Privacy Policy

Purpose
The purpose of this policy is to define the guidelines to be used by SBH Solutions to ensure the privacy of individuals' personal information in its possession as laid out in the Privacy Act 1988 Privacy Amendment (Private Sector) Act 2000.

Scope
This policy applies to all employees within SBH Solutions. It also applies to any contractor who, while working within the business has access to information of a personal nature. Information gathered by an individual in the course of their work is not covered by the policy, except when it is published or recorded in a manner that makes the information public within the organisation.

Responsibility & Authority
The Managing Director is responsible for ensuring that the requirements of this policy are implemented and maintained.

Policy
There are a number of ways in which SBH Solutions receives information and details about private individuals, then stores it in databases, and uses it. Examples of these are resumes, warranty cards, direct mail lists, results from promotional campaigns, e-mail contacts. The policy is not technology specific and database includes paper as well as electronic storage methods.

Collection of Personal Information
- SBH Solutions will not collect personal information unless the information is necessary for one or more of its business functions. It will only collect this information by lawful and fair means, and where possible will maintain individual anonymity.
- Where reasonable and appropriate, it will advise that there is a Privacy Policy in place at the point where the information is being collected. It will advise the primary purpose for which such information is to be used.

Use and Disclosure
- SBH Solutions will use personal information gained only for the primary purpose for its collection except in the following circumstances:
  a) In direct marketing campaigns. In this event, SBH Solutions will include an option in its direct communication to allow the individual to opt out of any future direct communication. It will also clearly identify from whom the communication is sent, and an address.
  b) In product advice letters and as part of product recall policy. In these events, SBH Solutions will disclose personal information when it reasonably believes that a serious and imminent threat to an individual's or the general public's safety exists.
  c) Where the information is required to assist law enforcement agencies to perform their role.

Data Quality
- SBH Solutions will take every measure practical to ensure that its databases are maintained up to date.

Data Security
- SBH Solutions will take every measure practical to ensure that its databases are maintained and are secure from misuse. Access to electronic databases is restricted and those able to access personal information will be clearly identifiable by the System Administrator. Any computer not logged off when an employee leaves it, will have 'Screen Savers' passwords activated to start after 15 minutes.

Openness
- SBH Solutions holds to the values of openness, and will ensure that any person requesting information on the following will be given a written answer:
  a) What sort of personal information is held, and for what purposes.
  b) How the information is collected, held, used and disclosed.

Access and Correction
- SBH Solutions will provide access to personal information held on an individual upon written request, except in the following situations:
  a) Where the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings.
  b) Where providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations.
  c) Providing access would impinge on the privacy of others.
  d) Where providing access would reveal information generated of a commercially sensitive nature.
  e) Any number of reasons which contravene Australian criminal law.
- The type of access granted will depend on the information held, but will generally be on the company premises, and no copies will be taken. Should the information held be incomplete or inaccurate, the company will take reasonable steps to amend the information.
- The company will provide written reasons for denial of access, or refusal to correct personal information.

Identifiers
- SBH Solutions will not use as reference any identifiers (excluding an individual's name) associated with other organisations with which an individual has contact; nor will it disclose any such identifiers to third parties.

Anonymity
- Wherever it is lawful and practicable, SBH Solutions respects the individual's right to the option of not being identified when entering into transactions with the company.

Trans-border data flow
- SBH Solutions will not transfer personal information about an individual to someone in a foreign country, except in the following situations:
  a) The transfer is necessary for the performance of a contract between the individual and the company, or for the implementation of pre-contractual measures taken in response to the individual's request.
  b) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between SBH Solutions and a third party.
- SBH Solutions will take reasonable steps to ensure that information transferred will not be held or disclosed by the recipient in a way inconsistent with the National Privacy Principles.

Sensitive Information
SBH Solutions will as a matter of Policy not seek out or store sensitive information (as defined in Section 6 of the Privacy Act), except in one situation:
- In the recruitment process, note may be made of certain sensitive material, in particular membership of a professional or trade association, philosophical beliefs, criminal and general health information.
- Where sensitive material is gained or received, de-identification will be implemented as soon as this is practical. During the process of recruitment, significant personal information is gathered. Once the specified recruitment event is completed, all copies of the personal information of all those not recruited will be shredded, unless written agreement is reached with the individual to store that information on file for a maximum of six months.

Complaints / Request for Information Procedure
In the event of a complaint about a breech of the privacy provisions, or a request for information, being received by the company, the following procedure will apply:
- If the complaint is made in person, the individual will be requested to forward the complaint / request for information in writing to the Managing Director.
- The Managing Director will respond to the individual within 7 (seven) days of receipt of the complaint / request for information with the appropriate reply given company policy and the provisions of the Act. This response may be in person or in writing.
- Any further actions such as revealing actual information held will be coordinated by the Managing Director. Should the situation not be resolved at this point, the complainant will be directed to the Privacy Commissioner, where it will be handled under the relevant provision of the Act.
- A file of all correspondence and communication will be maintained by the Managing Director.

References
At all times where the Policy is unclear or does not cater for a specific instance, the provisions of the *Privacy Act 1988 Schedule 3 – National Privacy Principles*, shall be the reference.