Policy Center
SurveyMonkey
Precision Polling
SurveyMonkey Contribute
General Policies
Information
Security Statement
Requests & Forms

Security Statement

SurveyMonkey takes our users' 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.

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 SOC 2, Type II audited 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
- Environmental 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.

Questions?
If you have any questions about security on the SurveyMonkey website, please email us at support@surveymonkey.com.