

## **SurveyMonkey Anonymity and Security Statements**

### **Anonymity**

It is up to each survey creator to decide if they want to collect responses anonymously, or to capture respondents' personal information. Respondents' personal information can be captured by the survey creator in two ways: by expressly asking you for your personal details (name, address, etc.), and by configuring the survey to automatically capture your IP address and/or e-mail address.

SurveyMonkey provides survey distribution methods that range from e-mailing a survey link, embedding a survey on a personal or business website, using social networks to post survey links, and so on. All of these options allow the survey creator to collect responses anonymously. All collection methods permit the tracking of respondent IP addresses. Anyone using the E-mail Invitation collector could potentially track an e-mail address on the response.

We allow survey authors to disable the storage of e-mail addresses and disable IP address collection for all collection methods so that they can collect anonymous survey responses.

Survey creators may have their own privacy policies which apply to surveys that they create using our services and that detail how they handle your personally identifiable information. We encourage you to read any such policy, or to contact the survey creator directly to ask them any questions about their privacy practices. If the survey creator has not disclosed the collection method in the introduction of the survey, please contact him or her to verify if the response is anonymous.

Note that although survey creators may choose to collect responses anonymously, creators may still include specific survey questions that ask you for personally identifiable information. To review SurveyMonkey's privacy policy and how we handle respondents' personal information, click on the Privacy Policy link in the footer of our main SurveyMonkey site ([www.surveymonkey.com](http://www.surveymonkey.com)).

### **Security**

SurveyMonkey takes our user's security and privacy concerns seriously. We strive to ensure that user data is kept secure, and that we collect only as much personal data as is required to make our users' experience with SurveyMonkey as efficient and satisfying as possible. We also aim to collect data in the most unobtrusive manner possible. This Security Statement is aimed at being transparent about our security infrastructure and practices to help reassure you that your data is sufficiently protected.

If the URL of your survey contains <https://> at the start, your survey responses are sent to us over a secure, encrypted connection. Whether a survey offers this depends on whether the survey creator has enabled this feature on their account.

## **User Security**

SurveyMonkey utilizes some of the most advanced technology for Internet security commercially available today.

- SurveyMonkey requires users to create a unique user name and password that must be entered each time a user logs on. SurveyMonkey issues a session “cookie” only to record encrypted authentication information for the duration of a specific session. The session cookie does not include either the username or password of the user.
- When a user accesses secured areas of our site, Secure Sockets Layer (SSL) technology protects user information using both server authentication and data encryption, ensuring that user data is safe, secure, and available only to authorized persons.
- Passwords and credit card information are always sent over secure, encrypted SSL connections.
- Accounts which are SSL enabled ensure that the responses of survey respondents are transmitted over a secure, encrypted connection.
- We are PCI-DSS compliant.

## **Physical Security**

- Our data center is located in a SAS70 Type II certified facility.
- Data center staffed and surveilled 24/7.
- Data center secured by security guards, visitor logs, and entry requirements (passcards/biometric recognition).
- Servers are kept in a locked cage.
- Digital surveillance equipment monitors the data center.
- Environment controls for temperature, humidity, and smoke/fire detection.
- All customer data is stored on servers located in the United States.

## **Availability**

- Fully redundant IP connections.
- Multiple independent connections to Tier 1 Internet access providers.
- Uptime monitored constantly, with escalation to SurveyMonkey staff for any downtime.
- Database is log-shipped to standby servers and can failover in less than an hour.
- Servers have redundant internal and external power supplies.

## **Network Security**

- Firewall restricts access to all ports except 80 (http) and 443 (https).
- Intrusion detection systems and other systems detect and prevent interference or access from outside intruders.
- QualysGuard network security audits are performed weekly.
- McAfee SECURE scans performed daily.

## **Storage Security**

- All data is stored on servers located in the United States.
- Backups occur hourly internally, and daily to a centralized backup system for offsite storage.
- Backups are encrypted.
- Data stored on a RAID 10 array.
- O/S stored on a RAID 1 array.

## **Organizational Security**

- Access controls to sensitive data in our databases and systems are set on a need-to-know basis.
- We maintain and monitor audit logs on our services and systems (we generate gigabytes of log files each day).

- We maintain internal information security policies, including incident response plans, and regularly review and update them.

## **Software**

- Code in ASP.NET 2.0, running on SQL Server 2008, Ubuntu Linux, and Windows 2008 Server.
- Our engineers use best practices and industry-standard secure coding guidelines to ensure secure coding.
- Latest patches applied to all operating system and application files.
- Billing data is encrypted.

## **Handling of Security Breaches**

Despite best efforts, no method of transmission over the Internet, or method of electronic storage, is perfectly secure. Therefore, we cannot guarantee absolute security. If SurveyMonkey learns of a security breach or potential security breach, we will attempt to notify affected users electronically so that they can take appropriate protective steps. SurveyMonkey may also post a notice on our website if a security breach occurs.

## **Your Responsibilities**

Keeping your data secure also depends on you ensuring that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your system, to keep any survey data you download to your own computer away from prying eyes. We offer SSL to secure the transmission of survey responses, but it is your responsibility to ensure that that feature is enabled on your account.