STRATEGIC SURVEYS PTY LTD

Data Privacy, Security and Management Policy 2018

ACN 625 521 459

STRATEGICSURVEYS

At Strategic Surveys, we take data privacy and security extremely seriously. The following document outlines our policy on how we gather, administer and maintain personal data through our survey and reporting systems.

1. Definitions

For the purposes of this document we include the following definitions:

- "Strategic Surveys" refers to Strategic Surveys Pty Ltd, ACN 625 521 459
- "Customer" refers to the client of Strategic Surveys – an individual or an entity - with whom we have a contract to produce and administer one or more survey programs.
- "Participant" refers to a survey user who is partaking in a survey program for the purpose of having a report or data analysis generated.
- "Respondent" refers to a survey user who is partaking in a survey program by request of, or in relation to, a participant. Can also be referred to as a "Rater".
- "Program" and "System" refer to the fully developed and managed set of surveys, administration, emails and generated reports that constitute the service Strategic Surveys provides to our clients. A Program can be one of many types, including:
    - 360 Program with or without manager approval, with Participant and Respondent feedback.
    - 180 Program with Participant and Manager (as Respondent) feedback
    - Single-user survey for self/team/organisational feedback
- "Data" refers to any information gathered during a survey and report program. This can be data provided as part of the administration process such as participant information, or data provided by the users of the survey themselves when accessing and providing feedback.

2. How data is collected

2.1. Program Administration

Certain participant and respondent (including manager) data is required to set up and administer a program. This includes participant name and email address, for the purposes of creating a unique and identifiable survey link for use by the participant only. There is the option for a program administrator to provide additional information such as gender, title, or other personal or demographic attributes.

2.2. Survey Participation

Data is collected whenever a participant or respondent completes a survey. This can include any data that the customer has requested be collected and is treated by Strategic Surveys as private and confidential information owned by the Participant and accessible only by themselves, a program administrator, or another entity explicitly authorised by themselves or a program administrator. This may also include application data such as user IP address, browser information, and user actions taken.

3. How data is stored and managed

3.1 Software
Data collected from the surveys is stored in a secure SQL database. This data can only be accessed via the participant survey link itself, or by an administrator of Strategic Surveys, or by the report generation software that will use it to compile the specified program reports.

3.2 Hardware Storage
We store all survey and customer data on private, secure Australian servers with full redundancy and data backups, with 99.9% uptime SLA.

3.3. Backups
6 hourly server-wide backups are performed that can be restored within 30 minutes, and are stored across redundant systems with guaranteed high availability.

3.4. Length of storage
For privacy and security reasons we recommend only storing online survey data in a de-identified format. We will store backups of data offline for a period of up to 7 years or as requested, and we will store de-identified data online for the same period. We provide csv exports and pdf reports of a survey round after completion and by default leave the storage of these results up to the customer.

3.5 Customised Solutions
If the customer, or their client, has specific or additional data storage and management requirements – such as their own private dedicated server or network that they need to run the system from – Strategic Surveys can work with their IT administrators and/or system engineers to build a customised hardware and/or software storage solution that meets their unique storage and management needs. The customised solution must still meet the minimum Strategic Surveys standards for data storage and management, as outlined above in sections 3.1 - 3.4, while including any additional requirements unique to the client.

4. Privacy

4.1. Confidentiality and Ownership of Data
Strategic Surveys treats all customer data as private and confidential, owned solely by the customer running the survey system and the participants themselves. We do not share or distribute any information collected from the surveys or portals with any third parties. No survey or participant data is shared or accessible by anyone other than the participant themselves, the program administrators and Strategic Surveys administrators, without the express consent of the participant or their representative. Personal and survey data is accessed by Strategic Surveys for the purposes of managing the surveys, and report generation only.

4.2. Isolation of Customer Data
We offer hosting of each customer's data on a private database separate from any other customers, which isolates user data. We also offer a dedicated account on our server for

each customer which creates a virtual 'cage' around all data and databases, preventing any cross-accessibility between customer data.

4.3. Application and Usage Data
User interactivity and application data, such as user IP address, internet browser used, and whether a survey email was read/opened, may be collected only for application management and support purposes and will never be shared with non-administrators.

4.4. Anonymity and Aggregation of Data
We strongly recommend anonymity and aggregation of data for reporting purposes when respondent feedback is included, however we will adhere to the policies and requirements of each individual customer in this area. We do require that all survey participants are informed on the status of anonymity of their responses prior to participating in any programs run by Strategic Surveys. If they are not a direct participant themselves, for example a nominated respondent in a 360 program, the email correspondence or the instructions in a survey should outline how their data will be used and displayed, and the respondent may then decline to participate.

4.5. Personal Information
We only collect personal information required to administer the surveys, primarily name and email address of the participant or respondent taking part in a survey program, and data entered by the participant or respondent in the survey itself. This survey data is defined by the questions in the survey itself and is entirely up to the customer designing and administrating the survey. User entered survey data is never given to any third party and never provided in any context except in the specified report and data analysis as outlined by the customer. The personal information (name, email address, demographic or other participant attributes) is only used to create a unique survey access identifier and customise the surveys – such as email correspondence and survey text elements - for the individual participant or respondent.

4.6. De-identification
By default, we automatically de-identify participant and respondent information (such as name and email address) 30 days after a survey program is completed and the program reports and data analysis have been generated. If requested, the information can be kept for future retrieval by the customer who owns the data, or for linking to future programs for said customer, for the period specified in Section 3.4. Our recommended practise is to store a backup of the identified data offline and if required, we can import it for comparison reporting purposes.

4.7 Opt-out option
All respondent surveys are set by default to include an 'opt out' link in their footer. This will immediately remove any personal information provided by the participant from the survey and remove the respondent from the program. We can disable this option if requested, but if we do so we will then require that all nominated respondents be given an alternative means of opting out if they request it.
We can also provide an opt out link to participants if requested which will remove them from the program.

4.8 Updating or Accessing Information

If you or your authorised representative wishes to access your personal information, we can be contacted at any point.

We can provide you with all details of your account, and exports of all personal and application data that we hold directly related to you. If you wish to modify any of this data and are an authorised administrator, you can access it via the administration portal. You can also request that we modify or remove any personal data directly from the system database, which we will do upon request.

5. Security

5.1. Hardware

The servers are fully secured with 24/7 monitoring and security hardening. No data is stored in a shared hosting environment; our servers are secured and isolated from any other users, with guaranteed resources and uptime dedicated to our survey software and databases only.

The servers are protected by both hardware and software firewalls, anti-virus and exploit monitoring, and 24/7 DDOS protection.

These services are provided by an authorised Australian company, which has a well-defined privacy and security policy and maintains their systems according to all latest standards.

5.2. Software

The administration and survey applications are written in PHP, HTML and Javascript, and adhere to the latest software standards (outlined in the Open Web Application Security Project) for protection against attacks such as SQL injection and other vulnerabilities that can be found in these languages. Vulnerability scans and penetration tests are performed regularly by an independent Australian Security company, and all software is regularly updated and tested to prevent any new vulnerabilities from occurring.

We enforce strict password strength measures for all users, with a minimum of 8 characters and at least one uppercase and lowercase letter and one number.

We also enforce login-blocking on both account/username and IP address to prevent password-guess attacks, where if a user fails to login with correct details a certain number of times they are blocked from the system.

We enforce Transport Layer Security through SSL certificates and https redirection for all site access, and do not permit the transfer of unencrypted data when using our surveys or administration/user portals.

We also offer fully isolated customer accounts, where each customer can have their website/subdomain and data on their own private account, isolated from any other customers data by CageFS, the industry leading account isolation software.

For more information regarding the technical specifications of our software security please contact us.

5.3 Customised Solutions

As with data storage and management in section 3, if the customer, or their client, has specific or additional security requirements, Strategic Surveys can work with their IT

administrators and/or system engineers to build a customised hardware and/or software security solution that meets their unique security needs. The customised solution must still meet the minimum Strategic Surveys security standards for application security, as outlined above in sections 5.1 and 5.2, while including any additional requirements unique to the client.

If you have any questions about our privacy or security policies, please contact us any time at support@strategicsurveys.com.au or via our website at www.strategicsurveys.com.au/contact-us/

Document Change History

Date	Change	Version
18/04/2018	New Privacy and Security policy to comply with the Australian Privacy Principles (APP) privacy policy guidelines	1.0
04/05/2018	Included new 'opt out' feature and automatic de-identification	1.1