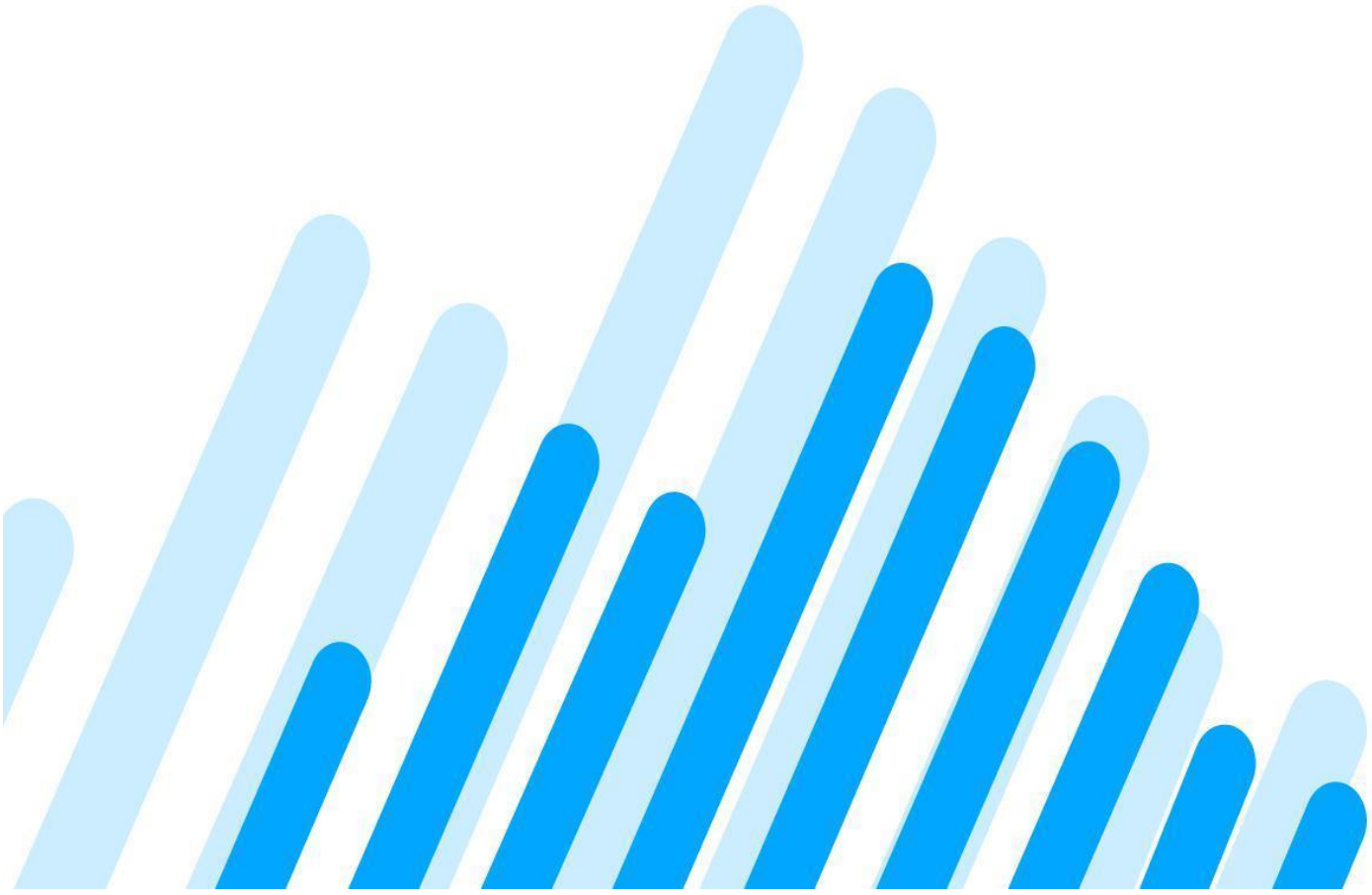
Cloudamize

Cloudamize Security Overview and FAQ



Cloudamize Security FAQs

How does Cloudamize Protect Personal Data?

Cloudamize intends not to collect any Personally Identifiable Information (PII) about its customers unless it is explicitly given this information by the customers themselves (either directly or via one of the APIs provided as part of the Cloudamize application).

In cases where PII is passed to Cloudamize that was not intended to be passed by the customer, it is the intention of Cloudamize to destroy this data as soon as it is identified. Discovery of any unintended PII data should be an immediate Security Incident to be dealt with appropriately by the CSWG.

For More information see Cloudamize Master Security Policy – Cloudamize Information Security Policy

How Does Cloudamize Protect the Data Once it is Collected?

All Customer Data should be kept entirely within the Cloudamize Application Hosting Cloud, such that it is only accessible either by Cloudamize personnel who have approved access to the machine instances running within the Cloudamize Application Hosting Cloud (via the Cloudamize Application Hosting Cloud firewall) or by the applicable customer via available Cloudamize SaaS application or Cloudamize APIs. At no point, will Customer Data be shared with any third parties.

Customer Data should not be downloaded to any local physical data storage outside of the Cloudamize Application Hosting Cloud by Cloudamize personnel, unless downloading this data is explicitly approved by the customer (for example, when troubleshooting an issue as part of a customer engagement).

Customer Data should be maintained exclusively within secured databases within the Cloudamize Application Hosting Cloud, with firewall settings such that no public ports are open to the greater internet outside of the Cloudamize Application Hosting Cloud for the machines hosting those databases and their replicas.

For More information see Cloudamize Master Security Policy – Cloudamize Information Security Policy

How Does Cloudamize Respond to a Security Incident?

A customer-specific Information Security Incident has occurred if any of the following conditions hold true:

- Customer Data has been exposed to any party not noted in the 'Information Access Policy' section.
- Customer Data has been downloaded by any party not noted in the 'Information Access Policy' section.
- Unauthorized access to a Cloudamize database within the Cloudamize Application Hosting Cloud has been detected.

In these circumstances, the following procedure will be followed:

- The POCs for the affected customer will be notified immediately.
- The disposition of the exposed of downloaded data will be included in the notification.

- Any information about whom the data was exposed to will be included in the notification.
- A Root Cause Analysis will be performed to evaluate how the data was exposed, and how this exposure will be prevented in the future.
- The action items from the Root Cause Analysis will be executed to properly secure the data.

For More information see Cloudamize Master Security Policy – Cloudamize Incident Response Policy

How Does Cloudamize Secure the Data That is Stored in the Cloud?

All systems used to support the Cloudamize SaaS Application (including databases, web servers, data processors, and back-end endpoints) should be hosted exclusively within the Cloudamize Application Hosting Cloud (maintained within Amazon Web Services, Microsoft Azure, Google Cloud Platform).

A full document of the security features provided by AWS is available here:
http://aws.amazon.com/security
Their Terms and Conditions can be found here:
https://aws.amazon.com/service-terms/

A full document of the security features provided by Microsoft Azure is available here:
https://www.microsoft.com/en-us/TrustCenter/Security
Their Terms and Conditions can be found here:
https://azure.microsoft.com/en-us/support/legal/

A full document of the security features provided by Google is available here:
https://cloud.google.com/security/
Their Terms and Conditions can be found here:
https://cloud.google.com/terms/

For More information see Cloudamize Master Security Policy – Securing the Cloudamize Application Hosting Cloud Policy

What is the Cloudamize Privacy Policy?

Cloudamize, Inc. ("Cloudamize") is committed to protecting the privacy and security of individuals and entities and their respective information and data who register to use and otherwise purchase the right to access and use the Purchased Products ("Customers", "you" or "your"). This Terms of Service Privacy Addendum ("Addendum") describes Cloudamize's collection and use of data and information, including Your Data and your Personally Identifiable Information (defined below), collected from or provided by you via Cloudamize's website, including all associated webpages, at https://www.cloudamize.com/ (collectively, the "Web Site") or in connection with your use of or access to the Purchased Products. Capitalized terms not otherwise defined herein shall have the meaning attributable to them in the Terms of Service. By agreeing to the Terms of Service or otherwise using or accessing the Products you hereby agree to be bound by the terms and conditions set forth in this Addendum as well.

For More information see Cloudamize Master Security Policy – Cloudamize Information Security Policy

What Data is Sent to the Cloudamize Servers?

When registering to use the Purchased Products (including in connection with the creation of an Account) or in connection with the submission of an Order Form, Cloudamize requires you to provide Cloudamize with personal contact information, such as name, company name, address, phone number, and email address, which information includes Personally Identifiable Information ("Required Contact Information"). When purchasing any Products, Cloudamize may require you to provide the Company with financial qualification and billing information, such as billing name and address, credit card number, and the number of employees within the organization that will be using the Purchased Products ("Billing Information"). Cloudamize may also ask you to provide additional information, such as company annual revenues, number of employees, or industry ("Optional Information").

Required Contact Information, Billing Information, and Optional Information about Customers are referred to collectively as "Data About Cloudamize Customers".

Cloudamize also collects certain Service Analyses for the reasons set forth in the Terms of Service, and may collect your Keys or other credentials, if provided by you to Cloudamize.
Additionally, Cloudamize may collect your Personally Identifiable Information when you:

- Submit a service request or a technical support question to an employee or agent of Cloudamize; or
- Otherwise expressly provide Cloudamize with your Personally Identifiable Information.

For More information see Cloudamize Master Security Policy – Cloudamize Information Security Policy

How Does Cloudamize Use the Information It Collects?

Cloudamize uses Data About Cloudamize Customers to perform its obligations and duties and otherwise provide you with the Purchased Products. Cloudamize may also use Data About Cloudamize Customers for marketing purposes, such as to provide you with information concerning other Products that you may be interested in.

Cloudamize uses credit card information solely to check the financial qualifications and collect payment from prospective Customers and Customers.
In addition, Cloudamize may use your Personally Identifiable Information for the following purposes:

- To respond to your service requests or technical support questions;
- To verify that you are an Account holder or to provide you details about your Account and who are your Authorized Users;
- To provide you with personalized information about Cloudamize.

For More information see Cloudamize Master Security Policy – Cloudamize Privacy Policy

Does Cloudamize Share the Data That It Collects?

Service Providers:
Cloudamize may share Data About Cloudamize Customers with Cloudamize's contracted service providers so that these service providers can provide services on our behalf. Cloudamize may also share Data About Cloudamize Customers with Cloudamize's service providers to ensure the quality of information provided. Unless described in this Addendum or the Privacy Policy, Cloudamize does not share, sell, rent, or trade any information with third parties for their promotional purposes.

Business Partners:
From time to time, Cloudamize may partner with other companies to jointly offer products or services. If you purchase or specifically express interest in a jointly-offered product or service from Cloudamize, Cloudamize may share Data About Cloudamize Customers collected in connection with your purchase or expression of interest with our joint promotion partner(s). Cloudamize does not control our business partners' use of the Data About Cloudamize Customers we collect, and their use of the information will be in accordance with their own privacy policies. If you do not wish for your information to be shared in this manner, you may opt not to purchase or specifically express interest in a jointly offered product or service.

For More information see Cloudamize Master Security Policy – Cloudamize Privacy Policy

How Does Cloudamize Protect Customer's Data?

Cloudamize uses commercially reasonable measures to protect Your Data from unauthorized disclosure or from being obtained in an unauthorized manner. Cloudamize uses a combination of firewall barriers, data encryption techniques and authentication procedures, among others, to maintain the security of your online session and to protect your Personal Information, Account Information and our system's security measures to protect Your Data from unauthorized access, maintain data accuracy, and help ensure the appropriate use of Your Data.

For More information see Cloudamize Master Security Policy – Cloudamize Privacy Policy

Who Has Access to Client Data?

All Customer Data should only be accessible by the following parties:

1. Active user accounts associated with that specific customer's organizational account within cloudamize.com/login.
2. Cloudamize personnel who have approved access to the machine instances running within the Cloudamize Application Hosting Cloud.
3. Cloudamize personnel who have approved access to the customer's organizational account within Cloudamize.com/login (including Customer Success representatives).

No customer user account should have access to any Customer Data besides data associated with their own organization.

The membership for groups (2) and (3) will be audited regularly to ensure only appropriate Cloudamize personnel has access to any Customer Data.

Any access to Customer Data via either Cloudamize.com/login or via direct access to the Cloudamize Application Hosting Cloud should be audited appropriated to track which user accessed the data and when the request was made.

Any access of Customer Data should be performed via an SSL-encrypted channel on either a wired LAN or via a private, password-protected wireless LAN. SSL security will be verified on a quarterly basis by going to https://www.ssllabs.com/ssltest/ with the results be sent to devopsgroup@cloudamize.com. The results and methodologies shall be reviewed on a quarterly basis by the CSWG.

Information Disposal Policy

Cloudamize will store customer data for 90 days after completion of the subscription period and then archive / delete the data.

In instances where Customer data needs to be destroyed immediately, the following practices are in place:

- For data contained within the Cloudamize Application Hosting Cloud, the data in question will be removed from its corresponding database using the best practice for the corresponding technology. All logs with the corresponding data will also be deleted to ensure the content is unrecoverable.
- For data outside of the Cloudamize Application Hosting Cloud, the data in question will be removed via the data destruction process described in the Cloudamize Physical Security Policy.

Does Cloudamize Have a Disaster Recovery Plan?

Cloudamize will ensure business continuity in the instance of a disaster or service outage (the potential dispositions of which are also described in the Disaster Recovery Policy). The implementation of this policy can be invoked by any member of the Cloudamize Security Group or Cloudamize Management Team. Once an emergency has been declared in accordance with this policy all media, social media or public statements shall be routed through Cloudamize's Marketing Director and/or a member of the Cloudamize Management Team.

For More information see Cloudamize Master Security Policy – Cloudamize Disaster Recovery Plan and Business Continuity Plan

How does Cloudamize Test Its Policies?

Testing Objectives:
To ensure the effectiveness of this policy the following exercises will be conducted annually:

1. Evacuation Drills (in accordance with the buildings safety policy)
2. Emergency Notification Tests
3. Application Recovery Tests
4. Remote Access Tests
5. Business Relocation Tests
6. Business Disruption Tests
7. Ability to Recover Vital Data Tests

The results of these tests shall be maintained by the CSWG and made available to the Cloudamize Management Team. The Cloudamize Management Team is the singular authority on the dissemination of these tests to any external entity.

For More information see Cloudamize Master Security Policy – Testing and Policy Review

How Does Cloudamize Train Personnel

All new Cloudamize Employees (and affiliated contractors) are expected to receive training on the Cloudamize Security Policy within seven (7) days within being hired. The Training is composed of the following units:

- Review of Cloudamize Information Security Policy
- Review of Cloudamize Physical Security Policy
- Review of Cloudamize Privacy Policy
- Review of Cloudamize Network Security Policy
- Acceptance of Cloudamize Personnel - Acceptable Use Policy
- Signature of Cloudamize Security Training - Sign-Off Form

For existing Cloudamize Employees, they are expected to receive a refresher of the Cloudamize Security Policy once a year, which includes the following:

- Discussion of all changes to policy in the last 12 months.
- Re-review of all Cloudamize Security Policy Subdocuments
- Signature of Cloudamize Security Training - Sign-Off Form

For More information see Cloudamize Master Security Policy – Cloudamize Security -Personnel Training