Vision Super Pty Ltd

ABN 50 082 924 561

Maintaining data security

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 which is protected from misuse, interference, loss, and unauthorised access, modification or disclosure.

Vision Super does not transfer personal information to third parties unless:

- it is sure that those parties are subject to legal obligations substantially similar to the Australian Privacy Principles; or
- the individual consents to the disclosure; or
- the transfer is necessary to comply with a contractual obligation with the individual or a third party, which contract was entered into in the individual's interests; or
- the transfer is for the benefit of the individual in a situation where it is impracticable to obtain the consent of the respective individual, it is likely that the individual would consent to the transfer of their personal information, and Vision Super has taken steps to ensure that the transferee will handle the information in accordance with the Australian Privacy Principles.

Measures taken to protect the security of personal information consist of:

Physical Security

- Security access control and 24-hour monitoring of any building where personal information is held.
- Ensuring that outsourced computing and backup storage facilities meet or exceed industry accepted standards of physical access security.

Computer and Network Security

- Thorough data backup procedures.

- Maintenance and independent testing of network security devices to guard against unauthorised electronic access wherever a connection to a public network (eg. the Internet) exists.
- Implementation of industry recognised virus protection software.
- Secure destruction, de-identification, or erasure of all media holding an individual's information once no longer required for any legitimate purpose, or no longer required by or under an Australian law or court/tribunal order to retain the individual's information. For example, the destruction of microfiche and microfilm, the shredding of paper documentation and the permanent erasure of magnetic media, including data stored on computer equipment prior to disposal.
- The design of the Vision Super website, which ensures that no personal information is stored on the actual web server. Personal information transferred to, or from, Vision Super using web services is encrypted using industry recognised methods, without being recorded on the web server.
- Regular review of business risks, and mitigation through the maintenance of an approved and tested Business Continuity Plan.

Communications Security

- Security identification checks performed by staff before disclosure of any personal information over the telephone.

Personnel Security

- Staff access control and review procedures to ensure that only authorised, qualified and trained personnel have access to personal information and computing facilities.
- Confidentiality agreements between third parties that may handle personal information on behalf of Vision Super.
- Wherever appropriate, sensitive personal information is obscured through the use of non-identifying codes. For example, the use of member numbers instead of names, and coded medical categories instead of descriptions of medical conditions.

Vision Super conducts regular reviews of all security measures and procedures to ensure personal information continues to be properly protected.

_____

CEO
7 March 2014