CYBER SECURITY – SERVICE DESCRIPTION

Email Threat Protection ("ETP")

This Service Description ("**ETP Service Description**") contains the terms governing the provision of Email Threat Protection Services by Interactive Pty Ltd (ABN: 17 088 952 023) of 461 Williamstown Road, Port Melbourne VIC 3207 ("**Interactive**") to the customer named in the CMS SOW that applies to this ETP Service Description ("**Customer**").

This ETP Service Description forms part of the Agreement, also containing the Cyber Security Service Terms (found at www.interactive.com.au/terms-and-conditions) and the Master Services Agreement.

1 Email Threat Protection ("ETP")

1.1 The ETP Service protects from known and unknown (zero-day) threats that are delivered through email to Permitted Users and business mailboxes. Interactive will provide the level of protection identified in the CMS SOW (being Essential, Enhanced or Enterprise) in accordance with Table 1, with each service element further defined in item 2.

Table 1. Service Elements for each Level of Protection

	Essential	Enhanced	Enterprise
Anti-Spam Filtering	x	x	x
Secure Email Gateway			
Data Leak Prevention	x	x	x
Signature & Disclaimer Management	x	x	x
End User Productivity Applications	x	x	x
Intelligent Email Routing	x	x	x
Threat Intelligence	x	x	x
Large File Send	*o*	*o*	*o*
Secure Messaging	*o*	*o*	*o*
Targeted Threat Protection			
URL Protect	x	x	x
Attachment Protect	x	x	x
Impersonation Protect	x	x	x
Internal Email Protect	-	x	x
Email Continuity and Recovery			
Sync & Recover	-	-	x
Email Continuity	-	-	x

Archiving & Email Retention			
30 Day Retention	x	x	-
1 Year Retention			x
99 Year Retention	-	-	*o*
Security Awareness			
	o	*o*	*o*

In Table 1:

(a) x = included in the level of protection.

(b) o = only included in the level of protection if stated in the CMS SOW.

1.2 Interactive will on-board the ETP Service as follows:

(a) organise a pre-engagement meeting with the Customer to define project timelines;

(b) define a configuration policy using best practice and Customer requirements, which will be used in the implementation of the service elements set out in item 2;

(c) the Customer must inform Interactive of all MX record entries and internal mail configurations to point the Customer's email service to the Cloud Platform; and

(d) Interactive will cutover the Customer's email service to the Cloud Platform.

1.3 The Service Start Date for the ETP Service is the earlier of:

(a) the date the Customer's legacy email platform is disconnected; or

(b) 7 days after the date of successful cutover to the Cloud Platform.

2 Service Elements

The Service Elements listed in this clause will apply if included in the level of protection stated in Table 1.

2.1 Anti-Spam filtering

As part of the secure email gateway service element, the ETP Service will protect against spam delivery. The Customer agrees and acknowledges there may be false positive or negative results (as set out in the Service Levels), which may result in emails being inadvertently blocked or held.

2.2 Secure Email Gateway

(a) Data Leak Prevention

Interactive will configure the data leak prevention policy based on pre-defined criteria specified during on-boarding, to enable the Customer to receive and action automated alerts based on the defined policy.

(b) Signature and Disclaimer Management

Enables consistent email signatures and disclaimers based on Active Directory credentials and defined policy.

(c) End User Productivity Applications

Enables self-service features and applications based on pre-defined policies for quarantined e-mails and e-mail archiving.

(d) Intelligent Email routing

(i) Interactive will assist with email system integration or separation associated with a merger, acquisition or divestiture.

(ii) No later than one week before the start of the on-boarding project, the Customer will implement all required DNS changes, or provide Interactive with access to perform DNS changes.

(e) Large file send

Enables large file send up to 2GB.

(f) Secure Messaging

Enables secure messaging with pre-defined controls and policies set out during on-boarding.

2.3 Targeted Threat Protection

(a) URL Protect

The Cloud Platform will scan email for URL's and perform on-click site inspection and identification and prevention for malware, phishing and URL rewrite.

(b) Attachment Protect

Blocks or quarantines suspicious attachments and performs static and dynamic analysis of suspicious attachments.

(c) Impersonation Protect

(i) Interactive will use the Cloud Platform to protect against impersonation attacks (for example: social engineering, CEO fraud, whaling, business email compromise, and phishing attacks).

(ii) The Customer will provide Interactive with a list of VIPs to protect through impersonation protection, maintain the list and provide an updated list to Interactive as the VIPs change.

(d) Internal Email Protect

Interactive will utilise the Cloud Platform to prevent the deliberate or unintentional spread of attacks internally and outbound, including automatic or manual remediation of files or emails post-delivery.

2.4 Email Continuity and Recovery

(a) Sync and Recover

Interactive will perform continuous synchronization of email that ensures an email or entire inbox can be recovered following an attack, breach or user error.

(b) Email Continuity

Allows the Customer to continue to send emails internally and externally during any planned or unplanned email service downtime in accordance with the Service Levels.

2.5 Archiving and Email Retention

(a) 30 Day Retention

Search and restoration of email over a thirty-day period in the event of accidental deletion or malicious attack.

(b) 1 Year Retention

Search and restoration of email over a one-year period in the event of accidental deletion or malicious attack. Data will be deleted at the end of the Individual Term. The Customer may request to migrate data before the end of the Individual Term.

(c) 99 Year Retention

Long term data retention with a multipurpose cloud archive for compliance, case review and restoration of email. Data will be stored for up to 99 years, deleted at the end of the Individual Term. The Customer may request to migrate data before the end of the Individual Term.

2.6 Security Awareness

(a) Interactive will provide access to the Cloud Platform training portal where the Customer can access available security awareness tools and reports.

(b) Interactive will provide up to 14 online training videos per year, scheduled up to 12 months in advance.

(c) Interactive will perform quarterly/half-yearly phishing campaigns.

(d) Interactive will report on the outcomes of the phishing campaigns.

(e) As part of the on-boarding of this Security Awareness option, Interactive will train up to 3 selected Customer employees in the use of the tools to enable them to train others in the use of the security awareness tools.

3 Support

3.1 Interactive will provide Level 1 and Level 2 support via telephone and will manage all Level 3 support with the Cloud Platform Provider.

4 Reporting

4.1 Interactive will provide a monthly report with email spam statistics, email phishing trends and recommended improvements to the Customer's email service.

5 Exclusions

5.1 Interactive is not required to:

(a) manage the Customer's email platform, including:

(i) Office 365;

(ii) Microsoft Exchange;

(iii) Gmail; and

(iv) Sendmail;

(b) action any alerts arising from data loss prevention events, except to notify the Customer that the event occurred; or

(c) notify the Customer that emails have been blocked or perform any actions in regard to those emails.

6 ETP Services Pricing

6.1 The Service Fees for the ETP Service are based on the quantity of users specified in the CMS SOW.

6.2 The Customer may request to add Users by making a Service Request and providing relevant details of the User. Interactive will add the Users and the Customer will be charged for the addition pro-rata from the date it is added.

7 Licensing

7.1 The Customer agrees to, and must comply with, the Cloud Platform Vendor Terms, with it being deemed that the Customer is also the Customer as defined in the Cloud Platform Vendor Terms. The Customer agrees and acknowledges that the Cloud Platform Vendor Terms may be updated or replaced from time to time without notice, and the Customer must comply with those terms as they are updated.

7.2 The Customer agrees and acknowledges that Interactive is not liable for any Failure of the Cloud Platform (including if the Cloud Platform is unavailable), or for any Failure to provide ETP Services, to the extent the Failure is caused or contributed to by the Cloud Platform or the Cloud Platform Vendor. Interactive's sole liability for such a Failure is to pass on any rebate or credit in accordance with item 8.2.

7.3 The following applies if the Cloud Platform is Mimecast:

(a) In this item 7.3, the following definitions apply:

(i) **Customer Data** means the data generated through Customer's use of the ETP Services, including the contents of the files and emails sent by or to Permitted Users.

(ii) **Personal Data** means the Customer Data generated through Customer's use of the ETP Services that relates to an identified or identifiable natural person.

(b) Cloud Platform Vendor acknowledges that the Cloud Platform Vendor has no right, title or interest in or to Customer Data. With respect to any Personal Data contained in Customer Data, as required in the GDPR, Interactive acts as **Data Processor** and the Cloud Platform Vendor acts as **Sub-processor**. The Cloud Platform Vendor will process any Personal Data contained in Customer Data in accordance with the terms set out in Appendix 1 of this ETP Service Description, which are hereby incorporated into the Agreement.

(c) The Cloud Platform Vendor will use and process the Personal Data solely in accordance with Interactive's Instructions (as that term is defined in the Data Processing Agreement set out in Appendix 1 of this Service Description) and any Instructions received directly from the Customer during the Individual Term. The Instructions are embodied in the agreement and applicable order between Interactive and the Cloud Platform Vendor, any Data Processing Agreement between the Cloud Platform Vendor and Interactive or the Cloud Platform Vendor and Customer, and as may be additionally agreed between the parties. Instructions may also be provided via the console for the ETP Services. Where permitted by applicable law, the Cloud Platform Vendor may process Customer Data to countries or jurisdictions outside of the country where it was collected, including to the United States. The Customer consents to such processing and transfer of Personal Data, including international transfers, and warrants that each Permitted User consents to such processing and transfer of Personal Data, including international transfers. If the Customer and Interactive are parties to an agreement that restricts the international transfer of Personal Data, the Customer's consent in this clause applies notwithstanding that restriction.

(d) The Customer and Interactive must enter into the Data Processing Agreement set out in Appendix 1 of this ETP Service Description.

(e) Notwithstanding any provision herein to the contrary, the Cloud Platform Vendor owns both: (i) the aggregated data derived from the ETP Services as aggregated with usage data from the Cloud Platform Vendor's other customers, including, without limitation, utilization statistics, reports, logs and information regarding spam, viruses or other malware processed by the ETP Services ("**Aggregated Data**"); and (ii) all data identified through the ETP Services as malicious, such as data which may perpetuate data breaches, malware infections, cyberattacks or other threat activity ("**Threat Data**"). Neither Aggregated Data nor Threat Data will include any Personal Data, nor shall the Customer or any individual be identifiable via the Aggregated Data nor Threat Data. The Customer agrees that the Cloud Platform Vendor may process Aggregated Data or Threat Data for its business purposes and share Aggregated Data or Threat Data with third-parties.

7.4 The following applies if the Cloud Platform is Microsoft Defender for Office365.

(a) The Customer must comply with Microsoft's terms applicable to Microsoft Defender for Office365 including those found at the following URLs (or successor URL):

(i) docs.microsoft.com/en-us/legal/microsoft-365/mde-terms-windows

(a) The Customer acknowledges the Microsoft terms may vary at any time without notice.

8 Service Levels

ETP SERVICES AND CLOUD PLATFORM SERVICE LEVELS

8.1 This Clause 8.1 applies if the Cloud Platform is Mimecast

(a) The Mimecast Service Levels apply to the ETP Services and the Cloud Platform.

(b) If a rebate or service credit is available under the Mimecast Service Levels, the Customer may request Interactive apply to the Cloud Platform Vendor for the rebate or credit. The Customer must comply with the Mimecast Service Levels and Cloud Platform Vendor Terms when making the request to Interactive, including in respect of any time frames. If a rebate or credit is available to a Customer in respect of the Mimecast Service Levels, Interactive is only required to pass on the rebate made available by the Cloud Platform Vendor.

8.2 This Clause 8.2 applies if the Cloud Platform is Microsoft Defender for Office365.

(a) The Microsoft Service Level Agreements ("**SLA"**) for Online Services Service Levels ("**Microsoft SLA**") apply to the ETP Services and the Cloud Platform.

(b) If a rebate or service credit is available under the Microsoft SLA, the Customer may request Interactive apply to the Cloud Platform Vendor for the rebate or credit. The Customer must comply with the Microsoft SLA and Cloud Platform Vendor Terms when making the request to Interactive, including in respect of any time frames. If a rebate or credit is available to a Customer in respect of the Microsoft SLA, Interactive is only required to pass on the rebate made available by the Cloud Platform Vendor.

SUPPORT SERVICE LEVELS

8.3 The following Response Time, Update Time and Resolution Target Service Levels apply to ETP Incidents. The target times for each Service Level are calculated from the time the Customer contacts Interactive in accordance with this item:

PRIORITY LEVEL	RESPONSE TIME	UPDATE TARGET	RESOLUTION TARGET
1 -Critical	30 min	Hourly	4 hours
2- High	1 hour	2 hours	8 hours
3- Medium	2 Business Hours	1 Business Day	3 Business Days
4- Low	3 Business Hours	2 Business Day	4 Business Days
5- Service Request	4 Business Hours	3 Business Days	5 Business Days

8.4 An ETP Incident may be Restored via temporary measures and permanent remediation is to be performed under problem management and is not part of Restoration.

8.5 Severity 1 and Severity 2 ETP Incidents must be logged by telephone only. Severity 3 and Severity 4 ETP Incidents may be logged by telephone or email.

8.6 Callers to the Service Desk must define the level of urgency of the ETP Incident in accordance with Table 2 and define the impact of the ETP Incident in accordance with Table 3. The Service Desk will determine the severity of any reported ETP Incident based upon the Customer's impact assessment having regard to the urgency and impact definitions.

8.7 Where there is doubt regarding impact to a significant number of users or a few users, the initial impact assessment will be conservative by classifying the ETP Incident at the next highest level. ETP Incident or problem severity level classification may be changed later with a valid reassessment.

8.8 Where the assessed severity does not reflect a caller's requirements, the call shall be escalated to the contract representative of Interactive, rather than assigning a higher severity.

8.9 Upon receiving advice of the severity and impact of the ETP Incident Interactive will allocate a severity level in accordance with Table 4.

8.10 Interactive will use commercially reasonable endeavours to provide the ETP Service in accordance with the Support Service Levels, but a Failure is not deemed a breach of the Agreement.

8.11 Interactive is not liable for any Failures caused or contributed to by:

(a) the Customer, its contractors or representatives;

(b) a Force Majeure event;

(c) This Clause 8.11(c) applies if the Cloud Platform is Mimecast.
(i) any circumstances set out in the Mimecast Service Levels where the Mimecast Service Levels will not apply;

(d) This Clause 8.11(d) applies if the Cloud Platform is Microsoft Defender for Office365.
(i) any circumstances set out in the Microsoft SLA where the Microsoft SLA will not apply; or

(e) any Third-Party Fault.

URGENCY DEFINITIONS

Table 2. URGENCY			
Critical	**High**	**Medium**	**Low**
Critical business function impacted.	Important business function is impacted.	Administration activities impacted.	Business function continues.

IMPACT DEFINITIONS

Table 3. IMPACT			
Critical	**High**	**Medium**	**Low**
All Customer users are affected.	All business unit or department users are affected.	All team users are affected.	Only an individual is affected.

SEVERITY DEFINITIONS

Table 4. SEVERITY					
		IMPACT			
		Critical	**High**	**Medium**	**Low**
URGENCY	**Critical**	SEV 1	SEV 2	SEV 2	SEV 3
	High	SEV 1	SEV 2	SEV 3	SEV 4
	Medium	n/a	SEV 3	SEV 4	SEV 4
	Low	n/a	SEV 4	SEV 4	SEV 4

9 Definitions

9.1 The following definitions apply to this ETP Service Description:

Cloud Platform refers to the distributed platform used to provide the ETP Service.

Cloud Platform Vendor means the person or entity providing the Cloud Platform, which may be Interactive, or a third party engaged by Interactive.

Cloud Platform Vendor Terms means either of the following:

(a) For Mimecast, the general terms and service level documents found at the following URL, or such other URL as may be used from time to time: www.mimecast.com/contracts

(b) For Microsoft Defender for Office365, the general terms and service level documents found at the following URL, or such other URL as may be used from time to time: learn.microsoft.com/en-us/legal/microsoft-365/mde-terms-windows

ETP Incident means an unplanned interruption to the standard operation of the ETP Service that disrupts the quality of the ETP Service to the extent the interruption is classified as part of Level 1 or Level 2.

ETP Services means the email threat protection services set out in this ETP Service Description.

Failure means where Interactive fails to achieve a Support Service Level in any given month other than where it is attributed to any excused event referred to in item 8.11.

Microsoft Service Level Agreements (SLA) for Online Services means the service levels as described at www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services .

Mimecast Service Levels means the service levels as described at assets.mimecast.com/api/public/content/fcc528d8fdc54f92add565e220215f80?v=bcf49104&_ga=2.186942696.178017869.1658762326-1607572779.1643125081

Permitted User means each User of the ETP Services, up to the number of Users specified in the CMS SOW.

Restoration/Restored, in relation to an ETP Incident, means the return to correct operability, which may be achieved by temporary measures.

Service Levels means either of the following:

(a) For Mimecast, the Mimecast Service Levels and the Support Service Levels.

(b) For Microsoft Defender for Office365, the Microsoft Service Level Agreements for Online Service.

Support Service Level means the response time, update time and restoration target service levels set out in item 8.

Third-Party Fault means an ETP Incident affecting the ETP Service or the Cloud Platform where:

(c) the root cause is solely or partly the responsibility of a third party (such as the Cloud Platform Vendor);

(d) the ETP Incident is caused by an issue with the Cloud Platform and the Cloud Platform Vendor has not issued a patch or other fix to remedy the ETP Incident; or

(e) the ETP Incident is caused by a new or undocumented issue that is inherent in the ETP Services or Cloud Platform.

User means a single user of the Cloud Platform and **Users** means all of them.

Appendix 1 Data Processing Agreement (Customer to Interactive)

This data processing agreement is between Interactive Pty Ltd (the "**Data Processor**") and the Data Controller(s) (as defined below) and incorporates the terms and conditions set out in this Appendix and its Schedules (the "**DPA**").

Each Data Controller has appointed Data Processor to provide services to the Data Controller(s). As a result of its providing such services to the Data Controller(s), Data Processor will store and process certain personal information of the Data Controller(s), in each case as described in further detail in Schedule 1 (*Processing Details*).

The DPA is being put in place to ensure that Data Processor processes each Data Controller's personal data on the Data Controller's instructions and in compliance with applicable data privacy laws.

The DPA only applies to ETP Services and any Personal Data Processed in the performance of the ETP Services.

The Parties to this DPA hereby agree to be bound by the terms and conditions in the attached Schedules as applicable with effect from the date of the CMS SOW (the "**Effective Date**").

This DPA may be executed in any number of counterparts, each of which is an original and all of which evidence the same agreement between the parties.

Accepted and agreed to the last day the CMS SOW is signed by both parties by Interactive (the "**Data Processor**") and the Customer (the "**Data Controller**").

1.1 Definitions

Capitalised terms not defined in this DPA are given the meaning as defined in the agreement for the provision of ETP Services.

"**Affiliates**" means an entity that controls, is directly or indirectly controlled by, or is under common control of the relevant party;

"**Aggregated Data"** means the aggregated data derived from the Services as aggregated with usage data from Data Processor's other customers, including, without limitation, utilization statistics, reports, logs and information regarding spam, viruses or other malware processed by the Services;

"**Applicable Law**" means any laws or regulations relating to the protection of Personal Data applicable in the jurisdiction in which the Personal Data is hosted. Where GDPR applies this definition is extended to include the laws of the Data Controller's Member State which implements the Directive and the e-Privacy Directive, and the GDPR and the e-Privacy Regulation and any national laws implementing the same, in each case once they take effect;

"**Data Subject**" means the identified or identifiable living individuals who are the subject of the Personal Data;

"**Data Subject Access Request**" refers to a request from a Data Subject in accordance with Chapter 3 of GDPR;

"**Directive**" means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995;

"**e-Privacy Directive**" means Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002;

"**e-Privacy Regulation**" means the final text of the regulation that will replace the e-Privacy Directive;

"**Instructions**" are embodied in this DPA including this Data Processing Appendix, the applicable Service Order and as may be additionally agreed between the parties.

"**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person processed by Data Controller in connection with the performance of the Services;

"**Process**", "**Processed**" or "**Processing**" means any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"**Regulator**" means the data protection supervisory authority that has jurisdiction over Data Controller's Processing of Personal Data;

"**Standard Contractual Clauses**" means any clauses for the transfer of personal Data to processors in Third Countries approved by the EU Commission in Commission Decision 2010/87/EU, dated 5th February 2010 a signed copy of which is set out at:
https://www.mimecast.com/company/mimecast-trust-center/

"**Third-Party Subcontractors**" means the third-party subcontractors used for the ETP Service set out at:
https://www.mimecast.com/company/mimecast-trust-center/

"**Third Country(ies)**" means countries outside of the scope of the data protection laws of the European Economic Area, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time-to-time;

"Threat Data" means all data identified through the Services as malicious, such as data which may perpetuate data breaches, malware infections, cyberattacks or other threat activity.

1.2 **Instructions.** Data Processor shall only process Personal Data on behalf of Data Controller in accordance with and for the purposes set out in the Instructions.

1.3 Each party shall comply with the obligations applicable to that party under Applicable Law.

1.4 Data Processor shall inform Data Controller if, in Data Processor's opinion: (i) Data Processor cannot comply with Applicable Law; or (ii) Data Controller's Instructions violate Applicable Law.

1.5 Data Controller represents and warrants that:

(i) Data Controller' use of the Services and the Instructions provided do not contravene Applicable Law; and

(ii) it has complied and continues to comply with Applicable Law, in particular that it has obtained any necessary consents and/or given any necessary notices, and otherwise has the right to disclose the Personal Data to Data Processor and enable the processing set out in these Data Processing Clauses and as contemplated by the provision of the Services; and

(iii) it has assessed the requirements of the Applicable Law as they apply to the Data Controller with regards to Personal Data and finds that the security measures specified on the Trust Centre are adequate to meet those requirements. Furthermore, it will ensure compliance with those security measures to the extent such compliance is required of the Data Controller; and

(iv) where processing hereunder includes, or may include special categories of Personal Data, it has complied and continues to comply with requirements of Applicable Law to notify Data Subjects of the processing and, where relevant, obtain any consents or otherwise have the right to enable the Processing of the special categories of Personal Data.

1.6 **Technical and organisational security requirements**. Data Processor shall implement and maintain technical and organisational security measures before Processing Personal Data and shall continue to comply with such technical and organizational security measures as a minimum standard of security during the Service Term.

1.7 **Notification of Data Breach.** Data Processor shall notify Data Controller without undue delay of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Data Controller's Personal Data or any accidental or unauthorised access or any other event affecting the integrity, availability or confidentiality of Data Controller's Personal Data.

1.8 **Audit Rights.** Data Processor shall provide reasonable assistance in response to inquiries from Data Controller or its Regulator relating to Data Processor's Processing of Data Controller's Personal Data.

1.8.1 Data Processor shall, upon written request from Data Controller, provide Data Controller with information reasonably necessary to demonstrate compliance with the obligations set forth in this DPA. This information shall consist of permitting examination of the most recent reports, certificates and/or extracts prepared by an independent auditor pursuant to Data Processor's ISO27001 or similarly held industry certification.

1.8.2 In the event the information provided in accordance with Section 1.8.1 above is insufficient to reasonably demonstrate compliance, Data Processor shall permit Data Controller to inspect or audit the technical and organisational measures of the Data Processor for the purposes of monitoring compliance with Data Processor's obligations under this DPA. Any such inspection shall be:

(a) at Data Controller's expense;

(b) limited in scope to matters specific to Data Controller;

(c) agreed in advance between the parties in writing;

(d) conducted in a way which does not interfere with the Data Processor's day-to-day business;

(e) during local business hours as specified by Data Processor and, upon not less than twenty business days advance written notice unless, in the Data Controller's reasonable belief an identifiable, material non-conformance has arisen;

(f) subject to the confidentiality obligations in the Agreement or, where a third-party auditor conducts the audit, such third-party auditor must be a professional bound by a duty of confidentiality or subject to a suitable non-disclosure agreement; and

1.8.3 For the avoidance of doubt, the provisions of Section 1.8 shall also apply to the audit provisions of any Standard Contractual Clauses entered into in accordance this DPA.

1.9 **Assistance from Processor.** Data Processor will provide reasonable assistance to Data Controller in complying with any Data Subject Access Requests or requests received by Data Controller from Regulators that occur in accordance with Applicable Law.

1.9.1 If Data Processor receives a Data Subject Access Request, Data Processor will refer the Data Subject to Data Controller, unless otherwise required by Applicable Law. In the event Data Processor is legally required to respond to the Data Subject, Data Controller will fully co-operate with Data Processor as appropriate. Data Controller agrees that provision of technical tools to enable Data Controller to take the necessary action to comply with such request/s shall be sufficient to discharge Data Processor's obligations of assistance hereunder.

1.9.2 Data Controller will reimburse all reasonable costs incurred by Data Processor as a result of reasonable assistance provided by Data Processor under this Section 1.9.

1.10 Transfer. Data Controller acknowledges and agrees that Data Processor may, in the course of providing the Services, process, access and/or store (or permit any affiliate or Third-Party Subcontractor to Process, access and/or store) the Data Controller's Personal Data in one or more Third Countries, provided that such Processing takes place in accordance with the requirements of Applicable Law. In such case, the Data Processor shall, as applicable (i) comply with (or procure that any affiliate or Third-Party Subcontractor comply with) the data importer obligations in the Standard Contractual Clauses; or (ii) confirm that the recipient of the Personal Data has the necessary certification under the Privacy Shield Programme. The Data Controller hereby grants the Data Processor a mandate to enter into the Standard Contractual Clauses with Third-Party Subcontractor it appoints on behalf of Data Controller.

1.11 Changes in Applicable Law. The parties agree to negotiate in good faith modifications to this DPA if changes are required for Data Processor to continue to process the Data Controller's Personal Data in compliance with Applicable Law including (i) GDPR; (ii) the Standard Contractual Clauses: or (iii) if changes to the membership status of a country in the European Union or the European Economic Area require such modification.

1.12 Subcontractors. Data Controller hereby consents to Data Processor's use of Third-Party Subcontractors to perform Services. Data Processor agrees that it has a written agreement in place with all Third-Party subcontractors that contains obligations on the Third-Party Subcontractor that are no less onerous on the relevant Third-Party Subcontractor than the obligations on Data Processor under this DPA in respect of the specific Services provided by the Third-Party Subcontractor.

(a) If Data Processor appoints a new Third-Party Subcontractor or intends to make any changes concerning the addition or replacement of the Third-Party Subcontractors, it shall provide the Data Controller with reasonable advance written notice. For the purposes of this Section 1.12, notice may be provided electronically, including but not limited to posting on the administrative console for the Services or via a notice on:
the Trust Center https://www.mimecast.com/company/mimecast-trust-center/ and/or in a newsletter sent to Data Controller.

(b) If Data Controller objects to the appointment or replacement of Third-Party Subcontractor in writing within ten (10) days after Data Processor's advanced written notice of a new Third-Party Subcontractor, Data Processor may, at its option, suggest a commercially reasonable change to Data Controller's use of the Services so that the relevant Third-Party Subcontractor is not used in terms of the Service(s) procured.

(c) If Data Processor is unable to enact such change within a reasonable period of time, Data Controller may, upon no less than twenty (20) days' written notice from the date of notification by Data Processor, terminate those Services which cannot be provided without the use of the relevant Subcontractor. Termination of any Service Order under this Section 1.12 shall entitle the Data Controller to receive a pro-rata refund of any unused portion of the fees paid in advance. For the avoidance of doubt, termination under this Section 1.12 shall not entitle Data Processor to any refund of fees paid for the period up to the effective date of termination.

1.13 Confidentiality.

(a) These confidentiality provisions shall apply equally to this DPA and where applicable the Standard Contractual Clauses pursuant to Clause 6 herein.

(b) Each party (the "Recipient") undertakes to the other party (the "Discloser") to: (i) hold all Personal Data of the Discloser which it obtains in relation to this DPA, in strict confidence; and (ii) ensure that employees, agents, officers, consultants, sub-processors, subcontractors, and advisers authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

1.14 Return or deletion of personal data on termination. Upon termination of the DPA Data Processor shall:

(a) at Data Controller's request, delete all Personal Data Processed on behalf of the Data Controller, unless Applicable Law requires it to be retained; or

(b) assist Data Controller with return to the Data Controller of the Personal Data and any copies thereof which it is Processing or has Processed upon behalf of that Data Controller. The Data Controller acknowledges and agrees that the nature of the Services mean that the Data Controller may extract a copy of the Personal Data at any time during the term of the DPA, and providing the tools to allow Data Controller to do so shall be sufficient to show Data Processor has complied with this Section 1.14. If Data Controller requires the Data Processor to extract the Personal Data on its behalf, the Data Controller must provide the Data Processor with written instructions to that effect and engage Data Processor in a professional services project, which shall be subject to additional fees and

(c) in either case, cease Processing Personal Data on behalf of the Data Controller.

1.15 Aggregated Data and Threat Data. Notwithstanding any provision herein to the contrary, Mimecast owns both: (i) the aggregated data derived from the services as aggregated with usage data from Mimecast's other customers, including, without limitation, utilization statistics, reports, logs and information regarding spam, viruses or other malware processed by the Services ("Aggregated Data"); and (ii) all data identified through the services as malicious, such as data which may perpetuate data breaches, malware infections, cyberattacks or other threat activity ("Threat Data"). Neither Aggregated Data nor Threat Data will include any Personal Data. Partner agrees Mimecast may process Aggregated Data or Threat Data for its business purposes and share Aggregated Data or Threat Data with third-parties.

1.16 Limitations. The parties agree that Affiliates of the Data Controller and/or Third-Party Sub-processors Processing Personal Data **hereunder**, shall be bound by data protection obligations no less protective than the data protection obligations as specified in this DPA and any Standard Contractual Clauses entered into pursuant to this DPA. It is further agreed that the aggregate liability of the Data Processor, its Affiliates and third-party sub-processors under this DPA and any Standard Contractual Clauses entered into pursuant to this DPA, will be limited to an amount equal to the greater of: (i) USD $100,000 (or the equivalent in the currency of the applicable hosting jurisdiction at the time the claim arose) or (ii) two times the fees paid by Data Controller to Data Processor for the applicable Services during the twelve months preceding the event giving rise to the claim. Data Controller shall not be entitled to recover more than once in respect of the same claim.

1.17 Satisfaction of claim. In the event of any claim by the Data Controller against any Affiliate of the Data Processor under the Standard Contractual Clauses, the Data Controller shall accept payment from the Data Processor or entity with whom the Data Controller entered into the DPA, on behalf of the relevant Affiliate of the Data Controller in satisfaction of such claim.

Schedule 1 to the DPA
Processing Details

Duration of the processing

The Personal Data Processed by Data Controller will be processed for the duration of the DPA.

Data subjects

The Personal Data transferred concern the following categories of Data Subjects:

Employees, freelancers and contractors of the Data Controller;

Permitted Users and other participants from time-to-time to whom the Data Controller has granted the right to access the Services in accordance with the DPA;

End user customers of Customers and individuals with whom those end users customers communicate with by email and/or instant messaging;

Service providers of the Data Controller.

Other individuals to the extent identifiable in the content of emails or their attachments or in archiving content.

Categories of data

The personal data transferred concern the following categories of data:

Personal details, names, user names, passwords, email addresses of Permitted Users

Personal data derived from the Permitted Users use of the Services such as records and business intelligence information.

Personal data within email and messaging content which identifies or may reasonably be used to identify, Data Subjects.

Meta data including sent, to, from, date, time, subject, which may include personal data.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

No sensitive data or special categories of data are intended to be transferred, but may be contained in the content of or attachments to email.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Personal Data will be processed to the extent necessary to provide Services in accordance with this DPA and Data Controller's Instructions. The Sub-Processor processes Personal Data only on behalf of the Data Controller.

Technical support, Issue diagnosis and error correction to ensure the efficient and proper running of the systems and to identify, analyse and resolve technical issues both generally in the provision of the Services and specifically in answer to a customer query. This operation relates to all aspects of personal information processed but will be limited to metadata where possible by the nature of any request.

Virus, anti-spam and Malware checking in accordance with the Services provided. This operation relates to all aspects of Personal Data processed.

URL scanning for the purposes of the provision of targeted threat protection and similar service which may be provided under the Agreement. This operation relates to attachments and links in emails and will relate to any personal information within those attachments or links which could include all categories of personal information.

Schedule 2 to the DPA

Third-party subcontractors

Data Processor shall maintain a list of Third-Party Subcontractors at:
www.mimecast.com/company/mimecast-trust-center/