<insert company logo>

TEMPLATE DATA BREACH POLICY AND PROCEDURE

BACKGROUND AND OBJECTIVES

The *Privacy Act 1988* (Cth) and the *Australian Privacy Principles* protect personal information which belongs to individuals by placing restrictions on how that information can be collected, handled, used and disclosed.

Personal information must be managed in an open and transparent way. This requires us to:

- Implement practices, procedures and systems to ensure compliance with privacy laws and appropriately handle any enquires or complaints about privacy;
- Have a clear and up to date Privacy Policy that documents the way we manage personal information, including:
  - The kinds of information we collect;
  - How we collect and hold it;
  - The purposes for which we collect, hold, use and disclose it;
  - How people can access and correct the information we hold about them;
  - How people can make a privacy related complaint and how we deal with such complaints; and
  - Whether we are likely to disclose information to overseas recipients and if so, where they will be located;
- Report an 'eligible data breach' to the Office of the Australian Information Commissioner (**OAIC**) and any affected individuals.

Our **[USER NOTE: Amend to reflect the name of your Privacy Policy and Procedure documents]**Privacy Policy and Procedure outlines the way in which we collect, hold, use and disclose personal information.

This Data Breach Policy and Procedure outlines how we manage any potential privacy breaches.

WHAT IS PERSONAL INFORMATION?

Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable. It does not matter whether it is true or whether it is oral or in writing.

In effect, it is information or an opinion that can identify a person, for example, their name, physical description, address, date of birth, sex, phone number, email address, driver's licence number and information about their employer / place of work, salary and employment, business activities, investments, assets and liabilities – or any combination of these.

Sensitive personal information is information or an opinion about a person's racial or ethnic origin, political opinions, membership of a political, trade or professional association or a trade union, religious or philosophical beliefs or affiliations, sexual preferences, criminal record or health information (including biometric and genetic information).

WHAT IS A PRIVACY BREACH?

A privacy breach occurs if we hold personal information about an individual and breach:

- Our legal obligations in relation to its collection, handling, use or disclosure; or
- The provisions of our **[USER NOTE: Amend to reflect the name of your Privacy Policy and Procedure documents]** Privacy Policy and Procedure.

When you identify an actual or possible privacy breach, report it to the Privacy Officer immediately.

WHAT IS AN ELIGIBLE DATA BREACH?

When an 'eligible data breach' occurs, we must usually report it to the OAIC and affected individuals within strict timeframes. However, this may not be required if we act quickly to manage the breach and ensure that it will not cause any serious harm to an individual.

A privacy breach is an eligible data breach if it results in:

- Unauthorised access to or disclosure of personal information; or
- Information being lost in circumstances where unauthorised access to or disclosure of personal information is likely to occur,

and this is reasonably likely to result in serious harm to an individual.

What is serious harm?

Serious harm can include identity theft and serious physical, psychological, emotional, financial or reputational harm.

Some kinds of personal information breaches are more likely than others to cause serious harm e.g. those that involve sensitive information such as medical or health information, information or documents commonly used for identity theft (e.g. Medicare details, drivers licence or passport information) or financial information. Combinations of different types of personal information (as opposed to a single piece of information) may be more likely to result in serious harm.

Tip

If an eligible data breach involves personal information that you and another organisation hold (e.g. an outsourced service provider or joint venture partner), only one of you needs to assess and report the breach to the OAIC and affected individuals. If no-one undertakes the assessment or makes the report, you could both be liable for a breach of the requirements.

As a general rule, the entity that has the most direct relationship with the affected individual(s) should report.

Ensure that your service and other relevant contracts include provisions:

- Requiring compliance with the data breach reporting regime;
- Requiring the other party to notify you if there is a privacy breach and cooperate with any investigation and remediation you undertake; and
- Setting out who is responsible for assessing and reporting data breaches.

DATA BREACH RESPONSE PLAN

Our Privacy Officer will investigate and deal with privacy breaches in accordance with the following Data Breach Response Plan.

[USER NOTE: Customise this section to ensure that it accurately reflects the steps you will take in response to a privacy breach. Do not delete content that facilitates compliance with legal requirements. This is flagged with a User Note.]

Data Breach Occurs		
Step	**Action**	**Timeframe** **[USER NOTE: Do not delete or amend these timeframes.]**
1	**Contain the breach and do a preliminary assessment:** • Take immediate steps to contain breach	Within 24 hours of identification of