SCHEDULE K: SERVICE DEFINITION FOR MANAGED EMAIL SECURITY

1. Service Description for Managed Email Security

Exponential-e's Managed Email Security Service utilises a software agent that blocks email-based threats by providing:

- Anti-Virus
- Spam Protection
- Detection and block of malicious URLs in attachments
- Content Examination and Data Leak Prevention (DLP)

The Service is a licence-based Service provided using a cloud-based gateway that deploys best-practice configurations and applies threat intelligence from multiple sources in order to provide protection in both inbound and outbound emails.

Exponential-e does not warrant or otherwise assert that the Managed Email Security Service will always locate or block access to or transmission of all desired addresses, emails, malware, applications and/or files.

Licensing

Exponential-e will provide the Customer with the number of licences set out on the Order Form. The Customer is referred to the relevant licensor for details of the licences provided, based on the following bundles:

- S1: Email Security
- S2: Email Security & Remediation
- M2: Email Security & Continuity
- M2A: Email Security, Continuity & Archiving
- M3RA: Email Security, Remediation, Continuity & Archiving

Reporting

The Customer is granted access to the Reporting module, via the Administration Console, for a view of what is happening in their email environment, including detailed statistics on data volumes being transmitted, and number of messages being sent or rejected.

Implementation

Deployment responsibilities will depend on the Implementation Package specified on the Order Form.

Implementation Package	Customer Responsibilities	Exponential-e Responsibilities
Self-Implementation	- Make all necessary internal infrastructure changes including (but not limited to); DNS records and environmental mail routing configurations. - Full-service configuration and deployment of software agent. - Complete all the required implementation and onboarding tasks. - Knowledge/skills with email infrastructure (Exchange, Office365, GSuite, etc) as well as Directory Services. - roll out of endpoint agents.	- Provide a copy of onboarding kit – Guides & learning materials to the Customer. - Provide the Customer with access to online knowledge base. - Email/Phone support throughout the implementation process during Normal Working Hours.

Implementation Package	Customer Responsibilities	Exponential-e Responsibilities
Managed Implementation	- Provide Exponential-e with credentials and access to internal infrastructure. - Identify individuals for regular touch-points with Exponential-e technical team. - Roll out of endpoint agents.	- Provision of a named Senior Solutions Consultant available during Normal Business Hours to assist. - Kick-off call to verify Customer requirements and transfer knowledge. - Configuration of Domain Services Integration, DNS & Mail Routing (Inbound/Outbound), & Authentication. - Configure default/recommended policies for purchased elements (minor modifications to fit customer use-case/requirements). - Document implementation activities. - Customer knowledge transfer (overview of platform and basic policy configuration). - Regular touchpoints with Customer's technical team.
Advanced Implementation	- Same as Managed Implementation (Standard)	- Same as Managed Implementation plus: - Workshop customer policy requirements & configuration. - Configuration for complex environments (multiple domains and back-end mail systems)

Exclusions

The following elements are not included within any of the Implementation Packages:

- Migration of mail data from a legacy archiving platform/service
- End-User Application Deployment (Outlook Plug-in Installation & Setup)

Management

Exponential-e is responsible for:

- Operational support including creating, amending and updating email and archive policies;
- End user support including authentication, search, block and allow emails and domains;
- Recommended vendor upgrades to mitigate new risks and threats;
- Engage vendor support to assist with issues and upgrades;
- Minor upgrades including all updates to the software agents that can be performed on the existing system. A minor upgrade is defined as an upgrade that does not require the existing supported OS environment or the applications running on it to be rebuilt to perform the upgrades.

The Customer is responsible for implementing and maintaining reasonable and appropriate controls to ensure that user accounts are used only by the permitted users to whom they are assigned.

2. Target Service Commencement Date* and Service Commencement Date

Email Security: 7 Working Days

** From Order Acceptance*

The Service Commencement Date for the purposes of invoicing the Annual Charges is the date that Exponential-e places the order for the licences with the licensor.

3. Service Level Agreement

The Customer must submit a service credit request to clientrelations@exponential-e.com within fourteen (14) days of the end of the calendar month in which Exponential-e fails to meet the Service Levels provided in this Section. Any service credit claims not raised by the Customer within this period are irrevocably waived. This shall take precedence over the timeframe set out in Section 6.3 of the main body of this Service Document. A credit request must include all relevant Service and fault details and dates. In any event, Exponential-e's maximum cumulative liability to Customer under all the Service Levels in this Section in any calendar month shall be no more than one hundred percent (100%) of the Monthly Charge paid by Customer for the applicable month. Monthly Charge is the Annual Charge divided by 12.

Email Delivery: Archiving

This Service Level measures the ability to deliver email messages to or from Mimecast's servers for each individual Customer and for the Archiving element of the M2A and M3RA licences only.

Service Availability Per Calendar Month	Credit of Monthly Charge for the Affected Month
<100% but >=99%	10%
<99% but >=98%	20%
<98% but >=97%	30%
<97% but >=96%	40%
<96%	50%

Monthly Charge is the Annual Charge divided by 12.

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, measured in terms of "False Positives" and "False Negatives".

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.

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

Monthly Charge is the Annual Charge divided by 12.

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

Monthly Charge is the Annual Charge divided by 12.

Anti-Virus

This Service Level measures protection against infection of Customer's servers by a virus through the Service's, 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 Service, the Customer will be entitled to a service credit from Exponential-e equal to 50% of the Monthly Charges paid to Exponential-e for the affected calendar month. Monthly Charge is the Annual Charge divided by 12.

Exclusions

In addition to the Excused Reasons set out in the main body of this Service Document, Service Levels will not apply to the following circumstances:

- During any trial periods
- The 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 the Customer of excessively complex full text content policies.
- To emails sent by the Customer to large external distribution lists, which may be subject to serialized delivery.
- A denial of service attack from a third party or the Customer causes a denial of service attack to occur (or any similar event).
- The 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 the Customer.
- Problems caused by mail servers that are not RFC-822 compliant.
- Where the 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.

4. Definitions

"Administration Console"	The Administration Console is a Mimecast platform that allows administrators to configure and monitor their Mimecast Accounts.