TiCSA (South Australian Tourism Industry Council) Inc.

DATA BREACH POLICY

TiCSA (South Australian Tourism Industry Council) Inc is committed to protecting the personal information we collected.

This policy is a component of, and supports, our Privacy Policy.

We are required to protect personal information we collect from loss, unauthorised access and unauthorised disclosure (**data breach**).

Security of data

We are obliged under the Australian Privacy Principles to take such steps as are reasonable to protect personal information:

- from misuse, interference and loss
- from unauthorised access, modification or disclosure

We are also obliged to ensure the security of credit eligibility information.

All staff members must adhere to the data security requirements and procedures for client information as outlined in the Privacy Policy. A failure to provide adequate security may lead to an interference with the privacy of an individual.

Should we suspect or believe that a data breach has occurred we will undertake the following 5 steps:

- Identify
- Contain
- Assess
- Notify
- Review

1. Identify
We will maintain systems and procedures to ensure that any suspected or actual data breach can be identified, reported and escalated to management responsible for the implementation of the Data Breach Response Plan. Any staff member of SATIC who suspects a data breach has occurred must ensure that a Data Breach Report Form is completed and sent promptly to the CEO and a copy of the Communications Coordinator.

2. Contain
Once identified, we will take all reasonable steps that can be taken to contain that breach. We make a preliminary assessment of any remedial action we should take and provide that assessment to all relevant staff members within 24 hours.

Remedial action is anything we can reasonably do to stop the breach, prevent further similar breaches or prevent harm occurring to the individual whose data has been accessed or lost.

Examples of remedial action include:

- retrieving the personal data

- shutting down our system
- finding the lost device or file

3. Assess
The Data Breach Response Plan and the Data Breach Report Form provide for the proper assessment of the breach including:

- the type of information involved
- whether the breach can be remedied and the information recovered
- the identity and number of individuals affected or likely to be affected
- the possible financial, economic, social and emotional impact on any individual;
- the nature of the breach (i.e. –was it loss, access or disclosure of electronic or paper-based data and was it accidental or deliberate)
- the perpetrator of the breach (i.e. internal staff, contractors, third parties whether local or overseas)
- the risk of further breaches if remedial action not taken (i.e. is systemic problem or one-off)
- whether criminality evident (i.e. theft or hacking)
- whether the information was encrypted, de-identified or difficult to access

4. Notification
If we believe (not just suspect) on reasonable grounds that a data breach is likely to result in serious harm to any of the individuals concerned we will:

- Prepare the statement required by the *Privacy Act 1988* including the following information:
    - our identity and contact details;
    - a description of the breach we believe has occurred;
    - the kind of information involved in the breach;
    - recommendation about the steps the individuals should take in response and
    - if the data breach was caused by a third party service provider we engage, we will include their name and contact details.

- Provide a copy of the statement to the Office of the Australian Information Commissioner

- Provide a copy of the statement to each affected individual affected by means determined to communicate effectively and include additional information such as:
    - our response to contain the data breach and prevent its recurrence
    - any assistance we can offer to the individuals
    - that we have reported the breach to the Office of the Australian Information Commissioner and, if relevant, any law enforcement agency/ies
    - how individuals can make a complaint to the Office of the Australian Information Commissioner

5. Review
To prevent future breaches of the same kind, the Data Breach Response Plan must include a requirement for us to conduct a review of our policies, systems and procedures which may include the following:

- a post-investigation audit of physical and technical security controls
- a review of policies and procedures
- additional training of staff members including scenario practices
- identify external resources that may assist in to prevent future breaches, i.e. auditing firms, public relations firms, legal advisers
- review authority levels for access to and transfer of electronic data
- whether the Data Breach Response Plan was adequate.

Version 1, September 2018.