



## Appendix 1

### Web Security Services

Defined terms used in this web security appendix shall have the meaning given to those terms in the Terms and Conditions. If there is any conflict between this appendix and the Terms and Conditions, then this appendix shall take precedence.

Sure has been appointed as a Managed Service Provider by Mimecast to sell the Mimecast web security service. This appendix governs the use of the web security service as described further in the Order Form (the “**Web Security Service**”). The Web Security Service shall fall within the definition of Services referenced in the Terms and Conditions and the following web security terms apply to the Customer in addition to those set out in the Terms and Conditions:

#### **1. Support and SLA:**

Sure will provide first line support in relation to the Web Security Service. The Support Description and Service Levels are set out in Appendix 2 (Support Description) and Appendix 3 (Service Levels) of the Terms and Conditions.

Support does not include adjustments to the default configurations for the Web Security Service or configuration of Customer systems such as MX records, DNS, or FTP traffic, all of which are Customer’s responsibility.

The Customer will receive an instruction guide from Sure to enable the Customer to set-up and configure the Web Security Service. The Web Security Service will not be turned on until it is fully configured by the Customer.

All configuration information and policy settings are fully visible via the account administration system and should any changes need to be made, these can be made directly by the Customer.

#### **2. Data Protection:**

2.1 The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the data controller and Sure is the data processor in respect of the Relevant Data.

2.2 Clause 3 below sets out the scope of the processing carried out by Sure in relation to the Relevant Data.

2.3 Both parties acknowledge that Mimecast is also a Data Processor in respect of the Customer Data and that processing by Mimecast is dealt with in a separate data processing agreement.

2.4 The parties warrants that they will duly observe all its obligations under the applicable Data Protection Laws. In this Clause 2, the terms “Process”, and “Processing” shall be understood in their meanings as assigned by the applicable Data Protection Laws.



- 2.5 Without limiting Clause 2.1 and notwithstanding Clause 2.3, the following Clauses sets out Sure's obligations in respect of the Relevant Data (the "**Relevant Data**"):
- 2.5.1 Sure will not Process Relevant Data held by it under these Terms and Conditions except in accordance with these Terms and Conditions or otherwise on the written instructions of the Customer;
  - 2.5.2 Details of the processing of the Relevant Data by Sure is set out in paragraph 3 below;
  - 2.5.3 Sure will acquire no rights or interest in the Relevant Data and will return such Relevant Data to the Customer on demand;
  - 2.5.4 Sure will ensure that its employees will maintain proper records of the Processing of any Relevant Data received from the Customer or from a third party on behalf of the Customer;
  - 2.5.5 Sure shall as soon as reasonably practicable notify the Customer if it receives a subject access request in respect of the Relevant Data processed under these Terms and Conditions or any complaint, notice or communication which relates directly or indirectly to the processing of the Relevant Data or to either party's compliance with the Data Protection Laws and it shall provide the Customer with full co-operation and assistance in relation to any such request, complaint, notice or communication;
  - 2.5.6 Sure will not transfer any Relevant Data received from or on behalf of the Customer under these Terms and Conditions outside the European Economic Area or an approved "White List" country (or successor EU approval) except with the prior written consent of the Customer and in accordance with any additional terms the Customer may impose on such transfer;
  - 2.5.7 Sure shall ensure that the Relevant Data is kept secure and shall use all reasonable security practices and systems applicable to the use of the Relevant Data to prevent, and take prompt and proper remedial action against, unauthorised access, copying, modification, storage, reproduction, display or distribution of the Relevant Data;
  - 2.5.8 Sure shall take reasonable precautions to preserve the integrity of any Relevant Data processed by it and to prevent any corruption or loss of such Relevant Data;
  - 2.5.9 Sure warrants and represents that it will having regard to the state of technological development and the cost of implementing any measures, take appropriate technical and organisational measures against the unauthorised or unlawful processing of Relevant Data and against the accidental loss or destruction of, or damage to, Relevant Data to ensure a level of security appropriate to:
    - 2.5.9.1 the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and
    - 2.5.9.2 the nature of the Relevant Data to be protected.



- 2.6 Sure shall keep detailed, accurate and up-to-date records relating to the processing by Sure of Relevant Data provided by the Customer to Sure and to the measures taken under Clause 2.5.9.
- 2.7 Sure shall make available to the Customer and its third-party representatives, all information necessary to demonstrate compliance with its obligations in this Clause 2 and allow and contribute to audits when requested by the Customer (provided such audits are limited to the Customer's Service and the Relevant Data). Reasonable notice must be given to Sure in respect of such audits and such audit rights may be exercised only on Business Days, once in any calendar year during the term of the contract. Such audits shall be carried out at the cost and expense of the Customer.
- 2.8 Audit access by any third-party representative of the Customer shall be subject to such representative agreeing confidentiality obligations equivalent to those in these Terms and Conditions in respect of the information obtained, provided that all information obtained may be disclosed to the Customer.
- 2.9 Sure does not permit processing of the Relevant Data by any subcontractors.
- 2.10 If Sure:
- 2.10.1 becomes aware of any unauthorised or unlawful processing of the Relevant Data or that any such Relevant Data is lost or destroyed or has become damaged, corrupted or unusable;
  - 2.10.2 becomes aware of any security breach affecting, or potentially affecting, the Relevant Data; or
  - 2.10.3 learns or suspects that any security feature has been revealed to or obtained by any unauthorised person,
- Sure shall promptly notify the Customer and fully co-operate with the Customer to remedy the issue as soon as reasonably practicable.

### **3. Details of Relevant Data:**

#### **3.1 Data Subject Types:**

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

Employees, freelancers and contractors of the Customer;

Permitted users and other participants from time to time to whom the Customer has granted the right to access the Web Security Service.

#### **3.2 Duration of Processing:**



The Relevant Data Processed by Sure will be processed for the duration of the term of the Contract between the Customer and Sure.

### **3.3 Nature of Processing:**

Relevant Data will be processed to the extent necessary to provide the Web Security Service and invoice the Customer in accordance with these Terms and Conditions and the Customer's Instructions.

Sure processes Relevant Data only on behalf of the Customer.

Technical support to ensure the efficient and proper running of the Web Security Service and to identify, analyse and resolve technical issues in answer to the Customer's queries.

### **3.4 Business Purposes:**

In order to provide the Web Security Service Sure has contracted to provide including billing of this Web Security Service and support of the Web Security Service.

### **3.5 Personal Data Categories:**

The Relevant Data concerns the following categories of data:

Personal details, names, details of roles, email addresses and contact phone of the Customer's employees and copies of signatures on contracts.

Names and contact details of individuals contacting sure in relation to the product and technical support.

### **3.6 Technical and Operations Controls used to minimise access to the above data:**

Sure is ISO27001 certified in relation to provision of the Web Security Service. All controls under this standard are in place.

## **4. Warranty Disclaimer for the Web Security Service:**

THE CUSTOMER ACKNOWLEDGES THAT THE WEB SECURITY SERVICE AND DOCUMENTATION PROVIDED BY SURE AND/OR MIMICAST HEREUNDER ARE PROVIDED "AS IS" AND "WITH ALL FAULTS". IN REGARDS TO THE WEB SECURITY SERVICE AND DOCUMENTATION, ALL WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF OPERABILITY, CONDITION, TITLE, NON-INFRINGEMENT, NON INTERFERENCE, OR QUIET ENJOYMENT, AS WELL AS ANY WARRANTIES OF MERCHANTABILITY, SYSTEM INTEGRATION, SATISFACTORY QUALITY, SUITABILITY, OR FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IT IS NOT REPRESENTED THAT THE WEB SECURITY SERVICE OR THE PROFESSIONAL SERVICES WILL BE FULLY ACCURATE, UNINTERRUPTED OR ERROR FREE OR MEET CUSTOMER'S REQUIREMENTS, OR THAT ANY ERRORS RELATING TO THE WEB SECURITY SERVICE OR DOCUMENTATION WILL BE CORRECTED. NEW THREATS ARE CONSTANTLY EVOLVING; SURE DOES NOT WARRANT THAT THE WEB SECURITY SERVICE WILL ALWAYS LOCATE OR BLOCK ACCESS TO OR TRANSMISSION OF ALL DESIRED ADDRESSES, EMAILS, MALWARE, APPLICATIONS AND/OR FILES, OR THAT ALL DATABASES WILL BE APPROPRIATELY CATEGORIZED OR THAT THE ALGORITHMS USED IN THE WEB SECURITY SERVICE WILLBE FULLY COMPLETE OR ACCURATE.