

Policy Statement

Maintaining Data Security

Approved by: CEO
Issue Date: 10 December 2009

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 members rightly expect to be protected from misuse and loss, and from 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 National Privacy Principles, or
- the individual consents to the disclosure, or
- the transfer is necessary to comply with a contractual obligation with the member or a third party, which contract was entered into in the individual's interests, or
- the transfer is for the benefit of the individual; it is impracticable to obtain his/her consent; the individual would be likely to consent and Vision Super has taken steps to ensure the transferee will handle the information in accordance with the National 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 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 or erasure of all media holding personal information once no longer required for any legitimate purpose: eg. destruction of microfiche and microfilm, shredding of paper documentation and permanent erasure of magnetic media, including data stored on computer equipment prior to disposal
- design of the Vision Super website such 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 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 - eg. member numbers instead of names, 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.

Approved by the Chief Executive Officer on 10 December 2009