

Services Levels and Support Description

1. Definitions

“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.

“False Negative” is a spam email that the Service does not identify as spam.

2. SERVICE LEVELS

Mimecast will maintain the following Service Levels in connection with the Services.

1.1 Email Delivery

This Service Level measures the ability to deliver email messages to or from Mimecast’s servers.

Service Availability Per Calendar Month	Credit of Fee for the Affected Month
Less than 100% but more than 99%	10%
Less than 99% but more than 98%	20%
Less than 98% but more than 97%	30%
Less than 97% but more than 96%	40%
Less than 96%	50% and Customer may terminate the Agreement and receive a pro-rata refund of any unused pre-paid fees.

1.2 Spam Protection:

This Service Level measures the effectiveness of the protection against receipt of spam for those Services that include such functionality. This Service Level is measured in terms of “False Positives” and “False Negatives”. 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).

1.2.1 Service Levels:

False Positive Service Levels:

False Positive Capture Rate per Calendar Month	Credit of Fee for the Affected Month
Greater than .0001% but less than .001%	10%
Greater than .001% but less than .01%	20%
Greater than .01% but less than .1%	30%
Greater than .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%

1.3 Anti-Virus Service

This Service Level measures protection against infection of Customer’s servers by a virus through the

Services, for those Services that include anti-virus functionality. Upon confirmation by Mimecast that Customer's systems has 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 for the affected calendar month.

1.4 Search Performance

This Service Level relates to the search time where Permitted Users access Mimecast's email archiving service. This Service Level measures the time elapsed 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").

Query Time *	Credit of Fee for the Affected Month
More than 7 seconds but less than 20**	10%
More than 20 seconds but less than 25**	15%
More than 25 seconds but less than 30**	25%

* Service Level applies only where Customer has performed at least 250 searches in the given month.

** Query Time calculated via the median search times for Permitted Users searches in the given month, not including searches performed by Customer's internal IT administrator(s) through the Mimecast Administrative Console interface (an administrative tool provided to the IT administrator by Mimecast).

3. Credit Request Process and Service Credits

To receive a credit under this Section, the customer must submit a credit request to accounts@firstnet.co.za within 14 days of the end of the calendar month in which Mimecast fails to meet the standards provided. A credit request will include details and dates of the relevant anomalies. Subject to verification by FirstNet and Mimecast, the appropriate credit will be applied and the customer will be notified accordingly. In any event, the maximum accumulative liability to Customer under this Agreement in any calendar month shall be no more than 100% of the fees paid by Customer for the applicable month.

4. 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 best practice implementation policies and reasonable usage allowances. The reasonable usage limit for Services which include archiving and/or journaling is three times the typical average user as benchmarked across the entire Mimecast Service).
- To emails containing attachments that cannot be scanned (i.e., encrypted or password protected attachments).
- The implementation by Customer of excessively complex full text content policies.
- To emails sent by Customer to large external distribution lists, which may be subject to serialized delivery. Customer is required to utilize Mimecast's Bulk Mail Service for large external distribution lists.
- A denial of service attack from a third party or Customer causes a denial of service attack to occur (or any similar event).
- Customer 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.
- 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 any Customer which is using the Services in excess of the reasonable usage allowance to renegotiate contract terms.

5. CONTACTS

The customer will nominate specific people as technical contacts ("TC"), whose details will be registered with FirstNet. The customer is required to ensure that the TC is and continue to be fully informed on the relevant services being used, by using web-based training provided by Mimecast.

6. Logging a Service Request

There are several methods whereby a Client may log an SR. In order of preference there are:

6.1 Customer Zone <http://customerzone.firstnet.co.za>

The system will send an auto-reply containing the SR number. The TC should place a follow-up call to the FirstNet RR team if this auto-reply is not received within 30 minutes.

6.2 Email to support@firstnet.co.za

The system will send an auto reply containing the SR number. The TC should place a follow up call to the FirstNet RR team if this auto reply is not received within 30 minutes

6.3 Telephonically – 0861 989896

The SR will be logged and the TC will be given the SR number for future reference. This is the preferred method of logging a Sev1 Service Request

7. SUPPORT REQUEST PRIORITY

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

Severity Level	Impact
1	Total loss or significant impairment of the Services. Must be logged by telephone. More than 75% of users affected
2	Impairment of a specified function (e.g. search functionality, access to the administrative interface, etc.) – 50% to 75% users affected
3	Interferes with NORMAL completion of work – 25% to 50% users affected
4	Query or planned change required

7.1 RESPONSE TIMES

Severity Level	RESPONSE TIME
1	2 hours
2	6 working hours
3	8 hours
4	16 working hours

7.2 EXCLUSIONS

FirstNet and 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 FirstNet'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 Customer (including Permitted Users) that violate the terms of this Agreement.

8. 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. 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 Customer.