Filestack Idera Security Statement

Filestack, Inc., a Delaware corporation ("Company"), is committed to respecting and protecting the privacy of its customers, partners and website visitors (collectively "You" or "Your"). For more information about our Privacy Statement, please click here.

The security of your personal information is very important to the Company. We use robust security measures, which encompass both technical and organizational security controls, to prevent data loss, information leaks, or other unauthorized data processing operations.

By default, requests that modify existing files or account settings are authenticated. Requests are authenticated by checking a policy string that is signed by a shared secret. Applications can be configured on an individual basis so that every request is authenticated. All security settings are configurable in the Developer Portal.

Authentication and authorization against our APIs relies on Base64URL-encoded JSON “policies” and HMAC-SHA256 “signatures”. The policy determines which actions are authorized and the signature authenticates the policy.

Domain Whitelists for Upload:

Domain whitelists prevents File Picker from being embedded on unapproved websites. Whitelisting works by blocking requests that don’t contain an approved domain in the “Origin” header. It’s one way of securing your solution and your resources, so others don’t attempt to piggyback on your account.

Domain Whitelists for Delivery:

Delivery domains whitelists provide developers with the ability to provide a list of domains from where their files can be downloaded from. This will limit abusers that either steal API keys or use someone else’s files on their websites.

For example, the Company requires that its processors and sub-processors (collectively, "Vendors") have implemented and maintain a security program in accordance with industry standards, specifically the Company Vendors shall include the following security program:

I - Physical Access Control: Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms where personal data processing systems are located. Vendors have implemented the following controls:

1. prevent unauthorized individuals from gaining access to the processor's premises.
2. restrict access to data centers were data servers are located.
3. use video surveillance and intrusion detection devices to monitor access to data processing facilities.
4. ensure that individuals who do not have access authorization (e.g. technicians, cleaning personnel) are accompanied at all times when accessing data processing facilities.

II – System Access Control: Data processing systems must be prevented from being used without authorization. Vendors have implemented the following controls:

1. implement measures to prevent unauthorized personnel from accessing data processing systems.
2. provide dedicated user IDs for every authorized personnel accessing data processing systems for authentication purposes.
3. assign passwords to all authorized personnel for authentication purposes.
4. ensure that all data processing systems are password protected to prevent unauthorized persons accessing any personal data: (a) after boot sequences; and (b) when left unused for a short period.
5. ensure that access control is supported by an authentication system.
6. have implemented a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password, and requires the regular change of passwords.
7. ensure that passwords are always stored in encrypted form.
8. implement a proper procedure to deactivate user accounts when a user leaves the processor (or processor function).
9. implement a proper process to adjust administrator permissions when an administrator leaves the processor (or processor function).

III – Data Access Control: Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and personal data must not be read, copied, modified or removed without authorization in the course of processing or use and after storage. Vendors have implemented the following controls:

1. ensure that personal data cannot be read, copied, modified or removed without authorization during processing or use and after storage.

2. grant data access only to authorized personnel and assigns only the minimum data permissions necessary for those personal to fulfil their duties.
3. ensure that the personnel who use the data processing systems can access only the data to which they have a right of access.
4. restrict access to files and programs based on a "need-to-know-basis".
5. store physical media containing personal data in secured areas.
6. have measures in place to prevent use/installation of unauthorized hardware and/or software.
7. have established rules for the safe and permanent destruction of data that are no longer required.

In addition, the Company requires its Vendors (i) to maintain a list of sub-processors that may process the Personal Data of Vendor's, and make available such list to the Company; and (ii) to require all sub-processors to abide by substantially the same obligations as Vendor under the Company Data Processing Agreement for Vendors.

The Company incorporates encryption, incident management, network and system integrity, and availability and resilience requirements into its security program.

The Company uses standard security protocols mechanisms to exchange the transmission of sensitive data such as credit card details. When you enter sensitive personal information such as your credit card number on our site, we encrypt it using Secure Socket Layer (SSL) or Transport Layer Security (TLS) technology.

In the event that your personal information is acquired, or is reasonably believed to have been acquired, by an unauthorized person and applicable law requires notification, the Company will notify you by e-mail or mail. The Company will give you notice promptly, consistent with the reasonable needs of law enforcement and/or the Company to determine the scope of the breach and to investigate and restore the integrity of the data system.

If you have additional questions about privacy, please contact us at compliance@filestack.com