proofpoint

Data Security, Protection, Audit and Compliance Policy

The data security, protection, audit and compliance terms ("Policy") described herein are provided by Proofpoint to each Proofpoint customer ("Customer") subject to the terms and conditions of the General Terms and Conditions or other applicable license agreement ("Agreement") between each Customer and Proofpoint or between a Customer and an authorized Proofpoint partner. In the event of a conflict between the Agreement and this Data Security Policy the terms of the Agreement shall govern. Capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement. This Policy does not apply to Proofpoint's Cloudmark, TAP Isolation, or Wombat Security products.

1. Subcontractors. Proofpoint shall perform all Services and Professional Services using only its own employees or contractors. Except for Proofpoint technical support services, or for staff augmentation, if Proofpoint desires to engage any subcontractors to perform any portion of the Services or Professional Services hereunder, the following shall apply: (i) Proofpoint will provide written notice to Customer prior to engaging any such subcontractor (ii) Proofpoint will be responsible for the direction and coordination of the services of subcontractors; (iii) Proofpoint will be responsible and liable for all of the acts and omissions of all subcontractors and compliance with the applicable terms of this Policy; and, (iv) Customer shall have no obligation to pay or to be responsible for, in any way, the payment of monies to any subcontractor.

2. Background checks. Proofpoint agrees to process and complete its normal background check on all of its employees, consultants or independent contractors (for purposes of this Section, "Employees") that provide sustained Professional Services at a Customer facility under any SOW. As such, Proofpoint agrees to adhere to the prescreening requirements for the background check as specified herein. The background check shall be performed via state and local databases in which the Employee has resided during the ten (10) years preceding the commencement of his/her employment with Proofpoint. The criminal background check will include cross referencing the name of each Employee to be assigned to provide Services to Customer against the Office of Foreign Asset Control (OFAC) database. Proofpoint will also complete Social Security number checks for the Employee to ensure that his/her name and number match those recorded with the Social Security Administration, an employment verification check and an education verification check to ensure his/her last educational level is as stated.

3. Data Security. Proofpoint will maintain, during the Term, an information security program that provides for the security and protection of Customer Confidential Information, Customer Data and Personal Data. Proofpoint will align with the physical, technical, operational and administrative measures and protocols regarding data security as set forth in its then current SOC 2 Type II Report (or equivalent report) ("SOC 2"), received from its third party auditors. The following Proofpoint Products are not yet certified under the SOC 2 report: Email Fraud Defense, SaaS Defense and TAP for SaaS.

4. Security Audit. Provided that Customer has paid Subscription Fees on an annual basis in excess of $250,000, Customer is entitled, at its sole cost and expense and no more than once per calendar year, to monitor and/or audit Proofpoint's compliance with this Section during regular business hours at a time to be mutually agreed by the parties and upon not less than thirty (30) business days' advance written notice to Proofpoint. Further, such audit shall be limited to (i) a sixty (60) minute site inspection of Proofpoint's data center and an eight (8) hour visit at Proofpoint's headquarters, and (ii) a review of the Proofpoint Products with Proofpoint personnel. Proofpoint will, upon written request, provide Customer with copies of the then-current SOC 2 report issued by its third party independent auditors in relation to the data security policies and procedures designed to meet the requirements set forth above.

5. GLB Act Compliance. Customer Confidential Information, Customer Data and Personal Data may include the email content of Customer emails, and the rules and policies for management of email delivery. Customer retains all title, intellectual property and other ownership rights in such data. Customer Confidential Information, Customer Data and Personal Data may or may not include data, information and/or records of or pertaining to the Customer's or its Affiliate's customers (current, former or prospective), and employees (current, former or prospective) or its customers' customers (current, former or prospective) or employees (current, former or prospective), including but not limited to names, addresses, telephone numbers, account numbers, account and transaction information and any other "Nonpublic Personal Information" as defined in the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq. (the "**GLB Act**") (collectively, "**GLB Act Personal Information**"). All GLB Act Personal Information shall remain at all times during and after the term of this Policy the exclusive property of the disclosing party. Proofpoint agrees to comply with applicable law, if any, governing the Services, which may include the GLB Act, the Federal "Privacy of Consumer Financial Information" Regulation (12 CFR Part 30), as amended from time to time, issued pursuant to Section 504 of the GLB Act.

proofpoint

6. Data Breach Notification. If Proofpoint accesses Personal Data:

(i) Proofpoint is only authorized to use or disclose Personal Data for the purpose of performing under this Policy and providing the Services and Support to Customer;

(ii) Proofpoint will store Personal Data in a secure manner and use at least the same degree of reasonable care to prevent unauthorized and improper disclosure as Proofpoint uses in protecting its own confidential information, however, never less than the standard degree of care in Proofpoint's industry; and

(iii) In the event of a known unauthorized use, disclosure or acquisition by a third party of Personal Data that compromises the security, confidentiality, or integrity of Personal Data maintained by Proofpoint ("Security Breach"), Proofpoint will notify Customer in writing of the breach within 48 hours and provide periodic updates afterwards.

7. Data Breach Damages. If either party's negligence directly and solely causes a Security Breach and such unauthorized third party is one whom is reasonably suspected to misuse such Personal Data, then the negligent party shall pay the reasonable costs and expenses for breach notification and credit monitoring as required by applicable law for a period of twelve (12) months.

8. Sub-processors. Customer acknowledges and agrees that Proofpoint may engage third-party sub-processors in connection with the provision of the Proofpoint Products. To the extent Proofpoint allows any sub-processor access to Personal Data Proofpoint shall make available to Customer a current list of sub-processors upon Customer's request. The sub-processors will be limited to use of Personal Data solely to the extent necessary to provide the Proofpoint Products.

9. Financial Audit. Proofpoint will maintain billing and payment records related to this Policy for up to seven (7) years, for review upon 30 day notice, but no more than annually by Customer.

10. Governmental Audit. Upon 30 day advance written notice by Customer, Proofpoint will make its internal policies, practices, and procedures relating to the use and security of Personal Data reasonably available to relevant governmental authorities as required by applicable law.

11. US Only Data Centers [for Email Protection Customers only]. If requested in writing by a Customer of Proofpoint's Email Protection product, Proofpoint will set up the Customer's instance of the Email Protection product within Proofpoint's U.S. gateways or data centers. So long as Customer configures its MX records to point to URLs provided to Customer by Proofpoint for the instance in the United States, Customer's email will be filtered in US-based data centers.

12. Disaster Recovery/Business Continuity Planning. Proofpoint has a Disaster Recovery and Business Continuity plan, which it reviews and tests annually. Upon request, Proofpoint will provide copies of its Disaster Recovery and Business Continuity planning and management practices, and the same shall be treated and Confidential Information under this Policy. If Proofpoint experiences a business disruption in one of its services Proofpoint will implement its disaster recovery plan and will make situational update reports at an appropriate frequency determined by Proofpoint available to Customer that includes a summary description of the event, the impact to Customer, and an estimate of when services will return to normal operations.

13. Privacy Shield. Proofpoint is certified with the EU-US Privacy Shield and Swiss-US Privacy Shield regimes. Detailed information can be found at www.privacyshield.gov; look up Proofpoint on the Certified List.