How SurveyMonkey handles security

Commitment to trust

At SurveyMonkey, we process important, valuable, and confidential customer data on behalf of our customers. Our customers use our survey platform to collect employee performance reviews, commercially-sensitive market research data, confidential personal data from customers, and other critical information.

SurveyMonkey values the trust that our customers place in us to handle their data in a secure, respectful, transparent, and appropriate way. We have prepared this white paper about our security practices to add to this transparency.

At this time, this document primarily addresses SurveyMonkey's core survey service and does not necessarily reflect other services, such as Wufoo, SurveyMonkey Apply, SurveyMonkey CX, SurveyMonkey Engage, or TechValidate (although large portions will still be relevant to other services).

About us

SurveyMonkey operates an online survey platform as our core business, and also provides survey-related products and services. Most of our survey services are provided on a self-serve basis, which means that customers can create, distribute, and analyze their own surveys without any interaction with a human at SurveyMonkey.

Our survey services are provided via a software-as-a-service (SaaS) model, which means that all of your data is hosted on SurveyMonkey's servers and accessed through your web browser (or our mobile applications). When we refer to a "SurveyMonkey account" in this document, we are referring to an account that gives access to our core service. Our core service is available for free, as well as for a fee, under various subscription plans. Paid subscription plans are more fully featured than free accounts.

Contents:

Contents:

01. Your Data

Privacy and data handling

SurveyMonkey's services are predominantly self-serve, so customers have complete control over what sort of data they want to collect through SurveyMonkey. SurveyMonkey's Privacy Policy describes the types of data we collect from customers, how we use that data, and with whom we share that data in the course of providing our services. We also cover topics such as data retention, where data is physically stored, and cookies.

Data ownership

Under our user agreements, we maintain that any survey data you collect is owned by you, not us. If individuals within your organization hold separate self-serve accounts, we treat those individuals to be the owners of the data stored within their accounts per our user agreements.

Confidentiality

We also agree under our user agreements to treat your survey data as confidential information. This is in addition to the commitments we lay out in our Privacy Policy.

Security

Our Privacy Policy exists to say what we do with your data, but security is about ensuring that we are able to do what we say. The rest of this document focuses on the security measures that we employ to ensure that we are able to protect the information assets you have stored with us.

SurveyMonkey Global

SurveyMonkey Inc. is headquartered in the United States. We also have an entity in Ireland called SurveyMonkey Europe UC.

SurveyMonkey Europe UC contracts with our customers located outside of the United States. This is the reason you may sometimes see references to SurveyMonkey Europe UC in legal documentation.

02. Security controls

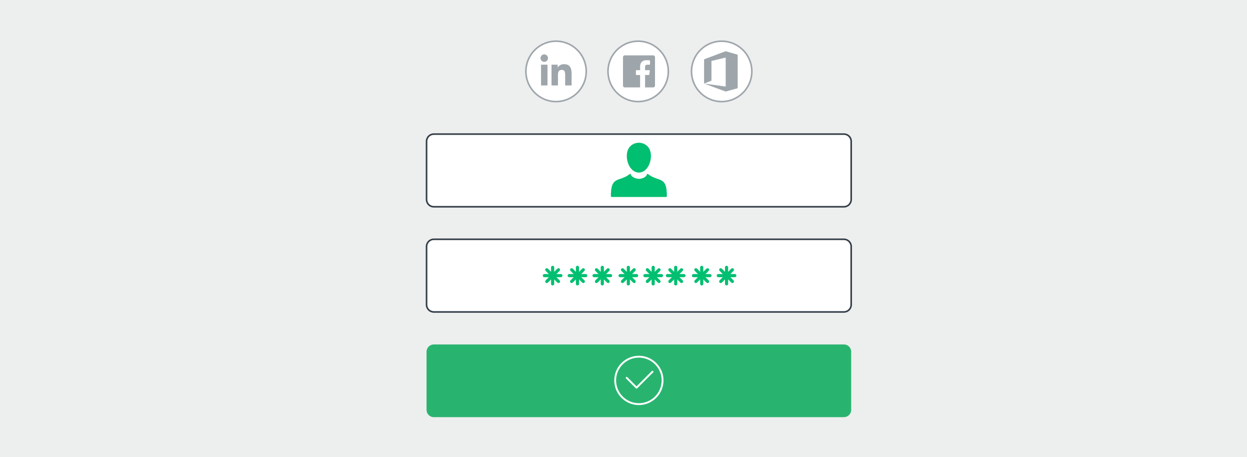
SurveyMonkey strives to adhere to industry best practices in handling our customer's sensitive and private data and complies with applicable privacy and consumer laws.

Secure in-transit communications

By default, all survey responses are collected over a secure HTTPS connection; however, survey creators can configure their surveys to collect responses over an HTTP connection. All other communications and traffic between an end user's web browser and the SurveyMonkey website are conducted over an encrypted connection using Transport Layer Security (TLS). SurveyMonkey works to maintain industry best standards implementing current encryption standards for all TLS traffic. Additionally, customers only have access to the data through the password-protected web application and API, never directly to the servers.

User authentication

Customers select an account username and password to use for accessing their data and surveys. Customers may also use their Google, Office 365, LinkedIn, or Facebook accounts to authenticate with SurveyMonkey (individual accounts only). SurveyMonkey Enterprise also supports single sign-on via SAML 2.0 (please see "Single Sign-On" section below) and partnerships with our supported identity providers. All logins are protected with TLS.



Passwords

Customer account passwords must have a minimum length (8 characters) and cannot be on a list of disallowed passwords. We also do not allow a user to use their username or email address as the password for any account.

We do not currently have a password reuse restriction or forced expiration, though these restrictions can be applied when a company chooses to use our Single Sign-On option (see below).

Customer passwords are stored in the database and hashed using multiple passes of SHA-256 with a unique 128-bit salt per user. Passwords are entered into the application using the HTML password field type, which obscures the password during entry.

Single Sign-On (SSO)

For users who prefer designating their own restrictions for password strength, reuse requirements, or forced expiry, we offer an option to incorporate Single Sign-On (SSO). SurveyMonkey supports SSO through SAML 2.0, allowing admins to manage access through corporate account credentials. For more information about this, please reach out to our sales team.

Team collaboration and Enterprise account management

Customers with Team or Enterprise plans can manage end user accounts contained in their plans. Enterprise plans have three roles: Primary Admin, Admin, and End User. Team accounts have two roles: a single Primary Admin and End Users.

The Primary Admin and any Admin can create new user accounts. They also have the ability to reassign or delete users' accounts, and change the role of individual users. Through reassigning an account, an Admin can also reset the End User account password. The Primary Admin also manages the billing details for the plan.

End Users have all the rights and permissions that a regular, non-Enterprise SurveyMonkey user has.

Logging and audit trails

Internally, we have comprehensive logging and auditing at all levels, including our application and infrastructure. SurveyMonkey ensures that all application logs are centrally managed, providing a unified logging framework for troubleshooting and analyzing user and systems events. The log management framework provides analytics tools, which present an interface to SurveyMonkey engineers, providing secure and efficient access to the required data while maintaining security best practices. Access to logs is protected through centrally managed authentication, restricting access to authorized SurveyMonkey personnel.

Team auditing and logging

Team Activity logging is an additional feature available via request for Team or Enterprise accounts. This will give Primary Admins and Admins of an Enterprise team visibility into granular activity and action logs across all the accounts in their team. Survey activity recorded in these logs include things like survey created, survey updated, collector created, collector updated, export created, data shared, survey transferred, survey deleted, and more. Administrative activity recorded in these logs includes things like admin re-assigned an account, admin deleted an account, admin exported data, and more. To learn more about this feature, please reach out to our sales team.

Data storage and encryption at rest

SurveyMonkey data is primarily stored within the United States across two facilities in the Western region. For customers with accounts in Canada, data is spread across two availability zones in the Central Canada region.

We encrypt data at rest using industry standard encryption techniques (e.g., AES).

03. Business continuity

Uptime and availability

SurveyMonkey uses a combination of best-of-breed monitoring technologies and services to ensure its quality of service to all end users. Key Performance Indicators (KPIs) are used to measure the quality of service for the various SurveyMonkey functions. Automated monitoring offers 24x7 immediate notification and escalation to our operational teams providing around-the-clock network, application, and server support.

Disaster recovery planning

SurveyMonkey's infrastructure has been designed to be highly available with primary and standby facilities hosting replicas and encrypted backups. In the event of a disaster at the primary facility, SurveyMonkey will engage in Disaster Recovery protocols. If escalated to the highest severity, SurveyMonkey's leadership and engineering teams will run through our Disaster Recovery Playbook to transition the site to the secondary facility.

To prepare for these disaster scenarios, SurveyMonkey engages in "Game Day" operations quarterly, where an artificial disaster scenario is introduced and the team responds accordingly. A full failover is executed once a year, during a scheduled maintenance window, to ensure the mechanics of our runbooks are current and to identify any areas for improvement.

Data retention

SurveyMonkey offers customers complete control over their data on a self-serve basis, with the ability to delete data within their accounts and, for Enterprise customers, to delete end user accounts. Customers may also request assistance from Customer Support to perform any of these actions.

Data that is deleted by users from within their account is permanently purged after a limited amount of time (typically 90 days) to allow users to restore mistakenly deleted data. Your data may be retained in monthly backups for up to three months before it is removed.

For information about our data retention practices, please see our Privacy Policy. Generally speaking, we retain survey data for as long as you have an account open, or until you request the deletion of the data or the account.

04. Policies and procedures

Information security plan

SurveyMonkey maintains a comprehensive written information security plan that covers all aspects of our information security practices, policies, and procedures.

Incident response plans and breach notification

SurveyMonkey has a formalized incident response policy that is generalized for all incidents, technical and physical. The policy describes the roles and responsibilities of each person during an incident, including security, engineering, operations, legal, marketing communications, customer operations, and management staff. The incident response policy covers the initial response to, and investigation, notification, communication, and remediation of events.

Should a security incident occur that affects customers, we will notify affected customers in accordance with our legal and contractual obligations. Please note that it is not always possible to notify customers immediately in the event of a security incident because of the time it takes to properly conduct an investigation and ascertain what occurred.

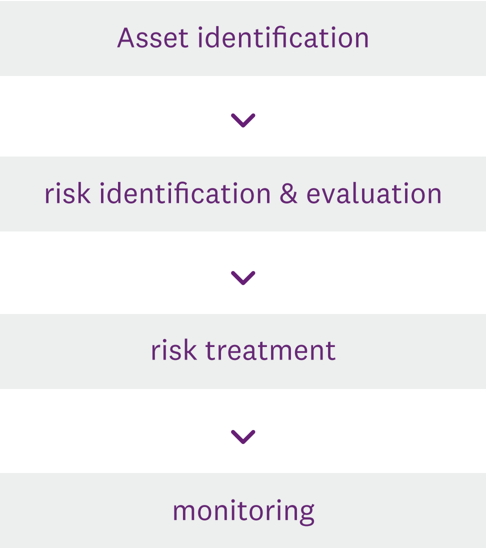
Customers are always welcome to report any actual or suspected incident to SurveyMonkey through our customer support team or security@surveymonkey.com.

Change management

SurveyMonkey maintains strict change control processes, ensuring a 360 degree view of production releases and all production changes. We maintain tight guidelines, processes built into our day-to-day workflow, and reporting that allows for proper checks and balances, all of which maintain our end user experience and security standards.

Risk management

The SurveyMonkey risk management process aims to promptly identify, evaluate and treat any potential risk that could affect the business and assets of the company. SurveyMonkey leverages a combination of industry-standard risk management practices that adhere to the following approach:



Asset identification

risk identification & evaluation

risk treatment

monitoring

Review and use of third-party service providers

We work with several third party providers that help us provide our services to customers, including email service providers, data center facilities, and credit card processors. We enter into confidentiality and data processing terms with each of these partners to ensure they comply with high levels of confidentiality and best practices in privacy and security standards, and we regularly review these standards and practices. For more information, please see our Privacy Policy.

05. Application security

Application engineering and coding practices

SurveyMonkey uses an agile development methodology. Our application is broken into multiple components, and each component has a team assigned to it. Development is performed in a development environment, which is separate and segmented from production, and then moved into test environments for thorough quality assurance reviews. Once the code is approved, it is then released into the production environment.

Our development team employs secure coding techniques and best practices that are described by The Open Web Application Security Project (OWASP). Developers are formally trained in secure web application development practices at least annually. We also use a peer-review model to ensure code complies with stated objectives. Important security functions, such as authentication and Cross-Site Request Forgery (CSRF) protection, are contained in shared code libraries that can be reused by multiple teams.

Additionally, SurveyMonkey's application security team is tightly integrated with the development process to ensure secure coding practices are being followed. The team has implemented security tooling and automation to ensure a secure software build and deployment.

Bug bounty program

SurveyMonkey maintains a private, invitation-only bug bounty program with a team of security researchers examining our application for vulnerabilities.

06. Network and physical security

Data center physical security

SurveyMonkey's information systems and technical infrastructure are hosted within world-class, SOC 2-accredited data centers in the United States and Canada. We have carefully chosen hosting providers that adhere to security and technical best practices while supporting a carrier neutral infrastructure. Physical security controls at our data centers include 24×7 monitoring, cameras, visitor logs, and entry requirements. Hosting facilities also feature environmental controls, and redundant power and connectivity systems (such as uninterrupted power supply and on-site generators).

Network security

User access

SurveyMonkey uses central user authentication to maintain identity and access management. This system manages all authentication and authorization to all corporate and production infrastructure, systems, and services. Strict access policies are maintained and reviewed on a quarterly basis. The reviews include but are not limited to user access lists, policy groups, and third party access reviews.

Additionally, SurveyMonkey maintains tight controls of employee onboarding and offboarding for all network and data access. Administrator (root/admin) level access to all devices is tightly controlled and accessed through infrastructure that provides reporting and tracking of all escalated privileged access.

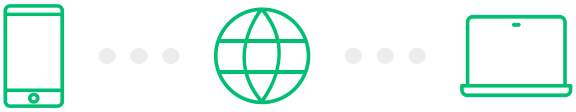
SurveyMonkey imposes password management requirements on its internal systems, including password lockout attempts, password complexity requirements, and password rotation intervals. All devices are centrally configured, managed, and monitored to meet industry best practices, including user restrictions, application security best practices, and default user management/removal.

Network infrastructure

The SurveyMonkey network is built on best-of-breed technology and best practices and is fully redundant at all layers. All network links and devices are monitored for traffic trends and health. The production network is physically and logically separated from all corporate and internet access via firewalls, edge router access lists, and VPN access. In addition, all administration of network devices is centrally managed and monitored for changes.

Remote access

All authorized SurveyMonkey employees and contractors with remote access privileges are required to connect to SurveyMonkey-controlled resources from an authorized computer using the approved VPN. Additionally, all such users are required to authenticate via the approved two-factor authentication method.



Vulnerability scans and patching

SurveyMonkey maintains a documented vulnerability management program which includes periodic scans, identification, and remediation of security vulnerabilities on servers, workstations, network equipment, and applications. Critical patches are applied to servers on a priority basis and as appropriate for all other patches.

We also work with third parties to conduct penetration tests at least annually. These tests mimic an outside attack as well as internal threats to ensure a full view of our environment.

Systems security

All SurveyMonkey servers are built from an internally certified “golden” image. This image is thoroughly scanned to ensure the most up-to-date patches are applied, default usernames and passwords are removed, and only the necessary services are running.

Active Directory Authentication

Active Directory Groups are used to provision roles to individuals, thus granting them access to the appropriate systems. The Active Directory also provides basic network services for the systems such as DNS and NTP.

Employee devices

Mobile devices are not permitted to connect to the SurveyMonkey production network.

Employees are only permitted to access the SurveyMonkey corporate network with company issued and maintained computers. All issued computers by default are running management software, up-to-date antivirus protection, and are fully encrypted.

07. Administrative and organizational security

Security team

SurveyMonkey has a dedicated Trust & Security organization, which focuses on application, network, and system security. This team is also responsible for security compliance, education, and incident response. The team reports directly to the Chief Information Security Officer (CISO) and works closely with the legal and operations team.

Incident response team

SurveyMonkey's Trust & Security team leads a trained Incident Response Team (IRT), which includes members of all integral functions across the business. This cross-functional IRT conducts tabletop sessions regularly and maintains a well-defined, organized approach for handling any potential threat to the information on SurveyMonkey systems, computers, and data, or on supplier/vendor, partner, or affiliate systems.

Human resources

Employee confidentiality obligations

All employees are required to sign a non-disclosure agreement when they are hired. Our policies, non-disclosure terms, and security trainings stress the importance of maintaining the confidentiality of customer data.

Employee confidentiality obligations

All new employees have a 7-year criminal background check performed on them at the time of hire, where permissible under local laws and regulations in the country in which the employee works.

Employee training

Security awareness training is conducted upon hire and we regularly engage our employees in additional training throughout the year. Prior to granting access to systems, employees are required to complete additional compliance and best practice trainings and to acknowledge their understanding of our acceptable use policies. Employees are also trained in initiating our incident response plans, if needed.

08. Certifications and compliance

Regulatory compliance standards

PCI DSS 3.2

A third-party Qualified Security Assessor (QSA) assesses SurveyMonkey's compliance with Payment Card Industry Data Security Standards annually.

HIPAA

SurveyMonkey enables covered entities to collect Protected Health Information (PHI) in online surveys in a way that permits compliance with the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA). This legislation only applies to entities collecting health information in the United States, not in other territories. As a business associate to covered entities, SurveyMonkey has adopted measures to ensure that we remain in compliance with HIPAA and any business associate agreements we enter into. SurveyMonkey allows our U.S. users to collect PHI in surveys if they have a HIPAA-enabled account and a business associate agreement in place. For more details, visit our HIPAA overview page, where you'll also find some best practices for using our features in a HIPAA-compliant way.

ISO 27001

SurveyMonkey has achieved ISO/IEC 27001:2013 (ISO 27001) certification, one of the most globally recognized information security standards defined by the International Organization for Standardization (ISO). The ISO 27001 certification audit was conducted by BSI, the British Standards Institution. Focused on continuous security and compliance, the certification requires controls audits throughout the year, with an annual inspection by BSI to ensure ongoing compliance.

How can SurveyMonkey help you unlock the value of your data?

Looking for an enterprise plan for your team, or want to consolidate SurveyMonkey usage across your entire organization? We offer flexible plans and pricing to fit your needs.

Contact us to learn more: www.surveymonkey.com/business