Unique incident ID and link to the restricted incident file.

Field	Information to record
Facts	What happened, how and when it was discovered, exposure period, suspected cause and known recipients. Distinguish confirmed facts from assumptions.
Data types	Categories of personal data and relevant B3 inventory IDs; sensitivity and context.
Number of individuals	Known or estimated number affected, source of the count and uncertainty. Avoid counting records as individuals without checking.
Prescribed classes of data	Whether prescribed classes of data in the *Personal Data Protection (Notification of Data Breaches) Regulations 2021* are involved; identify the evidence and seek legal advice where uncertain.
Likelihood of significant harm	Potential harm, circumstances, likelihood, supporting facts, mitigating factors and unresolved questions.
Scale threshold	Whether the breach affects 500 or more individuals, or whether the number remains uncertain; record the basis.
Containment status	Actions taken, times, effectiveness, remaining exposure and evidence preserved.
Data intermediary involved	Name and role, data or systems involved, when Quillmarrow was informed, and information or assistance requested.
Assessor	Name or role of the person completing the assessment; DPO review where another person prepares it.
Date and time assessment completed	Date, time and time zone; record the version if subsequently updated.
Evidence and gaps	Links to logs, correspondence and other evidence; limitations, outstanding questions and next review date.

Where the information includes business contact information, consider its treatment separately where relevant and confirm the point with a Singapore-qualified lawyer. Do not assume that all data in a business record is business contact information.

7. Notification decision record

Complete this record after the assessment. The MD owns the decision, supported by the DPO. Keep it with, but separate from, the assessment form.

Field	Information to record
Incident and assessment reference	Incident ID, assessment version and completion date and time.
Decision	Notifiable or not notifiable; record whether the decision is based on significant harm, significant scale or both.
Decided by	MD and DPO; record any authorised delegation and legal advice obtained.
Date and time	When the decision was made and recorded.
Reasons	Concise reasons linked to the assessment, including material uncertainty and any reason for later review.
PDPC deadline	If assessed notifiable, compute the assessment completion date plus 3 calendar days; record the resulting deadline and independent check. If not notifiable, record “not applicable”, unless documenting a clearly labelled counterfactual.
Individuals to notify or exception	Identify the affected group and proposed notice where significant harm is likely, or record any exception relied on and confirm it with a Singapore-qualified lawyer.
Who sends	Role responsible for PDPC notification and, separately, notices to individuals.
Evidence	Approved content, submission time, acknowledgement, delivery records, advice and subsequent updates.
Review trigger	New facts, changed counts, additional access or a change in likely harm that requires reassessment.

A deadline calculation should be checked against the actual assessment record. Do not use the date of discovery as a substitute for the date on which the breach was assessed as notifiable.

8. Worked example: INC-2026-07

The following is the illustrative scenario supplied for this pack. The incident facts and decision are those in the case file. Entries identified as proposed follow-up actions are planning entries, not claims that work was completed.

Date and time	Entry	Owner and record
Saturday 12 September 2026; time not supplied	The SharePoint folder “Web-shop returns 2026” had been shared with “anyone with the link” since this date.	IT Manager to retain the relevant sharing-setting evidence; exact start time not supplied.
Monday 14 September 2026, 10:20	Head of Customer Service discovered the sharing. The link had been sent by mistake to one external courier contact.	Head of Customer Service; discovery report and incident timeline.
14 September 2026, 10:45	The link was removed and the exposure contained.	IT Manager and Head of Customer Service; containment record and setting change evidence.
14 September 2026; time not supplied	The DPO began the assessment. The folder held a spreadsheet containing 140 web-shop customers’ names, home addresses, mobile numbers and return-order details, and 1,850 B2B contacts described as business contact information.	Head of Operations as DPO; assessment and data-inventory references, including PD-02 and PD-12.
14–16 September 2026; exact review time not supplied	Client-reported access logs showed two opens from the courier’s address and none from elsewhere; a log export was kept. The available logs should be read with their limitations.	IT Manager; retained log export and evidence record.
15 September 2026; time not supplied	The courier confirmed deletion in writing.	Head of Customer Service; written confirmation retained in the incident file.
16 September 2026, 17:00	Assessment completed. The case assessment records fewer than 500 individuals whose personal data was affected; business contact information was treated separately for this assessment and that point should be confirmed with a Singapore-qualified lawyer. No NRIC numbers, financial account details, health data or other data in the prescribed classes identified in the case file as likely to result in significant harm were involved.	Head of Operations as DPO; completed assessment, evidence and identified limitations.
16 September 2026; decision time not supplied	MD and DPO recorded the decision: **not notifiable**. Reasons were recorded; no notification was made to the PDPC or individuals. The separate decision record should retain the exact decision time if available.	MD and DPO; notification decision record.
19 September 2026	Counterfactual only: had the breach been assessed as notifiable on 16 September, the case-file PDPC deadline would have been 19 September 2026. This was not an actual notification deadline under the recorded decision.	DPO; labelled deadline calculation.
By 30 September 2026; proposed follow-up	Review the SharePoint link-sharing settings, access evidence and staff handling of external sharing. Capture lessons and actions in B2 under G-07 and G-10.	Proposed owners: IT Manager for settings and evidence; Head of Operations for the incident process. Completion evidence and actual dates were not supplied.
By 30 September 2026; proposed follow-up	Review the courier communication and whether vendor escalation and deletion arrangements need strengthening in B9.	Proposed owner: Head of Operations, with the relevant operational owner. Completion evidence and actual date were not supplied.

The case file says lessons and actions were logged, but does not supply their full content, owners or completion dates. The follow-up rows above are therefore proposed actions, not a reconstruction of completed work. If further evidence showed a different scope, recipient or likelihood of harm, the DPO would update the assessment and return the decision to the MD.

9. Notification templates

These are drafts for adaptation to the incident and legal review. Do not include unnecessary personal data, speculation or assurances that cannot be supported.

A. PDPC notification content checklist

If the breach is assessed as notifiable, the designated sender should use the applicable PDPC notification channel and include the information available at submission, updating it as appropriate.

- Quillmarrow's details and an incident contact.
- When the breach occurred or is believed to have occurred, when it was discovered, and when it was assessed as notifiable.
- A description of the incident, the systems and data involved, and how the breach occurred or is believed to have occurred.
- The number or estimated number of affected individuals, the basis of the estimate and any material uncertainty.
- The potential consequences for individuals and the assessment of significant harm and scale.
- Containment and remedial actions taken or planned.
- Whether and how affected individuals have been or will be notified, or an exception relied on, confirmed with a Singapore-qualified lawyer.
- Any data intermediary involved and the assistance received.
- Further information to follow, where applicable.

Draft opening: "Quillmarrow Supplies Pte. Ltd. is notifying the PDPC of a personal data breach assessed as notifiable on [date and time]. The information below reflects the facts available at [time]; items identified as pending will be updated when confirmed."

The DPO retains the submitted content, submission time and acknowledgement. The MD approves the decision and designates the sender; a second person checks the deadline and recipient before submission.

B. Notice to affected individuals

Subject: Important information about your personal data

"Dear [appropriate description],

We are contacting you about a personal data breach affecting [describe the relevant data and circumstances in plain language]. We discovered the issue on [date]. Based on our current assessment, [explain what is known, including any material uncertainty].

We have taken the following steps: [containment and support measures]. The potential effects may include [specific, evidence-based explanation]. You can take these steps if relevant: [practical steps, without implying they eliminate all risk].

For questions or assistance, contact Quillmarrow's DPO at [confirmed contact details]. We will provide an update if material information changes.

[Authorised Quillmarrow role]"

Before sending, confirm the affected group, contact route, content, timing and any exception with the DPO and a Singapore-qualified lawyer. Where significant harm is likely, notices are sent as soon as practicable, on or after notification to the PDPC, subject to the exceptions in the Act.

C. Internal staff alert

Subject: Incident response instructions

"An incident involving [brief description] is being managed under Quillmarrow's breach plan. If you hold relevant information or receive an enquiry, contact [DPO or designated response contact] through [approved channel].

Do not forward affected records, speculate about the cause or speak externally on Quillmarrow's behalf unless authorised. Preserve relevant messages and follow the IT Manager's instructions. Customer and staff enquiries should be directed to [designated role].

Further updates will be provided through [approved internal channel]."

The DPO and relevant business owner should tailor the alert to what staff need to know. Staff should still report relevant facts promptly.

10. Evaluate and track improvements

After containment and the notification decision, the DPO should convene a review with the relevant owners. The review should be proportionate and should ask:

- What happened, what evidence supports that account, and what remains unknown?
- Was the incident recognised and escalated promptly? Did staff know whom to contact?
- Did containment stop further exposure, and what evidence supports that conclusion?
- Were logs, sharing settings and communications preserved without unnecessarily copying personal data?
- Were the number of individuals and data categories assessed accurately, including uncertainty?
- Was the assessment completed expeditiously? Was the decision recorded separately, with reasons and any deadline checked?
- Were vendor escalation, support and deletion arrangements effective?
- Were communications clear, authorised and limited to appropriate recipients?
- Which control, process, training or contractual changes would reduce recurrence or improve response?

For every agreed action, B2 and the action tracker should record the incident reference, gap ID, owner role, target date, expected evidence, status and verification result. For INC-2026-07, likely links include G-07 for sharing and access controls, G-09 where vendor arrangements need review, and G-10 for the breach process.

The DPO should also consider updates to B3 inventory records, B8 retention decisions, B9 vendor due diligence and B15's worked scenario. Keep the original incident assessment and decision traceable; do not silently replace them when new facts emerge. Record changes as dated updates.

11. Testing the plan

The DPO owns an **annual tabletop drill**. The exercise should involve the MD or authorised deputy, IT Manager, a relevant business owner and, where appropriate, Fictional Harbour IT. Quillmarrow may invite external legal or forensic support separately; forensic work is not part of this programme.

Use a scenario that tests discovery, containment, evidence preservation, assessment of harm and scale, the separate notification decision, deadline calculation and draft communications. Include an unavailable decision-maker or incomplete vendor response in at least one exercise scenario.

Keep the scenario, participants' roles, decisions, timing observations, lessons and action tracker. The DPO should assign owners and target dates for improvements, report material gaps to the MD and COO, and verify closure through evidence. A tabletop exercise tests the process; it does not by itself establish that technical controls work.

12. Document control

Owner: Head of Operations, Quillmarrow's appointed DPO.

Approver: Managing Director.

The DPO maintains this plan, confirms the response contacts and proposed deputies, and submits material changes to the MD for approval. Review the plan annually and after a significant incident, exercise or material change to systems, suppliers or relevant guidance. Record the review, approval and changes in Quillmarrow's controlled document process.

Before implementation, Quillmarrow should confirm the deputies and contact routes, agree the escalation process with Fictional Harbour IT and other relevant vendors, and have a Singapore-qualified lawyer review legal questions and notification procedures. No approval, test or implementation is evidenced merely by the preparation of this draft.

About this sample

Fictional organisation, illustrative only, not a client case study. Quillmarrow Supplies Pte. Ltd., its people, vendors, findings and dates are invented. Nothing in this document reports a client result.

I personally review and sign off every deliverable. You appoint your own DPO. I support them.

This is practical compliance support, not legal advice. For legal advice, use a Singapore-qualified lawyer.

What's not included

- Acting as your DPO. You appoint your own DPO; I prepare the handover and can support them separately.
- Legal advice, legal contract drafting, representation or a guarantee of compliance.
- Forensic investigation, penetration testing, security engineering or implementing changes in live systems.
- A detailed AI governance review or ISO/IEC 42001 readiness check unless separately scoped.
- Ongoing document upkeep after handover, unless agreed through monthly DPO support.
- Healthcare-sector work or on-site delivery.

Questions about this sample: DM @alewyl1 on X, or ask for a free intro call (coffee chat).