mimecast®

Service Levels and Support Description
(for Managed Service Providers)

Effective 24 June 2021

mimecast

Service Levels and Support Description

(for Managed Service Providers)

Effective 24 June 2021

This Service Levels and Support Description applies where Customer has subscribed to the Services through a Partner managed service provider. All credits shown will apply to the relevant Service only.

A. SERVICE LEVELS

1. Email Delivery:

This Service Level measures the ability to deliver email messages to or from Mimecast's servers for each individual Customer and for the Messaging Security and Archiving Services only.

Service Availability Per Calendar Month	Credit of Fee for the Affected Month
<100% but >=99%	10%
<99% but >=98%	20%
<98% but >=97%	30%
<97% but >=96%	40%
<96%	50% and Partner may terminate the applicable Order and receive a pro-rata refund of any unused pre-paid fees.

2. DNS Resolution:

This Service Level measures the ability to resolve customer DNS requests against Mimecast's servers for the Web Security Services only.

Service Availability Per Calendar Month	Credit of Fee for the Affected Month
<100% but >=99%	10%
<99% but >=98%	20%
<98% but >=97%	30%
<97% but >=96%	40%
<96%	50% and Partner may terminate the applicable Order and receive a pro-rata refund of any unused pre-paid fees.

3. Spam Protection:

This Service Level measures the effectiveness of the protection against receipt of spam for those Messaging Security and Archiving Services that include such functionality. This Service Level is measured in terms of "False Positives" and "False Negatives" (defined below) for each individual Customer. This Service Level applies across all of Customer's email traffic and SMTP connection attempts (any attempt to connect to a Mimecast SMTP mail gateway to send email).

(a) Definitions: A "**False Positive**" is an e-mail incorrectly classified as spam by the Service. False Positives do not include emails which: (i) do not constitute legitimate business email; (ii) are sent from a compromised machine; (iii) are sent from a machine which is on a third party block list; or (iv) are sent from a mail server that does not fully comply with the SMTP delivery standards as defined in RFC 2821 & 2822. A "**False Negative**" is a spam email that the Service does not identify as spam.

(b) Service Levels:

False Positive Service Levels:

False Positive Capture Rate per Calendar Month	Credit of Fee for the Affected Month
>.0001% but <= .001%	10%
> .001% but <= .01%	20%
> .01% but <= .1%	30%
> .1%	40%

False Negative Service Levels:

Consecutive days with False Negative Rate Exceeding 2%	Credit of Fee for the Affected Month
2 – 3	10%
4 – 5	20%
6 – 9	30%
10+	40%

4. Anti-Virus Service:

This Service Level measures protection against infection of Customer's servers by a virus through the Services, for those Messaging Security and Archiving Services that include anti-virus functionality. Upon confirmation by Mimecast that Customer's systems have been infected by one or more harmful viruses in any calendar month through the Services, Customer will be entitled to a service credit from Mimecast equal to 50% of the fees paid to Mimecast by Partner for the applicable Customer for the affected calendar month.

5. Search Performance:

This Service Level relates to the search time experienced by Permitted Users accessing Mimecast's email archiving service. This Service Level measures the time elapsed only when using the administrative console, Mimecast Personal Portal, Mimecast for Outlook or any Mimecast Mobile application between the receipt of the Permitted User's search request by Mimecast's systems and when the return of the search results is initiated by Mimecast (the "**Query Time**"). This Service Level does not apply to searches conducted using the Case Review or Supervision components of the administration console. This Service Level applies only where Customer has performed at least 250 searches in the given month.

Query Time *	Credit of Fee for the Affected Month
> 7 seconds but <=20	10%
> 20 seconds but <= 25	15%
Greater than 25 seconds	25%

*Query Time calculated via the median search times for all searches conducted by Permitted Users in the given month across all of the applicable applications.

6. Credit Request Process and Service Credits

To receive a credit under this Section A, Partner must submit a credit request by opening a support case within 14 days of the end of the calendar month in which Mimecast fails to meet the standards provided in this Section A. Credits are based on Mimecast's performance against the standards provided in this Section A for each individual Customer, not on Mimecast's aggregated performance for all Customers contracting through Partner. A separate credit request must be made for each affected Customer, and will include details and dates of the relevant anomalies, as well as a reference to the specific Customer's Order. Subject to verification by Mimecast, Mimecast will apply the appropriate credit and notify Partner accordingly. The amount of a Service Level credit will be calculated based on (i) the amount of fees paid to Mimecast by Partner for the applicable Customer for the affected month, and (ii) the percentages specified in this Section A. In any event, Mimecast's maximum

cumulative liability for any individual Customer under this Agreement in any calendar month shall be no more than 100% of the fees paid by Partner for the Services provided to that specific Customer for the applicable month.

7. Service Level Conditions

Service Levels will not apply to the following circumstances:

- During any trial periods, periods of planned maintenance, periods of non-availability due to a force majeure event, or periods of suspension of Service by Mimecast in accordance with this Agreement.
- Customer is not using the Services in accordance with the Documentation (including the best practice implementation policies therein) as well as reasonable usage allowances. The reasonable usage limit for Services which include archiving, journaling or SMS messaging is three times the typical average user (as per internal benchmarks). The reasonable usage limit for Web Security Services including DNS resolution is three times the typical average user (as per Internal benchmarks).
- To emails containing attachments that cannot be scanned (i.e., encrypted or password protected attachments).
- The implementation by a Customer or Partner of excessively complex full text content policies.
- To emails sent by a Customer to large external distribution lists, which may be subject to serialized delivery.
- A denial of service attack from a third party or Customer causes a denial of service attack to occur (or any similar event).
- Customer, Partner, or third party inability to access the primary or backup MX hosts servers due to a failing in the Internet.
- Viruses introduced to Customer's systems by Customer or Partner.
- Problems caused by mail servers that are not RFC-822 compliant.
- Where Customer's email system appears to be operating as an "open relay." "Open relay" means an email server configured to receive mail from an unknown or unauthorized third party and forward mail to recipients who are not users of that system.

Please note that Mimecast reserves the right to contact Partner regarding any Customer which is using the Services in excess of the reasonable usage allowance to renegotiate contract terms.

B. TECHNICAL SUPPORT

Mimecast will provide the following technical support ("**Technical Support**") in connection with the Services. Mimecast will respond to each Technical Support request from Partner within the time frames set forth below and will work diligently to resolve such request as soon as reasonably possible. Mimecast will log all support requests, provide Partner with an incident number and use all reasonable endeavours to provide a resolution. Mimecast may elect to provide a temporary solution until a resolution to the initial problem can be found.

1. CONTACTS

Partner will nominate specific people as support contacts ("**Designated Contacts**"), whose details will be registered with Mimecast based on their credentials and access within the Administrative Console. The Designated Contacts may be amended by an existing Designated Contact. Partner is required to ensure that the Designated Contacts are and continue to be fully trained on all the licensed Services using web-based training provided by Mimecast. Designated Contacts will perform the following:

- Carry out initial analysis and attempt to replicate the problem in an effort to resolve simple end user-type errors. They will co-ordinate the gathering of relevant information from the end-users, computer room operators, system managers in order to diagnose reported problems.
- Distinguish between normal and abnormal operation of the Services; accurately describe symptoms of repeatable problems.
- Notify Mimecast of problem situations using agreed procedures if the problem is a Level 3 support case that cannot be resolved using established troubleshooting methodologies.

Mimecast will provide and maintain applicable contact information to enable Partner to contact the technical support team for the Applicable Region.

2. LEVELS OF SUPPORT

Partner will provide support to Customer for Level 1 and Level 2 support cases, and Mimecast will provide support to Partner for Level 3 support cases. The support case levels are defined as follows:

Type	Description
Level 1	A Level 1 case is a matter which can be solved via the information available on Mimecast's public knowledgebase, Mimecaster Central.
Level 2	A Level 2 case is one which requires additional expertise obtained via the Mimecast training and certification programs. Queries of this nature can be addressed via the information available in our knowledgebase and the tools available in Mimecast's applications, such as the Mimecast Administration Console.
Level 3	A Level 3 case is one that does not fall into the two categories above and which cannot be addressed using the tools and information available in Mimecast's applications (such as the Administration Console) or public knowledgebase. Cases of this nature may require review by Mimecast's specialist support teams depending on the nature of the problem.

3. HOURS OF SUPPORT

Mimecast will respond to Priority 1 support requests made by Designated Contacts on a 24x7x365 days a year basis. All other support requests will be dealt with in accordance with the level of support purchased.

Type	Description
MSP SUPPPORT	Includes the online Support Portal, the Mimecast Customer Community, Knowledgebase and Administration Console access. Also includes 24 X 7 Telephone support for Priority 1 issues. Other issues will be addressed during normal business hours.

4. SUPPORT REQUEST PRIORITY

Mimecast will investigate and assess the support request and assign a priority number as detailed below:

Priority	Description
1	Total loss or significant impairment of the Services. Must be logged by telephone.
2	Impairment of a specified function (e.g. search functionality, access to the administrative interface, etc.

5. RESPONSE TIMES

Support Option	Priority	Response Time
MSP Support	1	2 hours
MSP Support	2	12 working hours

6. EXCLUSIONS

Mimecast shall be under no obligation to provide technical support due to improper installation or operation of the Services or use of the Services not in accordance with the Documentation or the instructions of Mimecast's support team. In addition, Mimecast shall not be responsible for any performance delays or failure of the Services if the failures or delays are caused by (a) equipment, software, systems, services or data not provided by Mimecast, or (b) acts or omissions of Partner or Customer (including Permitted Users) that violate the terms of this Agreement.

7. SERVICE UPGRADES

Mimecast may from time to time upgrade and/or enhance the Services, which may require the cessation or interruption of the Services. Mimecast shall use reasonable endeavours to avoid doing so during the hours of 8:00am to 8:00pm on business days in the Applicable Region. Where Mimecast is required to undertake emergency maintenance which is necessary to safeguard the Services and/or any systems on which it operates then it may do so at any time but nonetheless shall endeavour to provide as much advance warning as it reasonably can to Partner.