# Data Breach Notification Plan

### Terms

Personal information is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term personal information is necessarily broad. The definition of personal information is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified using information that is linked or linkable to said individual. In performing this assessment, it is important to recognise that information that is not personal information can become personal information whenever additional information is made publicly available - in any medium and from any source - that, when combined with other information to identify a specific individual, could be used to identify an individual (e.g. SSNs, name, DOB, home address, home email).

### Breach

A breach is an unauthorised disclosure, unauthorised acquisition, unauthorised access and/or any similar occurrence where a person, other than an authorised user, accesses personal information or an authorised user accesses personal information for other than an authorised purpose.

### Training

VeroGuard Systems Pty Limited (**Company**) protects the information entrusted to it. The Company representatives undergo security and privacy training prior to obtaining access to information and annually to ensure individuals are up to date on the proper handling of personal information. Failure to complete required training results in denial of access to information.

### Monitoring

Users and systems are tested annually to determine their incident response capability and incident response effectiveness. The Company meets annually for a tabletop exercise that is designed to test the breach response procedure and to help ensure members of the Response Team are familiar with the plan and understand their specific roles.

### Reporting

The Company employees and contractors with access to data and information systems must report all concerns, suspected breeches or confirmed breaches. Core event information must be collected and reported: date of the incident, location of the incident, breached data, nature of the breach (loss of control, compromise, unauthorised access or use, other) and the suspected number of impacted individuals, if known.

A breach involving personal information in electronic or physical form must be reported to the company secretary within one hour of discovering the incident, who in turn must report it to the CEO. In terms of reporting, there should be no distinction between suspected and confirmed personal information breach incidents.

### Response Team

A Response Team will be formed to determine the level of risk to the impacted individuals with the appropriate remedy and form a Data Breach Response Plan.

The Response Team will respond to all breaches and will perform an initial assessment of the risk of harm to individuals potentially affected.

This team will analyse reported breaches to determine whether a breach occurred, the scope of the information breached, the potential impact the breached information may have on individuals and on the Company.

This team consists of the manager of the area experiencing or responsible for the breach, the head of development, the head of systems and the company secretary.

## Notification

### Notification Delays

Within the confines of the law, notification may be delayed if a notification would potentially cause harm, including further breaches. Notification to affected parties may not occur or may be delayed if a national security or law enforcement agency determines that the notification will impede a criminal investigation.

**Determination of Notification to Impacted Parties**

The Response Team will determine whether notification is necessary for all breaches under their purview. To determine whether notification of a breach is necessary, the Response Team will determine the scope of the breach, to include the types of information exposed, the number of people impacted, and whether the information could potentially be used for identity theft. The Response Team will also assess the likely risk of harm caused by the breach. Finally, the Response Team will assess the level of risk and consider a wide range of harms that include harm to reputation and potential risk of harassment, especially when personal records such as health or financial records are involved.

**Communication to Impacted Parties**

In the event the decision to notify is made, every effort will be made to notify impacted parties as soon as possible unless otherwise precluded above. Notification must contain details about the breach, including what information was compromised and whether credit monitoring will be offered. Initial notification must be completed without undue delay from the time the incident was determined to be a breach.

**Breach Response Plan Reviews**

At the end of each financial year, the Company will review reports, if any, from the Response Team detailing the status of each breach reported during the financial year and consider whether it is necessary to take any action, which may include:

- Developing or revising documentation
- Updating the Data Breach Notification Plan
- Updating the Data Breach Response Plan
- Revising existing and/or implementing new policies to protect personal information holdings
- Improving training
- Modifying information sharing arrangements

**Changes to this Data Breach Notification Plan**

We may update this Data Breach Notification Plan.