mimecast

Signal and Spotlight Services TOMs

Last Updated August 2024

This document describes technical and organizational security measures and controls implemented to protect the data Customers entrust to us as part of the Signal and Spotlight Services. Mimecast acquired Nullable, Inc. d/b/a Aware in August 2024.

Within this document, the following definitions apply:

- "Customer" means any subscriber to the Signal and/or Spotlight Services.
- "Signal and/or Spotlight Services" means the Signal and/or Spotlight Services provided by Aware to our Customers.
- "Customer Data" means any information provided or submitted by the Customer that is processed by the Signal and/or Spotlight Services.
- "Personal Data" means any information relating to an identified or identifiable natural person.
- "Personnel" means Mimecast and/or Nullable, Inc. employees and authorized individual contractors/vendors.
- "Strong Encryption" means the use of industry standard encryption measures.

This document is a high-level overview of the Signal and/or Spotlight Services technical and organizational measures.

Mimecast may change these measures from time to time to adapt to the evolving security landscape and where required will notify customers of material changes.

1. **Organization of Information Security**

   Objective:

   To outline Mimecast's information security structure.

   Measures:

a. Mimecast employs full-time dedicated trained/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 Personnel have signed legally reviewed confidentiality agreements.
e. All 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:

a. Mimecast has deployed an ISMS (Information Security Management System) that serves as the foundation of our information security practices.
b. Mimecast ISMS has been and continues to be assessed by an independent, external auditor and currently receives attestations under SOC 2 Type 2 compliance.
c. Customers can request copies of these assessments on an annual basis through their Customer Experience contact.

3. Physical Access

Objective:

To protect the physical assets that contain Customer Data.

Measures:

a. The Signal and/or Spotlight Services operate from several industry certified third-party production data centers (each, a "Data Center") with a defined and protected physical perimeter, strong physical controls including access control mechanisms, controlled delivery and loading areas, surveillance, and security guards.
b. Each Data Center is audited for compliance to security controls.
c. Only authorized Personnel have access to the Data Center premises storing Customer Data and access is controlled through a security registration process requiring a government issued photo ID.

d. Power and telecommunications cabling carrying Customer Data or supporting information services at the production data centers are protected from interception, interference, and damage.
e. The Data Centers, and their equipment are physically protected against natural disasters, unauthorized entry, malicious attacks, and accidents.
f. Equipment at the Data Center is protected from power failures and other disruptions caused by failures in supporting utilities and is appropriately maintained.
g. The Signal and/or Spotlight Services are hosted with the Microsoft Azure Cloud environment in US East by default. Microsoft's description of their data center physical security controls can be found here: https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

4. **System Access**

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

Measures:
a. Access to Aware systems is granted only to 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 Aware systems with a unique identifier (UID).
c. Mimecast has established a password policy that prohibits the sharing of passwords and requires default passwords to be altered. All passwords must fulfil defined minimum complexity requirements and are stored in encrypted form.
d. Access to Data Centers 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 and monitored.

5. **Data Access**

Objective:
To ensure systems containing Customer Data are used only by approved, authenticated Personnel.

Measures:

a. As a matter of course, Personnel do not access Customer Data.
b. Mimecast restricts Personnel access to Customer Data on a "need-to-know" basis.
c. Each such access and its subsequent operations are logged and monitored.
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 Signal and/or Spotlight Services portals are protected by the most current version of Transport Layer Security (TLS).
b. Mimecast uses Strong Encryption in the transmission of Customer Data within our Data Centers.
c. Each Customer is assigned a unique Strong Encryption key and that key is used:
    i. To encrypt Customer Data and store it in an encrypted format at rest within the Aware Services.
    ii. To decrypt Customer Data when requested as part of the Signal and/or Spotlight Services.
    iii. Customers also can self-service remove and terminate the encryption key at any point.
d. Upon termination of the Signal and/or Spotlight Services, Customer Data processed through the Signal and/or Spotlight Services will be promptly deleted.
e. Customer has the capability to delete Customer Data processed for providing the Signal and/or Spotlight Services at any time. Customer may request that Mimecast delete this Customer Data through a professional services engagement.

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 (SDL).
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 within the Signal and/or Spotlight Services are via a controlled, approved release mechanism within a formal change control program.
g. All encryption and other cryptographic functionality used by Mimecast within the Signal and/or Spotlight Services uses industry standard encryption and cryptographic measures.

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 service incident.

Measures:
a. Mimecast maintains a robust Business Continuity/Disaster Recovery program including (i) well defined updated plans and (ii) regular testing and retrospectives.
b. Each Data Center can be failed over/back in the event of flooding, earthquake, fire or other physical destruction or power outage to protect Customer Data against accidental destruction and loss.
c. Each Data Center has multiple power supplies, generators on-site and with battery back-up to safeguard power availability to the data center.
d. Each Data Center has multiple access points to the Internet to safeguard connectivity.
e. Each Data Center is monitored 24x7x365 for power, network, environmental and technical issues.

9. Data Separation

Objective:
To ensure each Customer's Data is processed separately.

Measures:

a. Mimecast uses logical separation within its multi-tenant architecture to enforce data segregation between customers.
b. In each step of the processing, Customer Data received from different Customers is assigned a unique identifier, so data is always physically or 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 plans. 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 routine penetration tests of the Signal and/or Spotlight Services using external security experts.
d. Customers can request summaries of these test results on an annual basis through their Customer Experience contact.