Vision Super Pty Ltd

ABN 50 082 924 561

Data breach policy

BACKGROUND

This policy supports the main Privacy Policy.

STATEMENT OF POLICY

In the course of conducting its normal business activities, Vision Super collects, records, maintains and uses personal information from members, which members rightly expect to be protected from misuse, interference, loss, and from unauthorised access, modification or disclosure.

Vision Super makes every effort to protect personal information from misuse, loss, unauthorised use, access, modification or disclosure (i.e. a data breach).

However, in the event of a data breach (or suspected data breach) the following five steps must be taken:

1.) Contain the breach.
2.) Conduct a preliminary assessment.
3.) Evaluate the risks associated with the breach.
4.) Notification.
5.) Prevent future breaches.

Please note that this policy is general in nature and is only meant to be used as a guide. Breaches or suspected breaches may be assessed on a case-by-case basis by Vision Super's Audit, Risk and Compliance Committee and additional steps may be taken if deemed necessary.

Responding to a data breach (or suspected data breach):

Step 1 – Contain the breach

Once Vision Super has discovered (or been notified) that a breach or suspected breach ("the breach") has occurred, it should take all reasonable steps necessary to contain the breach.

Step 2 – Conduct a preliminary assessment

During this preliminary stage, Vision Super should make an assessment regarding the breach and act accordingly. This may involve the:

- **appointment of an internal person and/or team to investigate the breach -** this may include the CEO, General Counsel, Risk and Compliance Manager, Head of Information Systems, Audit, Risk and Compliance Committee, and any other Manager whose department may be affected by the breach; and

- **drafting of a report concerning the breach –** this may include a report that makes recommendations concerning the breach, and should include: the information that is the subject of the breach, the cause of the breach, the extent of the breach, and the level of harm that affected individuals may suffer as a result of the breach.

Step 3 – Evaluate the risks associated with the breach

In determining what other steps should be taken, Vision Super should address the following issues/questions:

a) The type of information involved – the type of information that has been affected by the breach can have an important bearing on the severity of the breach. For example, a breach involving an individual's name, medical history, place and date of birth can be quite severe as they cannot be "re-issued". Whereas, a breach involving an individual's Medicare numbers, tax file numbers, and bank account numbers, while serious, can be "re-issued".

b) The type and number of affected individuals – i.e. are they members, beneficiaries, employees and how many of them will be affected?

c) The context of the information involved in the breach (and who has gained unauthorised access to the relevant information) – this issue looks at the kind of information that is the subject of the breach, and how its use may affect the individuals concerned. For example, if a list of the names of Vision Super members (by itself) is attained by an organised crime gang it will constitute a breach, however a list of the names of the Vision Super members who receive pension payments may be deemed to be a greater breach, as the organised crime gang may try to contact those individuals posing as an organisation that can set up a SMSF and defraud the individuals listed.

d) Whether there have been any other similar breaches – this may assist in determining who has committed the breach and the size of the breach. For example, a series of small breaches regarding member information committed by an individual or organisation that has not been addressed or remedied, may constitute a much larger breach if it is found that an individual or organisation is compiling member information.

e) The way in which the information may be used – could the information that is the subject of the breach be used for fraudulent purposes, or could it be used with publically available information to create a greater risk of harm to members?

f) Is there a risk of ongoing breaches or further exposure of the information?

g) Is there any evidence of criminal activity (for e.g. theft)?

h) Is the information that is the subject of the breach adequately encrypted, anonymised or otherwise not easily accessible?

i) Has the information that is the subject of the breach been recovered?

j) What steps have already been taken to mitigate the harm?

k) Is the breach a systematic problem or an isolated incident?

l) The number of affected individuals.

m) The risk of other harms – this may include reputational damage, loss of public trust, financial exposure, or regulatory penalties.

Step 4 – Notification

If Vision Super believes on reasonable grounds that there has been unauthorised access or disclosure of the personal (and/or sensitive) information that will result in a real risk of serious harm (economic or financial harm or harm to the individual/s reputation that is not remote) to the individual concerned ("serious data breach") Vision Super should:

1) **Prepare a statement** – this statement should include the identity and contact details of Vision Super, a description of the data breach, the kind/s of information concerned, and any recommendations about the steps that individuals should take in relation to the data breach (for e.g. change their passwords);

2) **Give a copy of the statement to the OAIC;**

3) **Consider whether it is appropriate to notify any other external bodies -** depending on the severity or substance of the breach, Vision Super may wish to notify: professional or other regulatory agencies (such as APRA or the ACCC), the ATO (if the breach concerns prohibited access to TFN's or Medicare numbers), the police (state and/or federal), insurers (depending on contractual obligations), any relevant banks, and any other agencies that have a direct relationship with the lost/stolen information;

4) **Contact the OAIC to determine whether Vision Super should:**

    a. **Send a copy of the statement to the affected individual**; and/or

    b. **Publish a copy of the statement on the Vision Super website and publish a copy of the statement in at least one newspaper in each state**;

        - **NOTE:** it is important to contact the OAIC **PRIOR to notifying the affected individual** as, if the breach is only deemed to be minor and the individual has not suffered any harm or loss, notifying them of such a breach may cause them unnecessary anxiety, de-sensitise them to further

notifications, or cause them to lose trust in Vision Super if they learn of the breach through the media at a later date.

5) **If it is found that the affected individual should be notified**, **Vision Super should consider:**

   a. **if a law enforcement agency is involved in investigating the breach –** if so, Vision Super should:
      - consult the investigating agency prior to making the details of the breach public;
      - be careful not to destroy any evidence that may be valuable in determining the cause of the breach or allow the investigating agency to take the necessary action; and
      - ensure that all records of the suspected breach are maintained, including the steps taken to rectify the breach and the decisions made concerning the breach.

   b. **how the affected individual should be directly notified –** i.e. by phone, letter, e-mail, or in person (if possible); and

   c. **who should be notified –** generally Vision Super should notify the affected individual/s, however in some circumstances they should contact the affected individual's guardian or representative (instead of, or in addition to, the affected individual) if it is deemed appropriate. In the event of a breach by a third party service provider, contractor or related body ("the third party") Vision Super should notify the affected individual, as Vision Super is the organisation that has the direct relationship with the affected individual/s and notification from the third party may confuse the affected individual;

6) **Notify the affected individual –** when notifying the affected individual, Vision Super should provide the affected individual with the following information:
   - Vision Super's response to the breach;
   - any assistance that Vision Super will offer the affected individual;
   - the contact details of Vision Super and any Vision Super employees that the individual may want to contact concerning the breach;
   - whether the breach has been reported to the OAIC or an investigation agency;
   - how the affected individual can make an internal complaint or a complaint to the OAIC (the OAIC has published an internal complaints guide, which is available on the OAIC website); and
   - any other sources of information that may be of use to the affected individual in protecting themselves from identity theft and other privacy related issues. For e.g. links to the OAIC and Attorney-General's Department website;

Step 5 – Prevent future breaches

To prevent future breaches Vision Super should conduct a review of its policies and procedures, which may include the following:

- conduct a post investigation audit of physical and technical security controls;
- a review of policies and procedures that relate to the breach, and a review of any other policies and procedures that may be at risk of a breach;
- regular training of employees with respect to information breaches;
- conduct breach 'drills' - to simulate what would happen during a breach;

- compile a list of the external service providers that Vision Super will use in the event of a breach - i.e. auditing firms, public relations firms, law firms etc.;
- review internal policies designed to prevent use of unregistered portable storage devices; and
- disabling transfer capabilities of any offending (registered) portable storage devices.

NOTE: once the prevention plan has been carried out it is important that there is an audit of the prevention plan, so as to ensure that the prevention plan has been fully executed.

_____

CEO

7 March 2014