Digsite Security

Digsite's most important concerns are the protection and reliability of customer data. We know your confidential information is extremely important to you and your business, and we're very protective of it.

Physical Security

- All Digsite data is stored in highly secure Amazon Web Services' data centers. The AWS infrastructure puts strong safeguards in place to help protect customer privacy.
- Nondescript AWS facilities help maintain low profile.
- Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.
- All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
- Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All physical access to data centers by AWS employees is logged and audited routinely.
- AWS manages dozens of compliance programs in its infrastructure.

Data Security

- Digsite uses Transport Layer Security (TLS) encryption (also known as SSL or HTTPS) for all transmitted Internet data.
- Customers may opt to password-protect their communities, or have unique ID links that are difficult to guess.
- All server volumes and backups are encrypted at rest using strong encryption (AES-256-XTS).
- Digsite maintains a set of annually rotating master keys within the AWS Key Management System. These master keys are used to generate a rotating set of secondary keys, with which the server data are actually encrypted. This provides envelop encryption for all Digsite data at rest and is also SSAE-16SOC1 Types 1, 2 and 3 attested.

Software Security

- Digsite products enable customers to control the individual permissions of their accounts and communities.
- All Digsite accounts are password protected, and all data are replicated in real-time.
- Passwords are salted, then hashed and stored, making them unknown to any Digsite employee.
- Digsite IDs may be linked to the customer's single sign-on services.

Credit Card Safety

- Digsite uses secure third-party services by Authorize.net for online credit card payment processing.
- We do not record or store credit card information at our site or on our servers.

Password Protection Measures

- Digsite will never ask for any user password. All user passwords are hashed and thus unusable.
- In order to block unauthorized access through password guessing, our systems disable account access after six invalid attempts. Once an account has been deactivated, the account stays deactivated for ten minutes (and reset each time a new log in attempt is successful).
- Digsite has an eight-character minimum for user passwords.
- Digsite has a self-service password reset option. This option sends users an email that includes a link to create a new password.

Log Files

- Log files contain requestor IP address, protocol, request, result, and other information. Logs are stored on each device.
- Logs are typically kept at least 90 days, and may be used for forensic analysis.
- Our logging and monitoring framework allows isolation of an incident to a specific customer if a security incident has been declared.

File Backups

- All participant data is backed up across servers (immediate upon collection) by Amazon Web Services – US West Region.
- Every backup file is encrypted using envelope encryption via the AWS Key Management System with an advanced crypto method (AES-256-XTS) using a rotating set of large keys.
- Completed backups are retained for one year. Backups of the entire Digsite Services are retained for one year. However restoration of this data is only for disaster recovery. The backups are electronic (no tape).
- Upon termination of a service agreement, customer data typically is retained to allow the customer access to download data. After termination of a service agreement, there is no guarantee that data will be recoverable.

Storage Device Decommissioning

- When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals.
- AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process.
- All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

Communications

- Community participants submit data using HTTPS (TLSv1.2 with AES 128/256 depending on browser) to the front-end web server.

Employee Access

- No Digsite employees ever access customer information unless required for support reasons.
- Digsite Customer Support may ask for personal information before accessing a user’s account, if the request is being made by live chat, phone, or email. However they will never ask for a user’s password. Passwords are salted-hashed values and not viewable by any Digsite employee.

Security Risk Analysis

- Digsite receives a third-party assessment of its privacy and security practices on an annual basis to identify potential threats and vulnerabilities to the confidentiality, integrity and availability of customer information.
- Digsite obtains regular intrusion detection and vulnerability scans of its system.
- Digsite complies with HIPAA privacy, security and breach notification rules.

Need to Report a Security Incident?

- Please contact monika@digsite.com. Digsite will assign a case manager who will conduct a thorough review of the incident and provide the findings to the user that requested the review.

Contact Us

Have a question, concern, or comment about Digsite security? Please contact monika@digsite.com