

END USER LICENSE TERMS

The following terms apply to each Public Sector Customer ("Customer") license of Proofpoint Products from the Public Sector Contractor ("Reseller" or "Contractor") under the applicable Schedule Contract:

"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").

"Documentation" means the description of the Proofpoint Product(s) contained in the then current Proofpoint Product descriptions provided by Proofpoint to Customer upon purchase or License of the Proofpoint Product(s), and the user manuals relating to the use of the Proofpoint Products that are either provided on-line at the time of Customer's purchase of the Proofpoint Product, embedded in the Proofpoint Product(s) or delivered with the Proofpoint Product. The Documentation does not contain additional legal terms and conditions, but serves to provide the Customer with user manuals and specifications applicable to the Proofpoint Product.

"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.

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 Reseller 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 federal 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).

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.

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.

Support and Service Levels. For Customers who purchase Support Services, Proofpoint shall provide Support Services in accordance with Proofpoint's standard support terms which are currently described on Exhibit A.

Reporting. Customer is under no obligation to increase the number of Users its uses for subscription based Proofpoint Products based on User count. However, Customer understands and agrees that if Customer adds Users to the Licensed User Count for such Proofpoint Products that exceed 10 percent of the Licensed User Count, Reseller or Contractor shall invoice Customer for the additional Users.

Customer shall also audit its User count on the thirtieth (30th) day preceding each anniversary of the Effective Date. Proofpoint may also itself at any time produce a count of the actual User Count for

verification by Customer. If such number exceeds the Licensed User Count, Reseller or Contractor shall invoice Customer for the additional Users.

Warranty Disclaimer. PROOFPOINT DISCLAIMS (AND PROOFPOINT IS ALSO REQUIRED UNDER ITS CONTRACTS WITH ITS SUPPLIERS AND LICENSORS TO STATE THAT SUCH SUPPLIERS AND LICENSORS ALSO DISCLAIM) ANY AND ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, INCLUDING WITHOUT LIMITATION REGULATORY COMPLIANCE, PERFORMANCE, ACCURACY, RELIABILITY, AND NONINFRINGEMENT. PROOFPOINT DOES NOT WARRANT THAT THE ACCURACY OF THE PROOFPOINT PRODUCTS WILL MEET CUSTOMER'S REQUIREMENTS OR THAT NO EMAIL WILL BE LOST OR THAT THE PROOFPOINT PRODUCTS WILL NOT GIVE FALSE POSITIVE OR FALSE NEGATIVE RESULTS OR THAT ALL SPAM AND VIRUSES WILL BE ELIMINATED OR THAT LEGITIMATE MESSAGES WILL NOT BE OCCASIONALLY QUARANTINED AS SPAM. PROOFPOINT DOES NOT WARRANT THE OPERATION OF THE PROOFPOINT PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE. PROOFPOINT DOES NOT WARRANT THE ACCURACY OF MANAGEMENT OF ANY DOCUMENT, OR THAT NO DOCUMENT WILL BE LOST. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT.

Disclaimer of Liability. All direct, 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; (2) for fraud; (3) for express remedies requiring the specific type of relief under the law or the contract; or (4) for any other matter for which liability cannot be excluded by law.

Proofpoint Contract Rights. Proofpoint shall have the right to monitor and reset harmful outbound email configuration settings impacting the Proofpoint platform.

Law. This Agreement shall be governed by the federal law of the United States. The Uniform Computer Information Transaction Act shall not apply to this Agreement.

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.

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.

Termination. When the end user is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be made as a dispute under the Contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Proofpoint and the Contractor shall proceed diligently with performance of this contract, pending final resolution of any request for relief, claim, appeal, or action arising under the contract, and comply with any decision of the Contracting Officer or a court of competent jurisdiction. 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.

Product Specific Terms. Some Proofpoint Products include additional terms, set forth on Exhibit B to this Agreement.

EXHIBIT A

SUPPORT SERVICES PROGRAM FOR PROOFPOINT CUSTOMERS

Overview: The support services described herein are provided by Proofpoint to each Customer pursuant to the terms and conditions of the applicable license agreement (“Agreement”) between each Customer and Proofpoint or between a Customer and an authorized Proofpoint partner. Capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement. Subject to customer paying the applicable support related fees, Proofpoint will provide the support described herein.

1. Bronze Support services consist of the following:

1.1 Error Corrections. Proofpoint shall use commercially reasonable efforts to correct and/or provide a work-around for any error reported by Customer in the current unmodified release of the Software in accordance with the priority level reasonably assigned to such error by Customer.

1.2 Software and Documentation Updates. Proofpoint shall provide to Customer one (1) electronic copy of all updated revisions to the Documentation and one (1) electronic copy of generally released bug fixes, maintenance releases and updates of the Software (collectively, “Updates”). Updates do not include products or options that are designated by Proofpoint as new products or options for which Proofpoint charges a separate fee. Software releases are supported for the current and prior release that are designated by a change to the right of the decimal (e.g. 1.1 to 1.2). Prior to discontinuing support services for any Software product line, Proofpoint shall provide at least six (6) months advance notice on its support website.

1.3 Support Requests and Named Support Contacts. Technical support is available during the technical support hours for the primary support center specified on the Product Order Form. Technical support hours for the Americas are Monday through Friday, 12:00 UTC to 03:00 UTC the following day (e.g. 07:00am to 10:00pm EST during standard time and excluding Proofpoint holidays). Technical support hours for Europe are Monday through Friday, 04:00 UTC to 19:00 UTC (e.g. 05:00am CET to 08:00pm CET during standard time and excluding Proofpoint holidays). Technical support hours for Asia Pacific are Sunday through Thursday 21:00 UTC to 12:00 UTC (e.g. Monday through Friday 06:00am JST to 09:00pm JST during standard time and excluding Proofpoint holidays). Technical support hours for the Middle East are Saturday through Thursday 03:00 UTC to 15:00 UTC (e.g. 07:00am GST to 07:00pm GST during standard time and excluding Proofpoint holidays). Customer may initiate electronic Support requests through Proofpoint’s web-based call submission and tracking system (“CTS”) at any time. Support request submitted via CTS will be addressed by Proofpoint during the Support hours listed above. Customer will promptly identify two internal resources who are knowledgeable about Customer’s operating environment and operation of the Proofpoint Products (collectively, “Named Support Contacts”). Named Support Contacts will serve as primary contacts between Customer and Proofpoint and are the only persons authorized to interact with Proofpoint Technical Support, including accessing CTS to submit and track cases. All Support requests will be tracked in CTS and Customer can view the status of Customer’s cases on CTS at any time.

1.4 Platinum Support. In addition to the Bronze support services defined above, for an additional charge, Customer shall receive (i) two additional Named Support Contacts (for a total of four) and Proofpoint shall provide assistance for Priority I errors, as reasonably determined by Proofpoint, 24x7, 365 days per year; and (ii) a dedicated phone line for submitting cases. Handling of non-Priority I errors will take place during the support hours specified in Section 1.3 above.

1.5 Premium Support. In addition to the Bronze and Platinum support services defined above, for an additional charge, (i) Customer shall receive (i) two additional Named Support Contacts (for a total of six) and (ii) Proofpoint will assign a designated Technical Account Manager to Customer’s account.

1.6 Global Time Zone Add On. Any Customer that has purchased support at the Platinum level or higher, may purchase the Global Time Zone Add On. For an additional charge, Customer shall receive six additional Named Support Contacts (for a total of twelve) and Proofpoint shall provide assistance for errors of any priority, as reasonably determined by Proofpoint, 24x7, 365 days per year; and (ii) a dedicated phoneline.

1.7 Named Support Contact Training. In order to receive support in accordance with the foregoing, within ninety days of the Effective Date, all Named Support Contacts must take and pass exam(s), as applicable and available, to become an “Accredited Engineer” for each Proofpoint Product licensed by Customer. If any Named Support Contact fails to pass the exam, Proofpoint may reasonably request that such Named Support Contact be replaced by Customer. Failure to pass the applicable exam(s) may result in limited access to CTS.

2. Priority Levels of Errors and Responses

In the performance of Support services, Proofpoint will apply the following priority ratings.

2.1 Priority I Errors.

A "Priority I Error" means a Software program error which both (i) prevents some critical function or process from substantially meeting the Documentation and (ii) seriously degrades the overall performance of such function or process such that no useful work can be done and/or some primary major function of the Software or Appliance is disabled. Priority I Errors shall receive an initial response within one (1) hour (during standard Support hours referenced above), of the case being submitted to Proofpoint. In addressing a Priority I Error, Proofpoint shall use all reasonable efforts to develop suitable workaround, patch, or other temporary correction to restore operation as soon as possible. Proofpoint efforts to resolve a Priority 1 Error will include the following: (1) assigning one or more senior Proofpoint engineers on a dedicated basis to develop suitable workaround, patch, or other temporary correction; (2) notifying senior Proofpoint management that such P1 Error has been reported; (3) providing Customer with periodic reports on the status of corrections; and (4) providing a final solution to Customer as soon as it is available.

2.2 Priority II Errors.

A "Priority II Error" means a Software program error which both (i) degrades some critical function or process from substantially meeting the Documentation and (ii) degrades the overall performance of such function or process such that useful work is hindered and/or some major function of the Software or Appliance is not operating as expected but can be worked-around. Priority II Errors shall receive an initial response within four (4) hours (during standard Support hours referenced above). Proofpoint shall use all reasonable efforts to provide a workaround, patch, or other temporary correction as soon as possible.

2.3 Priority III Errors. Description: A "Priority III Error" means a Software program error which both (i) prevents some non-essential function or process from substantially meeting the Documentation and (ii) significantly degrades the overall performance of the Software or Appliance. Priority III Errors shall receive an initial response within eight (8) hours (during standard Support hours referenced above). Proofpoint shall use all reasonable efforts to provide a workaround, patch, or other temporary correction as soon as possible.

2.4 Priority IV Errors.

A "Priority IV Error" means a Software program error which prevents some function or process from substantially meeting the Documentation but does not significantly degrade the overall performance of the Software or Appliance. Priority IV Errors shall receive an initial response within sixteen (16) hours (during standard Support hours referenced above). Proofpoint shall use all reasonable efforts to include a workaround, patch, or other temporary correction in the next Software update.

3. Customer Cooperation.

Proofpoint's obligation to provide Support services is conditioned upon the following: (i) Customer's reasonable effort to resolve the problem after communication with Proofpoint; (ii) Customer's provision to Proofpoint of sufficient information and resources to correct the problem, including, without limitation, remote access as further discussed in these policies, (iii) Customer's prompt installation of all Software maintenance releases, bug fixes and/or work-around supplied by Proofpoint, and (iv) Customer's procurement and installation and maintenance of all hardware necessary to operate the Software. As related to Priority I Errors, Customer shall provide continuous access to appropriate Customer personnel and the Appliance (if applicable) during Proofpoint's response related to the Priority I Error or Proofpoint shall be permitted to change the Priority of the error. During the term of the Support services and for purposes relating to providing Support to Customer, Proofpoint may obtain information regarding Customer's e-mail communications and Customer agrees that Proofpoint may use any statistical data generated relating to Customer's e-mail. Notwithstanding the foregoing, Proofpoint shall not disclose the source and content of any such e-mail.

4. Reproducing Problems; Remote Access.

Subject to the applicable Support services fees, Support services assistance is limited to Software on platforms that are fully supported, running unaltered on the proper hardware configuration. Where applicable for a reported error, Proofpoint will use commercially reasonable efforts to reproduce the problem so that the results can be analyzed. Proofpoint's obligation to provide the Support services described herein, including without limitation meeting the response times set forth in Section 2 above, is subject to Customer providing shell or Web-based remote access to Customer's computer system(s) and network. Any such remote access by Proofpoint shall be subject to Proofpoint's compliance with Customer's security and anti-virus procedures and the confidentiality requirements set forth in the license agreement between Proofpoint and Customer. Any delay occasioned by Customer's failure to provide the foregoing remote access shall extend the response time periods set forth in Section 2 accordingly and resolution of the problem may be subject to payment of additional fees. Prior to proceeding with work that will be subject to additional fees, Proofpoint will notify Customer and will not start such work until Proofpoint receives authorization from Customer. If Customer fails to provide remote access to its computer system(s) and network and Proofpoint and Proofpoint and Customer cannot agree on a mutually

satisfactory alternative method of reproducing the problem, Proofpoint shall not be obligated to resolve the problem.

5. Support Services Conditions.

5.1 Support Issues Not Attributable to Proofpoint. Proofpoint is not obligated to provide Support services for problems related to: (i) unauthorized modifications and/or alterations of the Software, (ii) improper installation of the Software by non-Proofpoint personnel, use of the Software on a platform or hardware configuration other than those specified in the Documentation or in manner not specified in the Documentation, or (iii) problems caused by the Customer's negligence, hardware malfunction, or third-party software. In the event Proofpoint provides Support services for problems caused by any of the above, Customer will reimburse Proofpoint for such services at the then-current time and materials rate. Proofpoint shall be entitled to discontinue Support services in the event of Customer's non-payment of Subscription Fees when due.

5.2 Exclusions from Support services.

The following items are excluded from Support services:

(a) In-depth training. If the Support request is deemed to be training in nature, and will require an extended amount of time, Customer will be referred to Proofpoint's training or consulting departments.

(b) Assistance in the customization of the application. Support services do not include providing assistance in developing, debugging, testing or any other application customization

(c) Information and assistance on third-party products. Issues related to the installation, administration, and use of enabling technologies such as databases, computer networks, and communications (except an Appliance) are not provided under Proofpoint Support services.

(d) Assistance in the identification of defects in user environment. If Proofpoint concludes that a problem being reported by a Customer is due to defects in Customer's environment, Proofpoint will notify the Customer. Additional support by Proofpoint personnel to remedy performance issues due to the user environment are categorized as consulting services, which are provided for an additional fee.

(e) Installation. Support Services provided herein do not include the use of Proofpoint Support services resources to perform installation of updates or Customer-specific fixes.

If Customer wishes to have Proofpoint perform services related to any of the above items, such services will be performed pursuant to a mutually executed SOW.

6. Description of Appliance Support Services.

6.1 Services.

For as long as the Appliance purchased by Customer is under Proofpoint's Appliance warranty, Customer shall contact Proofpoint for any and all maintenance and support related to the Appliance. If support for the Appliance purchased by Customer includes on-site support, Proofpoint shall provide or cause to be provided 8-hour response service during the support hours specified in Section 1.3. A technician will arrive on-site, depending on Customer's location and the availability of necessary parts, as soon as practicable (within the business hours specified in Section 1.3) after problem determination. Optional 24x7 service is available subject to Section 1.4.

6.2 Customer Obligations.

Customer must also install remedial replacement parts, patches, software updates or subsequent releases as directed by Proofpoint in order to keep Customer's Appliance eligible for Support services. Customer agrees to give Proofpoint at least thirty (30) days written notice prior to relocating Appliance. It is Customer's responsibility to back up the data on Customer's system, and to provide adequate security for Customer's system. Proofpoint shall not be responsible for loss of or damage to data or loss of use of any of Customer's computer or network systems. Customer agrees to provide the personnel of Proofpoint or its designee with sufficient, free, and safe access to Customer's facilities necessary for Proofpoint to fulfill its obligations.

6.3 Exclusions.

Appliance Support services do not cover parts such as batteries, frames, and covers or service of equipment damaged by misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by Customer, removal or alteration of equipment or parts identification labels, or failure caused by a product for which Proofpoint is not responsible.

EXHIBIT B

PRODUCT SPECIFIC TERMS

DEFINITION

“**Customer Equipment**” means Customer’s computer hardware, software and network infrastructure used to access the Proofpoint Products.

DIGITAL RISK SUITE PRODUCTS

The Digital Risk suite includes any combination of the following: Domain Discover for Digital Risk, Mobile Discover, Social Archiver, Social Anglerphish, Social Discover, Social Patrol, Social Sight, and Social Syndicate, and any future names or bundles by which Proofpoint identifies and makes available these Products.

Customer Responsibilities. Customer is responsible for (i) all activities conducted under its User logins; (ii) obtaining and maintaining any necessary equipment and configurations set forth in the Documentation; and (iii) complying with all applicable laws, rules and regulations, and acquiring all necessary data subject consents. Customer is responsible for maintaining the user accounts and the security of its user names and passwords at the user level and for promptly changing or deleting any user name or password that Customer believes may have been compromised. Proofpoint reserves the right to institute password requirements (such as the length of password or the required use of numbers, symbols etc.) and to refuse registration of, or cancel passwords it deems inappropriate.

Third-Party Services. The Proofpoint Products may allow Customer to interface with a variety of third-party software or services (e.g., Facebook, Twitter, LinkedIn). No endorsement of any such service should be inferred as a result of any integration with the Proofpoint Products and Proofpoint is not responsible for the data, operation or functionality of such third-party services. While Proofpoint may, in its sole discretion, customize the Proofpoint Products to interoperate with various third-party services: (i) Customer is responsible for complying with the terms and policies of each such third-party service including, without limitation, any payment obligations related thereto; and (ii) Proofpoint cannot guarantee that such third-party services will continue to interoperate with the Service.

INFORMATION & COMPLIANCE SUITE

The Information & Compliance suite includes any combination of the following: Archive, Archiver, Compliance Gateway, Content Collection, eDiscovery Analytics, Governance, and Supervision, and any future names or bundles by which Proofpoint identifies and makes available these Products.

Archive. Customer’s right to use Archive is limited to the maximum number of Users and storage amount for each module specified in each Quote and/or Purchase Order. Provided Customer has purchased the applicable license, Customer may use the user interface provided on the Appliance to search customer data and export customer data. 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 Archive and ensuring that the Customer Equipment and any ancillary services are (a) compatible with Archive and (b) comply with all configuration requirements set forth in Archive Documentation; and (iii) complying with all 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 and service providers (if applicable) in managing its electronic messaging system; and (iv) disposition of customer data after the expiry of the applicable retention period. Proofpoint warrants that the Archive storage media meets the conditions set forth in SEC Rule 17a-4 paragraph f (2) (ii), which requires electronic storage media to (i) preserve the records exclusively in a non-rewriteable, non-erasable format; (ii) verify automatically the quality and accuracy of the storage media recording process; (iii) serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media; and (iv) have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable as required by the SEC or the self-regulatory organizations of which the member, broker, or dealer is a member. Upon termination or expiration of Customer’s license to use the Proofpoint Product, for a period of thirty (30) days after termination or expiration (“Wind Down Period”) Customer may continue to access and retrieve its data that has been stored in the Archive product prior to termination.

During the Wind Down Period, Customer may not use the Proofpoint Product to archive new email messages. For an additional fee, Proofpoint will export customer's data for delivery to Customer on standard storage media. If Proofpoint has not received a written request from Customer to export customer's data prior to the end of the Wind Down Period, Proofpoint will initiate the removal of customer's data in such a manner that it cannot be restored in human readable form from any and all storage mediums (including backups), which will be completed within thirty (30) days.

Content Collection. 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 Content Collection and ensuring that the Customer Equipment and any ancillary services are (a) compatible with Content Collection and (b) comply with all configuration requirements set forth in Content Collection Documentation; and (iii) complying with all laws, rules and regulations regarding the management and administration of its electronic messaging and/or enterprise collaboration systems, including but not limited to, obtaining any required consents and/or acknowledgements from its employees and service providers (if applicable) in managing its electronic messaging and/or enterprise collaboration system. Customer shall have obtained or obtain appropriate consent or authorization and be deemed to have consented to and authorized Proofpoint (and its authorized subcontractors) to retain, store and transmit any Customer Confidential Information (including, but not limited to, Customer specific configuration settings) pursuant to the normal functioning of Content Collection, including but 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; and (iii) any requests by Customer or required hereunder for log, access, support-related or other transmissions under this Exhibit. When Customer's license to use the Proofpoint Product ceases Proofpoint will delete all backed-up Customer configuration settings and Customer metadata from Proofpoint systems within thirty (30) days.

Compliance Gateway. 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 Compliance Gateway and ensuring that the Customer Equipment and any ancillary services are (a) compatible with Compliance Gateway and (b) comply with all configuration requirements set forth in Compliance Gateway Documentation; and (iii) complying with all laws, rules and regulations regarding the management and administration of its electronic messaging and/or social media systems, including but not limited to, obtaining any required consents and/or acknowledgements from its employees and service providers (if applicable) in managing its electronic messaging and/or social media system. Customer shall have obtained or obtain appropriate consent or authorization and be deemed to have consented to and authorized Proofpoint (and its authorized subcontractors) to retain, store and transmit any Customer Confidential Information (including, but not limited to, Configuration Settings) pursuant to the normal functioning of Compliance Gateway, including but 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; and (iii) any requests by Customer or required hereunder for log, access, support-related or other transmissions under this Exhibit. When Customer's license to use the Proofpoint Product ceases Proofpoint will delete all backed-up Customer configuration settings and Customer metadata from Proofpoint systems within thirty (30) days.

Governance. 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 Governance and ensuring that the Customer Equipment and any ancillary services are (a) compatible with Governance and (b) comply with all configuration requirements set forth in Governance Documentation; and (iii) complying with all 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 and service providers (if applicable) in managing its electronic messaging system; and (iv) as applicable, disposition of customer data after the expiry of the applicable retention period. Customer shall have obtained or obtain appropriate consent or authorization and be deemed to have consented to and authorized Proofpoint (and its authorized subcontractors) to retain, store and transmit any Customer Confidential Information (including, but not limited to, customer data) pursuant to the normal functioning of Governance, including but 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; and (iii) any requests by Customer or required hereunder for log, access, support-related or other transmissions under this Exhibit. Upon termination or expiration of Customer's license to use the Proofpoint Product, for a period of thirty (30) days after termination or expiration ("Wind Down Period") Customer may continue to access and retrieve customer

data that has been stored in the Proofpoint Product prior to termination. During the Wind Down Period, Customer may not use the Proofpoint Product to manage new or additional documents. At the end of the Wind Down Period, Proofpoint will initiate the removal of customer's data in such a manner that it cannot be restored in human readable form from any and all storage mediums (including backups), which will be completed within thirty (30) days.

SECURITY PRODUCTS SUITE

The Security Products suite includes any combination of the following: Cloud Account Defense (CAD), Cloud App Security Broker (CASB), Cloudmark Authority, Cloudmark Safe Messaging Cloud (SMC), Cloudmark Security Program, and Cloudmark Spam Reporting Service (SRS), Continuity, Data Discover, Domain Discover for Email, Email Data Loss Prevention (DLP), Email Encryption, Email Brand Defense, Email Fraud Defense, Email Protection, Emerging Threats Intelligence Query, Emerging Threats Pro Ruleset, Emerging Threats Reputation, Internal Mail Defense (IMD), Mail Routing Agent (MRA), PhishAlarm, PhishAlarm Analyzer, Secure Share, Targeted Attack Protection (TAP), TAP Isolation – Personal Browsing Defense, TAP Isolation – Personal Webmail Defense, Security Awareness Training, Threat Response, Threat Response Auto Pull, and ThreatSim and any future names or bundles by which Proofpoint identifies and makes available these Products

Cloudmark Products. Cloudmark Products include Cloudmark Authority, Cloudmark Safe Messaging Cloud (SMC), and Cloudmark Spam Reporting Service (SRS). Notwithstanding anything to the contrary in the General Terms and Conditions, the parties hereby agree that Work Product resulting from Professional Services for Cloudmark Products includes Customer configurations. Proofpoint grants to Customer a license to such Work Product (including Customer configurations) pursuant to Section 5.1 of the General Terms and Conditions. Additionally, Customer acknowledges that use of the "Cloudmark Network Feedback System" involves sending unencrypted Customer e-mail and spam samples into this system. This process is optional for the Customer and only occurs for an email message when a User chooses to click on the "This is Spam" button or the "This is NOT spam" button for a given email message. Proofpoint analyses these spam reports and unblock reports in order to increase the accuracy of the Proofpoint Product.

Continuity. Continuity is licensed on a User basis. Customer acknowledges that Continuity is only to serve as a secondary, emergency failover option in the event of failure of Customer's email service, and not to serve as a primary email archive solution or a primary failover solution. Customer is required to have a current subscription for Proofpoint email protection to use Continuity. Customer is responsible for: (i) all activities conducted under its User logins; and (ii) obtaining and maintaining any Customer Equipment and any ancillary services needed to connect to, access or otherwise use Continuity and ensuring that the Customer Equipment and any ancillary services are compatible with Continuity and comply with all configuration requirements set forth in Continuity's Documentation; and (iii) supporting and resolving any password reset issues for Continuity for Customer's Users. Customer is solely responsible for any damage or loss to a third party resulting from the Customer's own use of the Proofpoint Product in violation of: (a) applicable law; or (b) the terms and conditions of the Agreement.

Continuity Plus. Continuity Plus is licensed on a User basis Customer must: (i) enable the email journaling feature within Customer's Microsoft Exchange Server, or Microsoft Office 365 service; and (ii) ensure that the Customer's network has proper policies to allow journaling emails to be transmitted to the Proofpoint hostnames and IP addresses for Continuity Plus. This feature for emergency storage of outbound and intra-domain email is only supported for select versions of Microsoft Exchange Server and Microsoft Office 365. Customer is solely responsible for any damage or loss to a third party resulting from the Customer's own use of the Proofpoint Product in violation of: (a) applicable law; or (b) the terms and conditions of the Agreement.

Domain Discover. Customer is responsible for (i) all activities conducted under its User logins; (ii) obtaining and maintaining any necessary equipment and configurations set forth in the Documentation; and (iii) complying with all applicable laws, rules and regulations, and acquiring all necessary data subject consents. Customer is responsible for maintaining the user accounts and the security of its user names and passwords at the user level and for promptly changing or deleting any user name or password that Customer believes may have been compromised. Proofpoint reserves the right to institute password requirements (such as the length of password or the required use of numbers, symbols etc.) and to refuse registration of, or cancel passwords it deems inappropriate. The Proofpoint Products may allow Customer to interface with a variety of third party software or services (e.g., Facebook, Twitter, LinkedIn). No endorsement of any such service should be inferred as a result

of any integration with the Proofpoint Products and Proofpoint is not responsible for the data, operation or functionality of such third-party services. While Proofpoint may, in its sole discretion, customize the Proofpoint Products to interoperate with various third-party services: (a) Customer is responsible for complying with the terms and policies of each such third-party service including, without limitation, any payment obligations related thereto; and (b) Proofpoint cannot guarantee that such third-party services will continue to interoperate with the Service.

Email Protection. Email Protection is licensed on a User basis. When using Email Protection Customer is responsible for all activities conducted under its user logins. Email Protection is for use with normal business messaging traffic only, and Customer shall not use Email Protection for the machine generated message delivery of bulk or unsolicited emails or emails sent from an account not assigned to an individual. Customer is responsible for maintaining the outbound email filtering Email Protection configuration settings to block emails identified by Proofpoint as either containing a virus or having a spam score of ninety-five (95) or higher. If Proofpoint has reason to believe that Customer has modified the outbound email configuration setting, Proofpoint reserves the right to monitor and reset such settings. Customer is solely responsible for any damage or loss to a third party resulting from the Customer's own use of the Proofpoint Product in violation of: (a) applicable law; or (b) the terms and conditions of the Agreement. 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.

Mail Routing Agent. Customer is responsible for maintaining the outbound email filtering MRA configuration settings established by Proofpoint to filter and block emails identified by Proofpoint as either containing a virus or having a spam score of 95 or higher. If Proofpoint has reason to believe that Customer has modified the outbound email configuration setting, Proofpoint reserves the right to monitor and reset such settings.

PhishAlarm & PhishAlarm Analyzer. PhishAlarm & PhishAlarm Analyzer do not filter, scan, analyze or determine if any email received by any User of the PhishAlarm Software is a phishing attack. Other Proofpoint Products provide these functions. "User" means Customer's and its Affiliates' employees, agents, contractors, consultants or other individuals licensed to use the Proofpoint Product.

Security Training Modules. Security Training Modules enable Customer to send security awareness training to Users to teach Users secure behavior. On-premise versions of the Training Modules can also be provided. Training Modules are compatible with single SCO SCORM 1.2 and 2004 compliant Learning Management Systems, controlled by the Customer.

Targeted Attack Protection (TAP). TAP is licensed on a User basis. Customer is solely responsible for any damage or loss to a third party resulting from the Customer's own use of the Proofpoint Product in violation of: (a) applicable law; or (b) the terms and conditions of the Agreement.

Threat Response. Threat Response is licensed on a User basis and interoperates with certain supported: (i) third-party data sources ("*Event Source*"); and (ii) third-party security enforcement platforms (e.g. firewalls, and web proxy servers) ("*Enforcement Device*"). As between Proofpoint and Customer, Proofpoint shall have no liability whatsoever with respect to the accuracy, availability, or quality of Event Sources or Enforcement Devices. Customer may configure additional Event Sources and Enforcement Devices as needed by Customer in connection to Customer's use of Threat Response. Customer is solely responsible for any damage or loss to a third party resulting from the Customer's own use of the Proofpoint Product in violation of: (a) applicable law; or (b) the terms and conditions of the Agreement.

Threat Response Auto Pull. Threat Response Auto Pull is licensed on a User basis and may only be integrated with either Microsoft Exchange Server, Microsoft Office 365, Google Gmail or IBM Domino as an Enforcement Device and can only be used with the following data Event Sources: Proofpoint TAP, FireEye EX, Proofpoint Smart Search results, Splunk (events for email quarantine only) and JSON (events for email quarantine only). Upon written notice (via email) to Customer's Named Support Contact from Proofpoint, Customer will send a copy of its specific TRAP system configuration to Proofpoint for review. Customer is solely responsible for any damage or loss to a third party resulting from the Customer's own use of the Proofpoint Product in violation of: (a) applicable law; or (b) the terms and conditions of the Agreement.

ThreatSim. Customer may only conduct simulated phishing emails to domains owned by the Customer as set forth in the Purchase Order. Customer may include in the simulated phishing emails logos, customer names, e-mail addresses of Users and any other identifying information (“Customer Information”). Customer represents and warrants that it has the right to distribute, reproduce, publish, upload, use the Customer Information.

TAP Isolation – Personal Browsing Defense & Personal Webmail Defense. Personal Browsing Defense and Personal Webmail Defense are both licensed on a User basis. Customer will not use either TAP Isolation product to monitor any User’s internet activities and will not allow Users to transmit through or post on either TAP Isolation product infringing, defamatory, threatening or offensive material.