

SCHEDULE K: SERVICE DEFINITION FOR MANAGED EMAIL SECURITY

1. Service Description for Managed Email Security

Vysiion's Managed Email Security Service utilises a software agent that deploys best-practice configurations and applies threat intelligence from multiple sources to provide protection in both inbound and outbound emails.

Vysiion 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.

Vysiion's Managed Email Security Service comprises:

- a) Licensing;
- b) Implementation; and
- c) Management.

A) Licensing

The licences are subject to the license terms of the third-party licensor which is accessible via www.mimecast.com/Contracts (hereinafter "Licensor Terms"). The Customer shall comply with the Licensor Terms. The Licensor Terms are also available upon request by email to sales@vysiion.co.uk.

Vysiion will provide the Customer with the number of licences, licence type(s) and add-ons set out on the Order Form.

The Service includes the below licence bundles options:

- Critical Protection
- Advanced Protection
- Premium Protection

Each bundle represents a defined set of email-security capabilities, with features varying per bundle. All bundles include:

- **Messaging Security:** Scanning all incoming, outbound and internal email communications for malicious or harmful content.
- **Internal Email Protect:** This includes but not limited to scanning of attachments and URLs, content inspections for violations of data leak prevention policies and providing comprehensive protection from threats originating from internal and outbound email.
- **Business Email Compromise:** Identifying anomalies and suspicious emails using threat-specific language in messages or subject line.

Furthermore, the Advanced Protection and Premium Protection bundles offer the following:

- **Browser Isolation:** Allows users to click on any URL embedded in an email or to surf any website whilst being protected from phishing attempts or malware infections.
- **Continuity:** The ability to trigger an email continuity event and switch all email clients to send and receive an email directly through the Mimecast Platform. During a disaster, users will still have secure access to their email and calendar information.
- **Sync and Recover:** 'Synchronise users' mailbox folder structure, calendar content, and contacts from email client to Mimecast Cloud. Data will be protected, allowing for the recovery of full point-in-time snapshots of users' environments.

In addition to the above capabilities, the Premium Protection bundle enables Customers to do more through the functionalities outlined below:

- **Collaboration:** AI-powered file and URL scanning in Microsoft Teams, Sharepoint, and OneDrive.
- **Large File Send:** Enables employees to send large files directly from Outlook overcoming attachment size limitation.
- **Secure Messaging:** Emails and attachments are uploaded to the cloud. The receiver will receive a notification to collect the email from the secure messaging service portal.

All bundles can be complemented by the following add-ons:

- **Engage:** A security awareness solution which offers a range of functionalities to manage human risk and enhance security behaviour such as providing centralised view of human risk which would lead to identifying and managing risks effectively.
- **Archive:** Archiving services for email retention policies.
- **DMARC Analyser:** to identify and reduce unauthorised use of customer domains.

As part of the licence, the Customer is granted access to a 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.

Customer obligations

To the extent Customer Personal Data is retrieved from or provided by Third Party Services, Vysiion

- (i) will not be responsible for nor makes any representations, warranties or commitments regarding any Third-Party Services; and
- (ii) shall not be liable for the condition of such Customer Personal Data, including, but not limited to, any Customer Personal Data that is incorrect, incomplete, corrupt or missing.

It is the Customer's sole responsibility to ensure it has

- (a) valid licenses for, and access to, all applicable Third-Party Services necessary to access and derive benefit from the Service; and
- (b) lawfully obtained necessary consents to use any personal data included in the Customer Personal Data.

The Customer hereby irrevocably waives any claim against Vysiion and its affiliates with respect to such Third-Party Services and Customer Personal Data.

The Customer acknowledges and agrees that any processing of Customer Personal Data carried out as part of using the Services will incorporate Mimecast data processing flow down terms (hereinafter "Third-Party DPA") to the extent the provisions of the Third-Party DPA are not already covered in Vysiion's Data Processing Addendum.

For the purpose of this Service Definition, "Third Party Services" means third party licenses (excluding the Mimecast licences for this Service), products, applications, application programming interfaces, web hooks, services, software, systems, directories, websites, databases and information which Customer may connect to or enable in conjunction with the Service.

B) Implementation

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

Implementation Package	Customer Responsibilities	Vysiion 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.	- Provide a copy of onboarding kit – Guides and learning materials to the Customer. - Provide the Customer with access to online knowledge base. - Email/Phone support throughout the implementation process during Normal Business Hours.

Implementation Package	Customer Responsibilities	Vysiion Responsibilities
	- Knowledge/skills with email infrastructure (Exchange, Office365, GSuite, etc) as well as Directory Services. - roll out of endpoint agents.	
Managed Implementation	- Provide Vysiion with credentials and access to internal infrastructure. - Identify individuals for regular touch-points with Vysiion's 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)

C) Management

Vysiion 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*

Email Security implementation requires 7 Working Days

* From Order Acceptance

3. Service Level Agreement

Email Delivery

This Service Level applies to the three bundles outlined above together with archive licences only.

Availability means the ability to deliver email messages to or from Mimecast's servers for each individual Customer.

Service	Target Availability
Email Delivery	100%

Service Availability Per Calendar Month	Service Credit*
<100% but >=99%	10%
<99% but >=98%	20%
<98% but >=97%	30%
<97% but >=96%	40%
<96%	50%

*The Service Credit is applied as a percentage of the Monthly Charge for the Managed Email Security Service only. Monthly Charge is the Annual Charge divided by 12.

Spam Protection

This Service Level applies to the three bundles outlined above together with archive licences only.

The effectiveness of the service is 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	Service Credit*
>.0001% but <= .001%	10%
> .001% but <= .01%	20%
> .01% but <= .1%	30%
> .1%	40%

*The Service Credit is applied as a percentage of the Monthly Charge for the Managed Email Security Service only. Monthly Charge is the Annual Charge divided by 12

Consecutive days with False Negative Rate Exceeding 2%	Service Credit*
2 -3	10%
4 -5	20%
6 – 9	30%
10+	40%

*The Service Credit is applied as a percentage of the Monthly Charge for the Managed Email Security Service only. Monthly Charge is the Annual Charge divided by 12.

The Customer must submit a service credit request to customerservices@vysiion.co.uk within fourteen (14) days of the end of the calendar month in which Vysiion 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, Vysiion'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.

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 trial periods, planned maintenance, force majeure events, or service suspensions by Mimecast.
- When the Customer uses the Services contrary to Documentation (including the best practice implementation policies therein) or reasonable usage allowances, defined as three times the typical average user (as Mimecast determines at its sole discretion) for archiving, journaling, SMS messaging, and DNS resolution.
- Emails with unscannable attachments (e.g., encrypted or password-protected).
- Implementation of excessively complex full text content policies by Customer.
- Emails sent to large external distribution lists, which may require serialized delivery.
- Denial of service attacks originating from third parties or the Customer.
- Inability to access MX host servers due to Internet failures.
- Viruses introduced by the Customer's systems.
- Issues caused by non-RFC-822 compliant mail servers.
- Customer's email system operating as an Open Relay, allowing unauthorized mail forwarding.

4. Miscellaneous

- 4.1.1 The Customer shall defend, indemnify and hold harmless Vysiion, its officers, Affiliates directors employees and consultants against any claim that use of the Services by the Customer breaches any provision of this Service Definition, the Licensor Terms and the Third-Party DPA.
- 4.1.2 Vysiion shall be entitled to increase the Charges with effect from each anniversary of the Service Commencement Date at a rate of up to eight percent (8%), such increase to apply at the start of each Renewal Period (as defined below).
- 4.1.3 The Customer is responsible for monitoring any changes made to the Licensor Terms and the Third-Party DPA.
- 4.1.4 Unless the Customer provides notice of termination at least three (3) months prior to the end of the Initial Term or any Renewal Term, the Managed Email Security Service shall automatically renew for successive terms of thirty days each (each a "Renewal Period").

5. **Definitions**

“Administration Console”	The Administration Console is a Mimecast platform that allows administrators to configure and monitor their Mimecast Accounts.
“Open Relay”	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.