Security Statement

Security

- Authentication: The safety of your account identification information is taken very seriously and is always encrypted in transit and at rest. Account passwords are subject to minimum complexity requirements. Login is required to access collected data and files by default.
- Authorization: Once authenticated, only your account, or sub-user accounts with correct permissions, will be able to perform actions on your data by default. We also offer secure options to share your results. We strive to maintain as tight controls on actions as possible. You may further customize your user and form permissions.
- Accounting: Access and activity to accounts and data are routinely logged and analyzed. This information is then regularly used for security reviews and monitoring, as well as performance maintenance. Major activity in your account is also logged and viewable online.
- Encryption: All data stored in your account, including data you collect with your forms, is encrypted at rest using the AES-256 encryption algorithm.

System and Network Security

- All Formsite servers are colocated exclusively in a cloud-based architecture with Amazon Web Services (AWS) using their datacenters with hosting in the United States. Find complete information on AWS Security on their security page. In addition to our own staff, AWS provides expert support and system maintenance.
- Formsite uses high-grade SHA-256 RSA encryption for secure (https) connections over TLS, the same level of security used by banks and other financial institutions. The AES-256 encryption algorithm is used to encrypt data at rest.

- High performance, stability, and DDOS mitigation are achieved through the use of load-balancing on public-facing servers, as well as redundant processing instances and databases across different physical locations. This allows us to support high traffic loads across our user base with high uptime.
- Formsite servers are routinely monitored and tested by internal and external PCI and system scans, and kept up to date with important security patches and software. Automated monitoring is also in place with the ability to alert Formsite personnel.
- Secure network access is enforced by multi-tiered firewalls, custom system configurations, and multi-zoned networks.

Administrative Security

- All Formsite personnel are trained and regularly updated with the latest best practices regarding security and threat management.
- Access to Formsite resources is reserved solely for employees of Formsite, with minimal access permissions as needed.
- Activity on Formsite servers and networks is constantly logged and audited. Access to systems and data is highly restricted to only essential skilled personnel, and activity is both tightly controlled and monitored. Our staff also use best security standards, including two-factor authentication, private key-protected secure shell, secure VPN, etc., where possible.

Business Continuity and Disaster Recovery

- 24/7 monitoring and intrusion prevention systems are enacted for all public-facing services.
- Robust alert systems, secure processes and systems allow vital Formsite personnel to respond to issues within minutes at any time.
- Disaster recovery plans are in place, reviewed regularly, and distributed to all necessary Formsite personnel.
- Our system and network architecture provide a high degree of fault tolerance and recovery, both in security and performance. Important systems have redundancies in place to support fail-over processes and are also backed up routinely.
- Backups of all vital systems and data are taken regularly, and copied as appropriate to secure locations in order to provide contingencies across multiple systems and locations.

- Results data can be exported from your account, allowing you to create personal backups.

PCI Compliance

- Formsite is PCI 3.2 compliant. Our servers pass routine PCI compliance scans and we will provide our scan certificate upon request.
- We are PCI compliant with respect to the handling of billing information for Formsite accounts.

Responsible Usage

Formsite offers many advanced features and functionality. Therefore, security of your data also relies upon your responsible usage. We provide many features, as noted above, to help protect your data. Responsible usage includes, but is not limited to, keeping your passwords and sensitive account information safe and handling your results data safely. Any data you distribute should be as limited in scope as possible and use relevant security features, such as password protection, where possible. In addition, your data security also relies upon the security of any devices or networks you use to access your Formsite account and data. This includes keeping your computer or device up to date with security patches, enforcing user security standards, and storing and deleting downloaded files safely. For more information on the responsibilities of using Formsite, also see our Terms & Conditions.