**[Company name]**

How to use this document: delete this paragraph before saving, sharing, or circulating it. Every part shown in blue is yours to replace: type your own details over each blue [field] until no blue remains. Then select all (Ctrl+A) and set the font colour to the same dark colour throughout. What is left is your finished document.

# Data Breach Response Checklist

*Work through the phases in order: detect, contain, assess, notify, recover, and review.*

## 1. Incident record

| | |
|---|---|
| **Incident reference number** | [Incident reference number] |
| **Date and time the breach was discovered** | [Date and time the breach was discovered] |
| **Person who discovered the breach** | [Full name of the person who discovered the breach] |
| **How the breach was discovered** | [Description of how the breach was discovered] |
| **Incident lead** | [Full name of the incident lead] |
| **Date this checklist was opened** | [Date this checklist was opened] |

## 2. Response team

| Role on the response team | Name of the person in this role | Contact details for this person |
|---|---|---|
| Incident lead | [Full name of the incident lead] | [Contact details for the incident lead] |
| Technical investigator | [Full name of the technical investigator] | [Contact details for the technical investigator] |
| Legal adviser | [Full name of the legal adviser] | [Contact details for the legal adviser] |
| Communications lead | [Full name of the communications lead] | [Contact details for the communications lead] |
| Senior manager notified | [Full name of the senior manager notified] | [Contact details for the senior manager notified] |

## Phase 1. Detect and report

| | |
|---|---|
| | The suspected breach has been reported to the incident lead immediately, and the time of that report is recorded in section 1. |
| | No one has deleted, altered, or overwritten anything that might be evidence, including logs, emails, and affected devices. |
| | Access to affected systems has been noted but not casually changed until the technical investigator advises, so evidence is not lost. |
| | A single incident record has been opened, and all later notes, decisions, and messages are filed against it. |

## Phase 2. Contain

| | |
|---|---|
| | Affected systems or accounts have been isolated or disabled as far as needed to stop further exposure, without destroying evidence. |
| | Compromised credentials have been revoked or reset, and any sessions still open under them have been ended. |
| | Network access used by the breach has been blocked where it has been identified, and the |

| | |
|---|---|
| | block is recorded with its date and time. |
| | Backups have been checked to confirm they are intact and have not been affected by the same breach. |
| | Short-term containment is recorded separately from any longer-term fix, so the incident record shows what stopped the harm and what fixed the cause. |

## Phase 3. Assess the scope and the data affected

| | |
|---|---|
| | The systems, accounts, and data stores involved have been listed, including any that were only possibly involved. |
| | The types of personal data involved have been identified, and whether sensitive categories of personal data are included. |
| | The number of people affected has been estimated, with the basis for the estimate recorded, and marked as estimated until it is confirmed. |
| | The period during which data was exposed has been established as far as the evidence allows. |
| | Whether data was only viewed, or was also copied, altered, or deleted, has been recorded for each affected system. |

## Phase 4. Notify

| | |
|---|---|
| | Senior management has been briefed with the confirmed facts, the unknowns, and the next decision needed. |
| | Legal advice has been taken on whether the applicable data protection regulator must be notified, and by what deadline. |
| | Where regulator notification is required, it has been made within the deadline, and the reference number is recorded here: [Reference number for the regulator notification]. |
| | A decision on notifying affected people has been recorded, with the reasons, even where the decision is not to notify. |
| | Where affected people are notified, the notice states what happened, what data was involved, what has been done, and what they should do. |
| | Insurers and any affected outside providers have been notified where the policy or contract requires it. |

## Phase 5. Eradicate and recover

| | |
|---|---|
| | The cause of the breach has been removed, including any unauthorised access route, malicious software, or misconfiguration that enabled it. |
| | Affected systems have been rebuilt or restored from clean backups, and the restored data has been checked before return to use. |
| | Passwords and access keys that may have been exposed have been changed, and affected users have been required to reset theirs. |
| | Additional monitoring has been put in place on affected systems for a defined period after recovery. |
| | Return to normal service has been approved by the incident lead, and the date and time of that approval are recorded. |

## Phase 6. Review and learn

| | |
|---|---|
| | A post-incident review has been held with everyone on the response team, covering what worked, what failed, and what was unclear. |
| | The root cause, the timeline, and the effectiveness of each phase are written up in the final incident report. |
| | Every lesson from the review has an owner and a completion date, and open lessons are tracked until closed. |
| | This checklist, and any related plan it follows, has been updated to reflect what was learned. |
| | The completed incident record, including notification decisions and evidence, has been filed and retained under the organisation's retention rules. |

## Sign-off

[Summary of the outcome of this incident, including whether notification was made and whether recovery is complete.]

| | |
|---|---|
| **Incident lead name** | [Full name of the incident lead] |
| **Reviewer name** | [Full name of the reviewer] |
| **Incident lead signature** | [Signature of the incident lead] |
| **Reviewer signature** | [Signature of the reviewer] |
| **Date of sign-off** | [Date of sign-off] |