Advanced BEC Protection Service TOMs

This document describes technical and organizational security measures and controls implemented by Mimecast to protect the data customers entrust to us as part of the Mimecast Advanced BEC Protection service. Within this document, the following definitions apply:

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

This document is a high-level overview of Mimecast's 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 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:

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

b. Mimecast and its Cloud Gateway ISMS has been and continues to be assessed by an independent, external auditor and currently receives attestations under various industry certifications. See here for more detail.
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 Mimecast Cloud Gateway Service operates 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 Mimecast security controls.
c. Only authorized Personnel have access to the data center premises housing 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 production data centers, and their equipment are physically protected against natural disasters, unauthorized entry, malicious attacks, and accidents.
f. Equipment at the production data center is protected from power failures and other disruptions caused by failures in supporting utilities and is appropriately maintained.

Mimecast Advanced BEC Protection provided through Cloud Integrated Services:
The Mimecast Cloud Integrated Services are hosted with the Amazon Cloud environment in the applicable hosting jurisdiction selected by the customer. 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 Data Centers containing Customer Data are 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, Mimecast 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:

Cloud Gateway Service:

a. Customer access to the Cloud Gateway Service 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 Cloud Gateway Service.
    II. To decrypt Customer Data when requested as part of the Cloud Gateway Service.
d. Upon termination of the Cloud Gateway Service, Customer Data processed through the Cloud Gateway Service will deleted in accordance with Mimecast's Data Retention Policies and Practices.
e. Other than Machine Learning Data and Threat Data, Customer has the capability to delete Customer Data processed for providing the Advanced BEC Protection Service at any time. Customer may request that Mimecast delete this Customer Data through a professional services engagement.

f. Mimecast equipment or disk media containing Customer Data are not physically removed from the Data Center unless securely erased prior to such removal or being transferred securely for destruction at a third-party site.

Cloud Integrated Service:

a. Customer access to the Mimecast Cloud Integrated Service portals is protected by the most current version of Transport Layer Security (TLS).
b. The Mimecast Cloud Integrated Service rely on Amazon Cloud controls for the destruction of media. An outline of these controls can be found at: https://aws.amazon.com/compliance/data-center/controls/

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 on the Mimecast 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 Mimecast 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:

Mimecast maintains a robust Business Continuity/Disaster Recovery program including (i) well defined updated plans and (ii) regular testing and retrospectives.

Advanced BEC Protection Service provided through Cloud Gateway Service:

a. Mimecast uses a high level of redundancy when storing Customer Data. Customer Data is stored in triplicate across 2 geographically separate data centers using 2 separate cross connections.
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.
f. Mimecast receives an annual independent ISO 22301 assessment of its Business Continuity practices applicable to the Data Centers.
g. Customers can request copies of this assessment on an annual basis through their Customer Experience contact.

Advanced BEC Protection Service provided through Cloud Integrated Service:
Mimecast utilizes Availability Zones in within AWS to ensure a high and redundant level of availability for the Cloud Integrated Service.

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 at least semi-annual penetration tests of the Mimecast Service using external security experts.
d. Customers can request summaries of these test results on an annual basis through their Customer Experience contact.