

|  |
| --- |
| Business Name |
| **Data Breach Response Plan**  **20xx – 20xx**  **Prepared for {IT Contact name here} on the {date}** |

This data breach response plan sets out procedures and clear lines of authority for staﬀ in the event that {Insert Company Name Here} Pty Ltd experiences a data breach (or suspects that a data breach has occurred). It should be reviewed, tested and updated regularly. All staﬀ should be familiar with this plan.

# Part 1 – all staff

## What to do in the event of {or the suspicion of) a data breach

1. Immediately notify {Primary IT Contact}, or if unavailable, {Secondary IT Contact}.
2. Record the time and date the suspected breach was discovered, the type of information involved, the cause and extent of the breach, and any other information you have. This page can be used to report the breach.

### DATA BREACH NOTIFICATION

|  |
| --- |
| DATE: |
| TIME: |
| SOURCE OF DISCOVERY: |
| TYPE OF DATA AT RISK: |
| SCOPE OF BREACH: |
| IT () NOTIFIED: YES / NO |
| DETAILS: |

# PART 2 – RESPONSE TEAM

## What to do once notified of a data breach

## Stage 1 – Contain and collect evidence

1. Immediately contain breach: Contact IT support if necessary
   * Contact building security if necessary
2. Ensure evidence is preserved that may be valuable in determining details of the breach
   * Contact an initial investigation and collect information promptly, including: the date, time, duration and location of the breach
   * The type of information involved in the breach how the breach was discovered and by whom
   * The extent of the breach (who’s information is potentially at risk?)
   * The seriousness of the breach (what type of information is potentially at risk?) the cause of the breach is known
3. CAREFULLY document what has happened and who is involved to this point

## Stage 2 – Notification

1. Determine who needs to be made aware of the breach internally and notify them as soon as possible.
2. Consider obtaining advice from legal or insurance representatives.
3. Determine whether to notify aﬀected individuals immediately - is there a real risk of serious hard to them?
4. Consider whether law enforcement should be notiﬁed.
5. If there has been an eligible data breach, notify the OAIC – via their web site [www.oaic.gov.au/ndb](http://www.oaic.gov.au/ndb) or phone 1300 363 992

|  |
| --- |
| **Eligible data breach**  An eligible data breach arises when the following three criteria are satisfied:   1. There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, 2. This is likely to result in serious harm to one or more individuals, and 3. The entity has not been able to prevent the likely risk of serious harm with remedial action. |

## Stage 3 – Review and improve

1. Fully investigate the cause of the breach.
2. Make changes to ensure this type of breach cannot happen again. Document these changes where appropriate.
3. Inform IT, Legal, Insurance contacts of changes as appropriate.
4. Revise staﬀ training practices as necessary.
5. Consider a follow up security audit to ensure changes are eﬀected.
6. Discuss these outcomes with the OAIC.

# TESTING THIS PLAN

This plan should be updated and tested regularly.

### example test scenarious:

#### Hacker gains access to a computer.

Imagine a hacker gets into your system because your remote access is not secure. Identify the damage they could do as a user setup for remote access.

#### Lost USB Drive

A USB Drive that had company data has been lost or stolen.

#### Computer left unattended

Your computer was left unattended or unlocked. On returning to your computer your realised that the screen was not at the same place.

For each of these scenarios, run through a simulated data breach response and satisfy the following questions:

1. Did a data breach occur?
2. Is there a likely risk of serious harm?
3. What do we need to do now?

# Contact Details

{Primary IT Contact}:   
{Secondary IT Contact}:

IT Support:

Legal Support: Insurance:

OAIC - Australian Government Oﬃce of the Australian Information Commissioner [www.oaic.gov.au/ndb](http://www.oaic.gov.au/ndb) or phone 1300 363 992.

Report prepared by:

[INSERT LOGO]

This report is based on unveriﬁed information provided by a person identifying themselves as {IT Contact name here}. It is intended to provide a reliable data breach response plan for a small business with a single manager. This plan should be regularly reviewed, tested and updated.