mimecast

CyberGraph Service TOMs

Last Updated June 2024

This document describes technical and organizational security measures and controls implemented by Mimecast to protect the Personal Data Customers entrust to us as part of the Mimecast CyberGraph.

- Within this document, the following definitions apply:
  "Customer" means any subscriber to the Mimecast CyberGraph Service.
- "Mimecast CyberGraph Service means the Service provided by Mimecast to our Customers further described in the Agreement.
- "Customer Data" means any information provided or submitted by the Customer that is processed by the Mimecast CyberGraph Service.
- "Personal Data" means any information relating to an identified or identifiable natural person.
- "Personnel" means Mimecast employees and authorized individual contractors/vendors.

1. **Organization of Information Security**
   Objective:
   To outline Mimecast's information security structure.

   Measures:
   a. Mimecast employs full-time dedicated trained and/or certified security Personnel responsible for information security.
   b. The information security function reports directly to the Mimecast senior leadership team.
   c. Mimecast has a comprehensive set of information security policies, approved by senior management and disseminated to all Personnel.

d. All Mimecast Personnel have signed legally reviewed confidentiality agreements.

e. All Mimecast Personnel are given training in information security.

2. Information Security Management System

Objective:

To demonstrate Mimecast's commitment to manage the assessment and treatment of these risks and to continually improve its information security.

Measures:

Mimecast has deployed an ISMS (Information Security Management System) that serves as the foundation of our information security practices.

3. Physical Access

Objective:

To protect the physical assets that contain Customer Data.

Measures:

The Mimecast CyberGraph Service is hosted with the Amazon Cloud environment. Amazon's description of their data center physical security controls can be found here: **https://aws.amazon.com/compliance/data-center/controls/**

4. System Access

Objective:

To ensure systems containing Customer Data are used only by approved, authenticated users.

Measures:

a. Access to Mimecast systems is granted only to Mimecast Personnel and/or to permitted employees of Mimecast's subcontractors and access is strictly limited as required for those persons to fulfil their function.

b. All users access Mimecast systems with a unique identifier (UID).

c. Mimecast has established a password policy that prohibits the sharing of passwords and requires passwords to be changed on a regular basis and default passwords to be altered. All passwords must fulfil defined minimum complexity requirements and are stored in encrypted form.

d. Access to systems containing Customer Data is only possible through a secure VPN tunnel and require a second factor of authentication.

e. Mimecast has a comprehensive process to deactivate users and their access when Personnel leaves the company or a function.

f. All access or attempted access to systems is logged.

5. Data Access

Objective:

To ensure Personnel entitled to use systems gain access only to the Customer Data that they are authorized to access.

Measures:

a. As a matter of course, Mimecast Personnel do *not* access Customer Data.

b. Mimecast restricts Personnel access to Customer Data on a "need-to-know" basis based on this justification.

c. Each such access is logged.

d. Personnel training covers access rights to and general guidelines on definition and use of Customer Data.

6. Data Transmission/Storage/Destruction

Objective:

To ensure Customer Data is not read, copied, altered, or deleted by unauthorized parties during transfer/storage.

Measures:

a. Customer access to the Mimecast CyberGraph Service are protected by Transport Layer Security (TLS) version 1.2 or above.

b. Upon Customer's request, applicable Customer Data will be deleted.

    i. It should be noted that with each deletion request, the applicable Customer Data is logically deleted in the first storage copy and then deleted across the other copies. This is done in order to prevent accidental deletions or possible intentional damage.

7. Confidentiality and Integrity

Objective:

To ensure Customer Data remains confidential throughout processing and remains intact, complete, and current during processing activities.

Measures:

a. Mimecast has a formal background check process and carries out background checks on all new Personnel.

b. Mimecast trains its engineering Personnel in application security practices and secure coding practices.

c. Mimecast has a central, secured repository of product source code, which is accessible only to authorized Personnel.

d. Mimecast has a formal application security program and employs a robust Secure Development Lifecycle (SDLC).

e. Security testing includes code review, penetration testing, and employing static code analysis tools on a periodic basis to identify flaws.

f. All changes to software on the Mimecast CyberGraph Service are via a controlled, approved release mechanism within a formal change control program.

8. Availability

Objective:

To ensure Customer Data is protected from accidental destruction or loss, and there is timely access, restoration, or availability to Customer Data in the event of a Mimecast CyberGraph Service incident.

Measures:

a. Where possible the Mimecast CyberGraph Service is housed in Amazon instances that are aligned to the same geographical regions as the Mimecast Service. The Mimecast CyberGraph Service is housed in Amazon's US East Region. All services utilize multi-availability zones to ensure availability.

b. Incident response plans are reviewed updated and tested.

9. Data Separation

Objective:

To ensure applicable Customer's Data is processed separately.

Measures:

a. Mimecast uses logical separation within its multi-tenant architecture to enforce data segregation between customers as applicable.

b. In each step of the processing, applicable Customer Data received from different Customers is assigned a unique identifier so data is logically separated.

10. Incident Management

Objective:

In the event of any security breach of Customer Data, the effect of the breach is minimized, and the Customer is promptly informed.

Measures:

a. Mimecast maintains an up-to-date incident response plan that includes responsibilities, how information security events are assessed and classified as incidents and response plans and procedures.

b. Mimecast regularly tests its incident response plans and lessons learned are used to improve the plan. In the event of a security breach, Mimecast will notify Customers without undue delay after becoming aware of the security breach

11. Audit

Objective:

To ensure Mimecast regularly tests, assesses, and evaluates the effectiveness of the technical and organizational measures outlined above.

Measures:

a. Mimecast conducts regular audits of its security practices.

b. Mimecast ensures that Personnel are aware of and comply with the technical and organizational measures set forth in this document.

c. Mimecast conducts at least semi-annual penetration tests of the Mimecast Service using external security experts.

d. Customers can request copies of these test results on an annual basis through their Customer Success contact.