

## STATE AND LOCAL / HIGHER ED (SLED) END USER LICENSE TERMS

These SLED End User License Terms shall apply to the use of Proofpoint Products by Customer pursuant to a subscription license.

**1. Definitions.** The following terms apply to each Public Sector Customer ("Customer") license of Proofpoint Products from the Public Sector Reseller or Distributor ("Contractor") under the applicable government prime contract:

**"Customer"** means only the public sector agency which has purchased the Proofpoint Product subscription license for its internal purposes and does not include any other agency or governmental subdivision unless expressly stated in this Agreement or the Proofpoint quote accompanying the purchase order.

**"Documentation"** means the technical description of the Proofpoint Product(s) contained in the then-current Product Terms.

**"Government"** means when this designation appears in a Proofpoint Product SKU, the Proofpoint Product (or Product bundle) includes one or more Proofpoint Products that are delivered inside the Federal Risk and Authorization Management Program [FedRAMP]. Refer to the FedRAMP Marketplace <https://marketplace.fedramp.gov/products> for those specific Proofpoint Products delivered inside FedRAMP.

**"Proofpoint Products"** means the appliance, service or software listed in the Contractor's Schedule Price List by and licensed by Customer from Proofpoint, Inc. ("Proofpoint") pursuant to a Customer Purchase Order ("Order").

**"Product Terms"** means the descriptions of Proofpoint Products and related terms contained at <https://www.proofpoint.com/us/legal/license/product-terms> that are hereby incorporated herein by reference and made a part hereof.

**"Service"** means any Proofpoint Product licensed on a hosted basis as software-as-a-service.

**"Software"** means any Proofpoint binary software programs licensed by Proofpoint to Customer, together with all the Software Updates.

**"User"** means Customer's employees, agents, contractors, consultants or other individuals who are licensed to use the Proofpoint Product, and each User must be assigned a separate account on Customer's email server for sending or receiving messages or data within Customer's email system or network, or if applicable, login credentials for Customer's social media accounts.

### **2. License.**

Customer is granted a limited term, non-sublicensable, non-transferable, and non-exclusive license to access or use the Proofpoint Products licensed by Customer from Contractor during the applicable subscription term, for its intended purposes, solely for Customer's internal business purposes and not for further use by or disclosure to third parties and in accordance with the Proofpoint Products Documentation and any applicable laws or regulations. Customer's right to access or use Proofpoint Products is limited to those parameters set forth in the applicable Order provided to Proofpoint including, but not limited to the maximum number of Users ("Licensed User Count") (and storage if applicable) for each module and the type of deployment (i.e., SaaS or appliance).

### **3. License Restrictions.**

Customer will not and will not allow any third party to:

- a) copy, modify, or create derivative works of the Proofpoint Products or Proofpoint Products Documentation;
- b) reverse engineer, decompile, translate, disassemble, or discover the source code of all or any portion of the Proofpoint Products except and only to the extent permitted by applicable federal law notwithstanding this limitation, provided however, that in any case, Customer shall notify Proofpoint in writing prior to any such action and give Proofpoint reasonable time to adequately understand and meet the requested need without such action being taken by Customer;
- c) remove, alter, cover or obscure any notice or mark that appears on the Proofpoint Products or on any copies or media;
- d) sublicense, distribute, disclose, rent, lease or transfer to any third party any Proofpoint Products;
- e) export any Proofpoint Products in violation of U.S. laws and regulations;
- f) attempt to gain unauthorized access to, or disrupt the integrity or performance of, a Proofpoint Product or the data contained therein;
- g) access a Proofpoint Product for the purpose of building a competitive product or service or copying its features or user interface;
- h) use a Proofpoint Product, or permit it to be used, for purposes of: (a) product evaluation, benchmarking or other comparative analysis intended for publication outside the Customer's organization without Proofpoint's prior written consent; (b) infringement or misappropriation of the intellectual property rights of any third party or any rights of publicity (e.g. a person's image, identity, and likeness) or privacy; (c) violation of any federal law, statute, ordinance, or regulation (including, but not limited to, the laws and regulations governing export/import control, unfair competition, anti-discrimination, and/or false advertising); (d) propagation of any virus, worms, Trojan horses, or other programming routine intended to damage any system or data; and/or (e) filing copyright or patent applications that include the Proofpoint Product and/or Documentation or any portion thereof; or
- i) upload or download, post, publish, retrieve, transmit, or otherwise reproduce, distribute or provide access to information, software or other material which: (i) is confidential or is protected by copyright or other intellectual property rights, without prior authorization from the rights holder(s); (ii) is defamatory, obscene, contains child pornography or hate literature; or (iii) constitutes invasion of privacy, appropriation of personality (e.g. image, identity, likeness), or unauthorized linking or framing.

Proofpoint Products are for use with normal business messaging traffic only, and Customer shall not use the Proofpoint Products for the machine generated message delivery of bulk, unsolicited emails or in any other manner not prescribed by the applicable Proofpoint Products Documentation. Proofpoint shall have the right to monitor and reset harmful outbound email configuration settings impacting the Proofpoint platform.

#### **4. Customer Responsibilities.**

Customer is responsible for (i) all activities conducted under its user logins; (ii) obtaining and maintaining any Customer equipment and any ancillary services needed to connect to, access or otherwise use the Proofpoint Products and ensuring that the Customer equipment and any ancillary services are (a) compatible with the Proofpoint Products and (b) comply with all configuration requirements set forth in the applicable Proofpoint Product Documentation; and (iii) complying with all federal laws, rules and regulations regarding the management and administration of its electronic messaging system, including but not limited to, obtaining any required consents and/or acknowledgements from its employees, agents, consultants and/or independent contractors (collectively referred to as "personnel," hereinafter) and service providers (if applicable) in managing its electronic messaging system and/or social media systems (as applicable). Customer shall be solely responsible for any damage or loss to a third party resulting from the Customer's data, or where Customer's use of the Proofpoint Products are in violation of federal law, or of this Agreement, or infringe the intellectual property rights of, or has otherwise harmed, such third party.

Customer shall (i) take all necessary measures to ensure that its users use Proofpoint Products in accordance with the terms and conditions of this Agreement; and (ii) in the case of any purchase of Proofpoint Secure Share, users of the Proofpoint Product will need to register to use the Secure Share. For the purposes of Proofpoint's compliance with its obligations under this Agreement, Customer consents to and authorizes Proofpoint (and its authorized subcontractors, subject to approval by the Contracting Officer) to retain, store and transmit any Customer information and data, subject to Government security requirements that Customer discloses to Proofpoint and pursuant to the normal functioning of Proofpoint Products. Customer information and data includes, but is not limited to (i) all configuration, rules and policies executed at Customer's direction; (ii) any document management or retention protocols that would delete, track, transmit or route documents or other data; (iii) any requests by Customer or required hereunder for log, access, support-related or other transmissions under this Agreement.

## **5. Data Security & Privacy**

5.1 Limited Use of Personal Data. Proofpoint and its subsidiaries are authorized to access and process Personal Data solely in accordance with the terms of the Agreement. Proofpoint and its subsidiaries shall take reasonable steps to ensure the reliability of any employee, agent or subcontractor who may have access to the Personal Data and will ensure access is strictly limited to those individuals who need to access the relevant Personal Data in the performance of Proofpoint's obligations under the Agreement.

5.2 Data Safeguards. Proofpoint will maintain reasonable administrative, physical, and technical safeguards for protection of the security and confidentiality of Customer Data and Personal Data, including, but not be limited to, measures for preventing unauthorized access, use, modification or disclosure of Customer Data and Personal Data. Proofpoint will comply with its Data Security, Protection, Audit and Compliance Policy at <https://www.proofpoint.com/us/legal/license> when processing any Customer Data and Personal Data.

5.3 "Customer Data" means the Customer specific configurations and rules implemented in the Proofpoint Products, and any Customer content processed by the Proofpoint Products (e.g., email text and attachments) that is not Personal Data. "Personal Data" means data about an identifiable individual that is protected by privacy laws where the individual resides. Examples of personal data include name, religion, gender, financial information, national identifier numbers, health information, email addresses, IP addresses, online identifiers and location data.

5.4 Proofpoint Products in FedRAMP. When Proofpoint delivers designated Government Proofpoint Products, notwithstanding anything contained in this license agreement to the contrary, the Proofpoint FedRAMP System Security Plan (SSP) on file with the FedRAMP Program Management Office (PMO) shall govern exclusively all data security obligations solely with respect to such Government Proofpoint Products.

## **6. Confidentiality**

6.1 Receiving Party shall not (i) disclose any Confidential Information of the Disclosing Party to any third party, except as otherwise expressly permitted herein, or (ii) use any Confidential Information of Disclosing Party for any purpose outside the scope of the Agreement, except with Disclosing Party's prior written consent. The Receiving Party shall not make Confidential Information available to any of its employees or consultants except those that have agreed to obligations of confidentiality at least as restrictive as those set forth herein and have a "need to know" such Confidential Information. The Receiving Party agrees to hold the Disclosing Party's Confidential Information in confidence and to take all precautions to protect such Confidential Information that the Receiving Party employs with respect to its own Confidential Information of a like nature, but in no case shall the Receiving Party employ less than reasonable precautions. The Agreement will not be construed to prohibit disclosure of Confidential Information to the extent that such disclosure is required to by law or valid order of a court or other governmental authority; provided, however, to the extent permitted by law, the responding party shall give prompt written notice to the other party to enable the other party to seek a protective order or otherwise prevent or restrict such disclosure and, if disclosed, the scope of such disclosure is limited to the extent

possible.

6.2 The Receiving Party will return all copies of the Disclosing Party's Confidential Information upon the earlier of (i) the Disclosing Party's request, or (ii) the termination or expiration of the Agreement. Instead of returning such Confidential Information, the Receiving Party may destroy all copies of such Confidential Information in its possession; provided, however, the Receiving Party may retain a copy of any Confidential Information disclosed to it solely for archival purposes, provided that such copy is retained in secure storage and held in the strictest confidence for so long as the Confidential Information remains in the possession of the Receiving Party.

6.3 The parties acknowledge and agree that the confidentiality obligations set forth in this Master Agreement are reasonable and necessary for the protection of the parties' business interests, that irreparable injury may result if such obligations are breached, and that, in the event of any actual or potential breach of this Confidentiality provision, the non-breaching party may have no adequate remedy at law and shall be entitled to seek injunctive and/or other equitable relief as may be deemed proper by a court of competent jurisdiction.

6.4 "Confidential Information" means all confidential and proprietary information of a party ("Disclosing Party") disclosed to the other party ("Receiving Party"), whether orally or in writing, that is designated as "confidential" or the like, or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure, including the terms and conditions of the Agreement (including pricing and other terms reflected in a Purchase Order), the Proofpoint Products business and marketing plans, technology and technical information, product designs, and business processes. "Confidential Information" shall not include information that (i) is or becomes a matter of public knowledge through no act or omission of the Receiving Party; (ii) was in the Receiving Party's lawful possession prior to the disclosure without restriction on disclosure; (iii) is lawfully disclosed to the Receiving Party by a third party that lawfully and rightfully possesses such information without restriction on disclosure; (iv) the Receiving Party can document resulted from its own research and development, independent of receipt of the disclosure from the Disclosing Party; or (v) is disclosed with the prior written approval of the Disclosing Party.

## **7. Support and Service Levels.**

7.1 Support Services. Proofpoint shall provide support and/or Managed Services provided Customer is current in payment of the applicable Subscription Fees and any additional fees for support and/or Managed Services, if applicable. Proofpoint's current support terms are described on Proofpoint's website at <https://www.proofpoint.com/us/legal/license>.

7.2 Service Levels. Proofpoint provides a Service Level Agreement ("SLA") for the applicable Proofpoint Service. The SLA is posted on Proofpoint's website at <http://www.proofpoint.com/license>. In the event of a breach of an SLA, as Customer's sole and exclusive remedy, Proofpoint shall provide the remedy set forth in the applicable SLA.

## **8. Reporting and Audit.**

Customer shall monitor and report its actual usage of the subscription-based Proofpoint Products ("License Count"). A "Base License" is the number of Licenses for which Customer has paid Subscription Fees. Customer will provide Proofpoint with a License Count on or before the date on which the then-current License Count exceeds the Base License Count by ten percent (10%) or more (if applicable) by email at [accountsreceivable@proofpoint.com](mailto:accountsreceivable@proofpoint.com). Proofpoint may also at any time produce an actual license count for verification by Customer. If, in either case, the License Count is greater than the Base License, Customer shall pay the Contractor upon receipt of an invoice for each License beyond the Base License from the time such Licenses were activated through the remainder of the Initial Term or Extension Term, as applicable.

## **9. Warranty.**

9.1 Warranties and Remedies.

(a) *Performance Warranties.* Proofpoint warrants that during the Subscription Term the applicable

Service (“SaaS Warranty”) and Software (“Software Warranty”) will substantially conform in all material respects to the Documentation. Customer will provide prompt written notice of any non-conformity. Proofpoint may modify the Documentation in its sole discretion. The Software Warranty does not apply to: (a) Software that has been modified by any party other than Proofpoint; or (b) Software that has been improperly installed or used in a manner other than as authorized under the Agreement.

(b) *SaaS and Software Warranty Remedy.* As Customer’s sole and exclusive remedy and Proofpoint’s entire liability for any breach of the SaaS Warranty or the Software Warranty, Proofpoint will (a) use reasonable efforts to fix, provide a work around, or otherwise repair or replace the Service or Software, as applicable, or if Proofpoint is unable to do so, (b) terminate the license to use such component of the Service or the applicable Software and return the Subscription Fees paid to Proofpoint for such allegedly defective Service or Software, as applicable, for the period commencing from Customer’s notice of nonconformity through the remainder of the Initial Term or Extension Term, as applicable.

## **9.2 Warranty Disclaimers.**

**EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH ABOVE, PROOFPOINT AND PROOFPOINT LICENSORS DISCLAIM ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AS WELL AS ANY WARRANTIES OF REGULATORY COMPLIANCE, PERFORMANCE, ACCURACY, RELIABILITY, AND NONINFRINGEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THE AGREEMENT.**

**PROOFPOINT DOES NOT WARRANT: (I) THE ACCURACY OF THE INTENDED EMAIL BLOCKING OF ANY MAIL MESSAGE; (II) THAT EMAIL WILL NOT BE LOST; (III) THAT THE OPERATION OF THE PROOFPOINT PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE; (IV) THAT ALL SOFTWARE ERRORS WILL BE CORRECTED; OR (V) THAT THE PROOFPOINT PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS OR ATTACKS.**

## **10. Limitation of Liability.**

All consequential, incidental, special, punitive, exemplary, and indirect damages (including lost profits and loss of data) are disclaimed on behalf of Proofpoint (and Proofpoint is also required under its contracts with its suppliers and licensors to state in this Agreement that such suppliers and licensors also disclaim such damages herein). The foregoing exclusions/limitations of liability shall not apply (1) to personal injury or death caused by Proofpoint’s negligence or fraud; (2) for express remedies requiring the specific type of relief under the law or these license terms; or (3) for any other matter for which liability cannot be excluded by law.

EXCEPT FOR (i) INTELLECTUAL PROPERTY INDEMNIFICATION OBLIGATIONS HEREIN, (ii) DAMAGES RESULTING FROM EITHER PARTY’S GROSS NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT, (iii) DAMAGES RESULTING FROM EITHER PARTY’S MATERIAL BREACH OF THE CONFIDENTIALITY SECTION, (iv) CUSTOMER’S BREACH OF THE CUSTOMER RESPONSIBILITIES SECTION, EACH PARTY’S AGGREGATE LIABILITY UNDER THE AGREEMENT FOR ANY CLAIMS, DAMAGES, OR LIABILITIES (“CLAIMS”) SHALL IN NO EVENT EXCEED THE SUBSCRIPTION FEES PAID FOR THE APPLICABLE PROOFPOINT PRODUCT OVER THE PRECEDING TWELVE MONTHS FROM WHEN SUCH CLAIM AROSE.

## **11. Intellectual Property Rights.**

11.1 Ownership. Customer retains all title, intellectual property and other ownership rights in all Customer Confidential Information, Customer Data and all data that Customer makes available for processing by the Proofpoint Products. Proofpoint retains all title, intellectual property and other ownership rights throughout the world in and to the Proofpoint Products, Documentation, and any work product and any modifications to, and derivative works of, the foregoing. Proofpoint hereby grants to Customer a non-exclusive, non-transferable, fully paid-up license to use any work product in connection with the Proofpoint Product licensed under the Agreement and solely for Customer’s internal business purposes.

11.2 No Implied Rights. There are no implied rights and all rights not expressly granted herein are reserved. No license, right or interest in any Proofpoint trademark, copyright, patent, trade name or service mark is granted hereunder. Customer shall not remove from any full or partial copies made by Customer of the Software, Software Updates and Documentation any copyright or other proprietary notice contained in or on the original, as delivered to Customer.

11.3 Proofpoint Authorization and License. During the Term of the Agreement, Customer hereby (i) grants to Proofpoint and its service providers a worldwide, limited term license to collect and process certain Customer Confidential Information and Customer Data, and (ii) authorizes Proofpoint to collect and process certain Personal Data, for: (a) abuse, fraud and threat awareness, detection and prevention, (b) compliance, and (c) security purposes, in accordance with the Agreement. "Customer Data" means the Customer specific configurations and rules implemented in the Proofpoint Products, and any Customer content processed by the Proofpoint Products (e.g., email text and attachments) that is not Personal Data.

Customer acknowledges and agrees that development of Threat Analytics from Proofpoint's ecosystem is critical to the functionality of the Proofpoint Products. Customer hereby authorizes Proofpoint to collect Threat Analytics during the Term of the Agreement. Further, Customer hereby authorizes Proofpoint to use Threat Analytics worldwide to build, enhance, improve and maintain Proofpoint services; provided that if Customer provides written legal notice to Proofpoint on or after expiration or termination of the applicable Proofpoint Services instructing Proofpoint to delete any Personal Data included in Threat Analytics, it will be deleted within 18 months of such notice. "Threat Analytics" means information collected, generated and/or analyzed by the Proofpoint Products such as log files, statistics, aggregated data and derivatives thereof.

## **12. Intellectual Property Rights Indemnification**

12.1 Proofpoint's Duty to Indemnify. Subject to the subsections below within this section, Proofpoint agrees to defend and indemnify Customer from and against any third-party claim filed against Customer alleging that the Proofpoint Product(s), as sold and delivered to Customer (the "Indemnified Products"), directly infringe the valid intellectual property rights of a third party (an "IP Claim"). Proofpoint agrees to pay and hold Customer harmless against any amounts finally awarded by a court having competent jurisdiction in respect of such IP Claim or pursuant to a settlement accepted by Proofpoint in writing. Proofpoint may, at its sole election and expense: (i) procure sufficient rights to allow Customer continued use of the Indemnified Products under the terms of the Agreement; (ii) replace or modify the Indemnified Products to avoid the alleged infringement; or (iii) if the foregoing options are not reasonably practicable, terminate Customer's rights to use the Indemnified Products and refund all amounts paid by Customer to Proofpoint attributable to Customers' future usage or access to the Indemnified Products.

12.2 Exclusions. Proofpoint shall have no obligation or any liability to Customer for any IP Claim arising out of or related to: (i) modifications or adaptations to the Indemnified Products made by Customer or Customer's agents; (ii) the use of the Indemnified Products in combination with any other product, service or device, if the IP Claim would have been avoided by the use of the Indemnified Products without such other product, service or device not provided by Proofpoint to Customer or Customer's agents; (iii) compliance with Customer's specific instructions for customization of an Indemnified Product made solely for or on behalf of Customer; (iv) use or exploitation of the Indemnified Products other than as set forth in the Agreement or applicable Documentation; or (v) Customer being given an update, modification, or replacement to an Indemnified Product by Proofpoint and failing to implement such update, modification, or replacement within a reasonable period of time.

12.3 Process. Proofpoint's obligations under this section are conditioned upon the following: (i) Customer first providing written notice of the IP Claim to Proofpoint within thirty (30) days after Customer becomes aware of or reasonably should have been aware of the IP Claim (provided, however, the failure to provide such notice will only relieve Proofpoint of its indemnity obligations hereunder to the extent Proofpoint is prejudiced thereby); (ii) Customer tendering control of the IP Claim to Proofpoint at the time Customer provides written notice of such IP Claim to Proofpoint; and (iii) Customer providing reasonable assistance, cooperation and required information with respect to defense and/or settlement of the IP Claim. Customer may at its sole expense participate in the IP Claim defense, except that Proofpoint will retain sole control of the defense and/or settlement, to the extent consistent with applicable State law. Proofpoint shall not

agree to any settlement of an IP Claim that includes an injunction against Customer or admits Customer liability without Customer's prior written consent.

12.4 **Exclusive Remedy.** This section describes the sole and exclusive remedy of Customer and the entire liability of Proofpoint with respect to any IP Claim.

### 13. **Term/Termination.**

Upon expiration of the initial term and any extension term(s) under each Purchase Order, the Subscription Term applicable to such Purchase Order may be renewed for subsequent extension terms upon mutual written agreement of the Parties.

Either party may terminate the Agreement or any Purchase Order (i) immediately upon written notice if the other party commits a non-remediable material breach; or (ii) if the other party fails to cure any remediable material breach within thirty (30) days of being notified in writing of such breach.

On termination or expiration of the Agreement, all Software licenses, Service access, granted under the Agreement shall automatically terminate with immediate effect. In the event of the termination or expiration of the Agreement, the provisions of the Agreement which by their nature extend beyond the expiration or termination of the Agreement shall survive. Within thirty (30) days after expiration or termination of the License to use the Proofpoint Product, Customer shall: (i) certify in writing to Proofpoint that all copies of the Software, Software Updates, and Documentation in any form, including partial copies or extracts thereof, have been destroyed or returned to Proofpoint, and (ii) retrieve or dispose of Customer data from or within the Proofpoint Products and/or systems. Upon 30 days of termination of the License to use the Proofpoint Product, Customer data in the Proofpoint Product and/or systems may be rendered illegible, deleted or written over, including any back-up Customer data.

### 14. **Miscellaneous.**

**A. Governing Law.** This Agreement shall be governed by the law of the State where the Customer resides, exclusive of its choice of laws rules. The Uniform Computer Information Transaction Act shall not apply to this Agreement.

**B. Force Majeure.** Neither party shall be liable to the other for any delay or failure to perform hereunder due to circumstances beyond such party's reasonable control, including, acts of God, or the public enemy, acts of Government in its sovereign or contractual capacity, fires, floods, earthquakes, epidemics, quarantine restrictions, strikes, unusually severe weather and delays of common carriers, and other acts beyond a party's reasonable control or possession including acts, civil unrest, acts of terror, strikes or other labor problems (excluding those involving such party's employees) or third-party service disruptions involving hardware, software or power systems and denial of service attacks.

**C. Entire Agreement.** This Agreement constitutes the entire agreement of the parties and supersedes all prior or contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. No amendment or waiver of any provision of the Agreement shall be effective unless in writing and signed by the party against whom the amendment or waiver is to be asserted. Notwithstanding any language to the contrary therein, any Purchase Order issued by Customer or Reseller shall be deemed a convenient order and payment device only and no terms (other than product name, license quantity, price, Subscription Term, and billing contact) stated in any Purchase Order shall be incorporated into the Agreement, and all such other terms shall be void and of no effect.

**D. Severability.** If any clause of the Agreement shall be adjudged by any board, court or tribunal of competent jurisdiction to be invalid or unenforceable, such judgment shall not affect, impair or invalidate the remainder of the Agreement, which shall remain enforceable by the parties.

**E. Open Source Software:** Proofpoint Appliance/Software for Customer On-Site Deployment. Open Source Software may be a component of the Software provided to Customer for on-site deployment. Proofpoint is required by Open Source Software requirements to inform the end user of certain facts, including the following:

“Open Source Software” means various open source software, including GPL software which is software licensed under the GNU General Public License as published by the Free Software Foundation, and components licensed under the terms of applicable open source license agreements included in the materials relating to such software. Open Source Software is composed of individual software components, each of which has its own copyright and its own applicable license conditions. Customer may obtain information (including, if applicable, the source code) regarding the inclusion of Open Source Software in the Software by sending a request, with Customer’s name and address to Proofpoint at the address specified in the Order. Customer may redistribute and/or modify the GPL software under the terms of the GPL. A copy of the GPL is included on the media on which Customer receives the Software or included in the files if the Software is electronically downloaded by Customer. This offer to obtain a copy of the source files for GPL software is valid for three (3) years from the date Customer acquired the Appliance Software.

**F. Annual Appropriation/Limitation of Funds.** To the extent a contract is funded with annual governmental appropriations, the following terms apply:

Funds are not presently available for performance under this contract beyond the expiration of 1] the Initial or Renewal Term (as applied to one-year subscription term contracts with renewal periods); or, 2] each annual subscription term under a multi-year contract, as applicable. To the extent that either the Government gives written notice, or the Partner provides written notice from the Government, of lack of funds to the Partner or Proofpoint, the Partner’s obligation for performance of this contract beyond the above applicable subscription term expiration date is contingent upon the availability of such appropriated funds from which payment for contract purposes can be made.



## Data Security, Protection, Audit and Compliance Policy

The data security, protection, audit and compliance terms (“Policy” or “Data Security 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.

1. 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 (“Customer Information”). The information security program may include, but is not limited to, multi-factor authentication for logging into data systems, conducting regular penetration tests, maintaining and regularly evaluating the security program, and maintaining system and facilities access controls. Proofpoint employees and contractors are required to undergo regular data privacy and security training.

2. Security Measures. 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 (“SOC 2”), received from its third-party auditors. 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 in this Data Security Policy.

3. 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.

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.

5. Background checks. Where permitted by applicable law, 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”). 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.

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 validated 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 72 hours and provide periodic updates afterwards that include (to the extent known by Proofpoint) details of the cause of the Security Breach, measures being taken to mitigate the effects of the Security Breach, anticipated impact to Customer and individuals, and anticipated timeframe for stopping the Security Breach.

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. Proofpoint maintains a list of sub-processors on the [Proofpoint Trust](#) site.

9. Subcontractors. Proofpoint shall perform all Services and Professional Services using only its own employees or contractors. Except for staff augmentation, if Proofpoint desires to engage any subcontractors to perform any portion of the Services or Professional Services hereunder, Proofpoint will provide written notice to Customer prior to engaging any such subcontractor. In addition, if Proofpoint utilizes a subcontractor to perform any portion of the Services or Professional Services: (i) Proofpoint will be responsible for the direction and coordination of the services of subcontractors; (ii) 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 (iii) Customer shall have no obligation to pay or to be responsible for, in any way, the payment of monies to any subcontractor.

10. 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.

11. 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.

12. 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.



## Secure Email Relay Service Level Agreement

### 1. Standard Terms Applicable to the SLA:

#### A. Definitions.

Except as otherwise modified or defined herein, all capitalized terms in this SLA have the same meanings as set forth in the Agreement. For purposes of this SLA, the following definitions will apply.

**A.1 “Emergency Maintenance”** means any time outside of the Scheduled Maintenance Window where Proofpoint is required to apply urgent patches or fixes or undertake other urgent maintenance activities. If Emergency Maintenance is required, Proofpoint will contact Customer and provide the expected start time and the planned duration of the Emergency Maintenance and if Proofpoint expects the SER service to be unavailable during the Emergency Maintenance.

**A.2 “Scheduled Maintenance Window”** means the window during which weekly scheduled maintenance of the Secure Email Relay (SER) service may be performed. The Scheduled Maintenance Window is between the hours of Friday 9:00 p.m. to Saturday 5:00 a.m. Pacific time.

**A.3. “Service Credit”** is defined in Section B.

**A.4 “System Availability”** is defined in Section E.

#### B. Service Credits.

**B.1 “Service Credit”** means the percentage of the monthly Subscription Fees paid or payable for the SER service product that is awarded to Customer for a validated claim associated with that portion of the SER service related to breach of the applicable SLA during that month.

**B.2** In any given month, Customer shall in no event be entitled to receive a credit that exceeds 100% of its monthly Subscription Fee for the nonconforming SER service product.

**B.3** Any Service Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next SER service product subscription period for which the Service Credit applies. Service Credits earned by Customer hereunder will be applied against amounts due for an Extension Term.

#### C. SLA Claims

**C.1** Customer must notify Proofpoint Customer Support via support ticket within five (5) business days from the occurrence of the SLA incident. Customer’s claim ticket must identify which specific SLA applies and the details of the relevant incident. Distributors and channel partners may NOT open SLA tickets on behalf of Customer. Failure to comply with these reporting requirements may forfeit Customer’s right to receive a remedy in connection with an SLA.

**C.2** For all claims subject to validation by Proofpoint, Proofpoint will use log files, database records, auditlogs, and any other information available to validate claims and make a good faith judgment on the applicability of SLAs to said incident. Proofpoint shall make information used to validate an SLA claim available for auditing by Customer at Customer’s request.

**C.3** In the event that more than one aspect of a SER service product is affected by the same root cause, the single SLA applicable to such SER service product of Customer’s choosing may be claimed and no other claim will be validated or otherwise allowed for that event.



**C.4** The remedies set forth herein represent Customer’s sole and exclusive remedy for Proofpoint’s breach of the SLAs defined in the SLA.

**D. Exclusions**

**D.1** Customer shall not have any remedies under any SLA to the extent any SLA claim is due to: (i) use of the SER outside the scope described in the Agreement; (ii) Customer Equipment and/or third party software, hardware or network infrastructure outside of Proofpoint’s data center and not under the direct control of Proofpoint; (iii) failure of Customer to meet the configuration requirements for Customer Equipment set forth in the Documentation; or (iv) a Force Majeure Event.

**E. The following SLA applies to Proofpoint Secure Email Relay System Availability**

**E.1** Proofpoint warrants at least 99.9% Secure Email Relay (SER) System Availability to securely route Customer’s outbound email (excluding bulk mail, newsletters and spam) and to access the SER Web console during each calendar month. System Availability means the total time during which SER is available to Customer, excluding the Scheduled Maintenance Window and Emergency Maintenance.

**E.2** Remedy: If SER System Availability is less than 99.9% and if Customer has fulfilled all obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this SER System Availability has occurred. The Service Credit will be calculated in accordance with the table below.

<b>% of Secure Email Relay System Availability per Calendar Month</b>	<b>Service Credit</b>
<99.9%	25%
<98%	50%
<95%	100%