mimecast

Mimecast CyberGraph Services Terms and Conditions

These Mimecast CyberGraph Services Terms and Conditions (**"CyberGraph Terms**") govern Customer's use of the Mimecast CyberGraph Services (f/k/a MessageControl Codebreaker and Silencer), MessageControl Gatekeeper, Cybergraph Controlled Availability, Cybergraph for SEG, and Misaddressed Email Protect Services (the "**Additional Services**") and are an addendum to and form part of the Customer's services agreement with Mimecast which is in place between the parties or which will be executed concurrently with these CyberGraph Terms (the "**Agreement**"). If there is any conflict between these CyberGraph Terms and the Agreement (and, if applicable, the DPA, which is defined below), then these CyberGraph Terms shall take precedence, with regard to the Additional Services. Any capitalized terms not otherwise defined herein shall have the same meanings as those noted in the Agreement and the Additional Services are "Services" within the meaning of the term used in the Agreement.

BY CLICKING 'I ACCEPT' YOU (i) AGREE TO THE TERMS AND CONDITIONS OF THESE CYBERGRAPH TERMS WHICH WILL FORM A BINDING CONTRACT BETWEEN MIMECAST AND THE CORPORATION, BUSINESS OR ENTITY YOU REPRESENT (THE "CUSTOMER"); (ii) AGREE THAT THE ADDITIONAL SERVICES ARE SUBJECT TO BOTH THESE CYBERGRAPH TERMS AND THE AGREEMENT; AND (iii) YOU REPRESENT AND WARRANT THAT YOU HAVE THE POWER AND AUTHORITY TO BIND THE CUSTOMER TO THESE CYBERGRAPH TERMS.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THESE CYBERGRAPH TERMS, OR YOU DO NOT HAVE THE POWER AND AUTHORITY TO ACT ON BEHALF OF AND BIND THE CUSTOMER, DO NOT PROCEED TO ACCEPT THESE CYBERGRAPH TERMS OR CONTINUE WITH USE OF THE ADDITIONAL SERVICES.

1. Additional Services. The Additional Services are designed to help protect Customer from identity attacks by seeking to identify misaddressed emails and risks within email content and by intercepting embedded email trackers. Customer acknowledges that the certifications, attestations, and assessments listed on Mimecast's Trust Center may differ for the Additional Services.

2. Additional Customer Responsibilities and Restrictions. Customer is responsible for (i) obtaining and maintaining any Equipment needed to connect to, access, or otherwise use the software and software services ("**Equipment**") shall include equipment and ancillary services including, but not limited to, modems, hardware, services, software operating systems, networking, web services, and the like); (ii) ensuring the Services meet Customer's regulatory requirements including without limitation, requirements and obligations with regard to data privacy and employment laws; (iii) obtaining all necessary consents, permissions and authority from individuals or regulators in respect of all Customer Data, including, where applicable, Personal Data transferred, processed and/or analysed in the use of the Services, including the right for Mimecast to use such data in the preparation of reports and analyses. In addition to any indemnification obligations contained in the Agreement, Customer will hold harmless, defend and indemnify Mimecast in the event of any third-party claim or regulatory action arising out of (i) Customer's breach (or alleged breach) of this Section 2; (ii) Mimecast's compliance with any Instructions or directions provided by Customer.

3. Disclaimer for Additional Services. Without limiting Mimecast's express obligations hereunder Mimecast hereby informs Customer that the Additional Services do not qualify as legal or expert advice. Customer should consider whether the Additional Services are appropriate for Customer's needs, and where appropriate, seek legal or expert advice. Mimecast does not warrant that the Additional Services will operate uninterrupted or error free or meet Customer's requirements. Customer acknowledges and agrees that reports, graphs, analyses or similar information (collectively " Information") provided as part of the Additional Services, are based on Information known to Mimecast at the time and is provided for Customer's internal business purposes only. Mimecast will use all reasonable efforts to provide accurate and up-to-date Information but makes no warranties as to the accuracy or completeness of the Information provided.

4. Export Restrictions. Each party agrees to comply with all applicable laws and regulations with respect to the export and import of the Additional Services, including but not limited to the regulations of the United States Department of Commerce and the United States Export Administration Act. Customer hereby warrants that Customer will not procure or facilitate the use of the Additional Services in any region that is the subject or target of any U.S. or other national government financial and economic sanctions or trade embargoes or otherwise identified on a list of prohibited, sanctioned, debarred, or denied parties, including those imposed, administered or enforced from time to time by the U.S. government through the Office of Foreign Assets Control ("OFAC") of the U.S. Department of Treasury, the Bureau of Industry and Security ("BIS") of the U.S. Department of Commerce, or the U.S. Department of State, the United Nationals Security Council, the European Union, or Her Majesty's Treasury of the United Kingdom (collectively,

"Sanctions"), without having first obtained any required license or other government authorization or in any manner which would result in a violation of Sanctions by Customer or Mimecast.

5. Threat Data, Machine-Learning Data and Aggregated Usage Data.

5.1. Customer Data. The parties acknowledge and agree that Mimecast has no ownership rights to Customer Data. In accordance with the Agreement and any Data Processing Agreement ("**DPA**"), Customer hereby grants to Mimecast all necessary rights and licenses to Process Customer Data, including Customer Data within Machine-Learning Data (as defined below), and Personal Data within Threat Data (as defined below) for the purposes of: (i) providing the Services; (ii) improving threat detection, analysis, awareness, and prevention; and/or (iii) improving and developing the Services.

5.2. Threat Data. As part of the Services, Mimecast Processes certain data reasonably identified to be malicious, including, without limitation, data which may perpetuate data breaches, malware infections, cyberattacks or other threat activity (collectively, "**Threat Data**"). Mimecast processes Threat Data primarily through automated processes and may share limited Threat Data with Third Parties within the cybersecurity ecosystem for the purpose of improving threat detection, analysis and awareness. In certain instances, Threat Data may include Personal Data.

5.3. Machine-Learning Data. Primarily through automated processes designed to develop and improve our machine learning algorithms within Services, Mimecast processes Machine-Learning Data that may include Customer Data and other data that describes and/or gives information about Customer Data. "**Machine-Learning Data**" includes, but is not limited to metadata, files, URLs, derived features and other data. These machine-learning algorithms are hosted by Mimecast and/or Third-Party Subcontractors. The output of these machine learning algorithms is owned by Mimecast, does not contain Customer Data or Personal Data, and is anonymized and irreversible. Mimecast does not share Machine-Learning Data with Third Parties.

5.4. Aggregated Usage Data. Mimecast processes certain aggregated data derived from the Services, including usage data, such as utilization statistics, reports, logs and information regarding spam, viruses and/or other malware ("**Aggregated Usage Data**"). Mimecast owns all Aggregated Usage Data.

6. Data Processing Agreement. If the Customer has not executed a DPA with Mimecast, Customer acknowledges and agrees that Personal Data is not processed through the Services and/or the Additional Services.