Proofpoint Product Terms

These Product Terms ("Exhibit") is an exhibit to the Master Subscription Agreement or other applicable license agreement, including but not limited to the Proofpoint General Terms and Conditions, ("Agreement") between each Customer and Proofpoint. In the event of conflict between the Agreement and this Exhibit the terms of this Exhibit shall govern. Capitalized terms used in this Exhibit without separate definition shall have the meaning specified in the Agreement.

1. GENERAL TERMS. Proofpoint shall make each applicable Proofpoint Product available to Customer and its Affiliates in accordance with the Agreement, Purchase Order, this Exhibit and the Documentation. Customer's right to use the Proofpoint Product is limited to the maximum number of Licenses for each module, the deployment type (Appliance, Software, or Service (SaaS)), and any other limitations specified in this Exhibit, and each Purchase Order and/or Quote.

2. PRODUCT SPECIFIC TERMS.

CASB Proxy. CASB Proxy identifies and classifies regulated or sensitive data, and monitors such data as it is uploaded, downloaded or shared in the Cloud.

Closed-Loop Email Analysis and Response (CLEAR). CLEAR integrates the functionalities of PhishAlarm and TRAP to streamline Customer's end user reporting and security response to phishing attacks.

Cloud Account Defense / Cloud Account Security Broker / CASB Protection for IaaS (add-on) / CASB OCR (add-on). Proofpoint Cloud Account Defense helps Customer detect suspicious activities around Customer's cloud accounts and identify compromised cloud accounts. Proofpoint Cloud Account Security Broker uses policies to prevent the loss of

storage, and monitor and stop unauthorized logins to Customer's Cloud accounts. CASB Protection for IaaS is subject to the DLP traffic limitation described in the quote or Order Form. CASB OCR technology for DLP extracts and analyzes text content in images to identify sensitive information. CASB OCR is subject to the image limitation described in the quote or Order Form.

Cloud Threat Response. Cloud Threat Response is a cloud-based email security solution used to respond to threats through automated and manual processes. The solution ingests threat information from multiple alert sources and integrates with the customer's mail server (Exchange, Office 365, G Suite) to retrieve and move messages.

Cloudmark Products. Cloudmark Products include Cloudmark Authority, Cloudmark Safe Messaging Cloud (SMC), and Cloudmark Spam Reporting Service (SRS). Cloudmark Products leverage intelligent threat analysis to provide email, SMS and mobile messaging security against spam and malware. Notwithstanding anything to the contrary in the Agreement, 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 the Agreement. 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 theses spam reports and unblock reports in order to increase the accuracy of the Proofpoint Product. Customer's license to Use Cloudmark Products includes the right to use the Cloudmark Products for the benefit of Customer's end user customers, pursuant to a written license agreement between Customer and each end user customer that is at least as protective of Proofpoint's rights as the terms of the Agreement and this Exhibit.

Continuity. Continuity provides temporary storage of Customer inbound and outbound email within the on-demand, Web-based email. Continuity is limited to the number of calendar days and the maximum per User data volume set forth in the Order Form or Proofpoint quote. 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.

Continuity Plus. Continuity Plus provides temporary storage of Customer inbound and outbound email within the on-demand, Web-based email. Continuity Plus is limited to the number of calendar days and the maximum per User data volume set forth in the Order Form or Proofpoint quote. 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

only supported for select versions of Microsoft Exchange Server and Microsoft Office 365.

Data Discover. Data Discover scans emails, files on network shared drives, and cloud storage services to find and track protect sensitive information (such as PII, PHI and GDPR Personal Data) so Customers can identify data risks and determine appropriate remediation.

Domain Discover. Domain Discover identifies suspicious domains that fraudulently use, impersonate or look like Customer's legitimate domains and trademarks. Customer is responsible for 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 Brand Defense (EBD). Using DMARC and threat intelligence, EBD identifies and blocks malicious emails, spoofing trusted brands and domains, before they hit consumer inboxes.

Email Data Loss Prevention (DLP). Email DLP utilizes policies to prevent the loss of Customer's sensitive or confidential data through email.

Email Encryption. Proofpoint Email Encryption provides a fully integrated message encryption and decryption solution.

Email Exfiltration Protection. Email Exfiltration Protection is a cloud-based email protection service that prevents exfiltration to unauthorized accounts, and potential loss of proprietary data and intellectual property without predefined rules or deny lists.

Email Fraud Defense (EFD). EFD blocks spear phishing emails spoofing trusted domains and evaluates the authenticity of senders to block emails from unauthenticated sources.

Email Protection. Email Protection includes functions such as spam detection functions to identify and classify spam messages; virus protection functions to detect and filter messages containing known viruses; zero-hour anti-virus functions to detect and filter messages

addresses that have displayed poor reputation. Email Protection is for use with normal external 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. If Customer is licensed for the SaaS deployment of Email Protection Customer is prohibited from deactivating the Dynamic Reputation feature. 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. If requested in writing, Proofpoint will set up the Customer's instance of the Email Protection product within Proofpoint's U.S. gateways or data centers. So long as Customer configures its MX records to point to URLs provided to Customer by Proofpoint for the instance in the United States, Customer's email will be filtered in US based data centers.

Email Threat Defense. Email Threat Defense is a cloud-based email defense service which uses machine learning to detect and prevent inbound email attacks, while providing end-users with in-moment contextual warning banners to help them decide whether an email is safe.

Emerging Threats Intelligence. ET Query, ET Pro Ruleset and ET Reputation are data feeds and may include network intrusion detection signatures, global intelligence portal, intelligence APIs, and reputation lists to enable Customer to detect and investigate network based threats in or against its environment.

Endpoint Data Loss Prevention (Endpoint DLP). Endpoint Data Loss Prevention is hosted on the Information and Cloud Security Platform and deploys software (an Agent) onto Customer owned or controlled desktops and servers on supported platforms. These Agents capture metadata recorded from the activities of licensed Users and store this data in Proofpoint's Endpoint DLP service. A licensed User of Endpoint DLP is a unique individual with a unique access credential being monitored by Customer, regardless of whether the Agents are deployed on physical or virtual systems. If an individual has more than one access credential, then a separate User license for each of that individual's unique access credentials must be purchased. A licensed User of Endpoint DLP may also be a unique Server (physical or virtual) with a unique access credential being monitored by the Customer. Endpoint DLP Metadata Feed allows Customer to export its captured User metadata. Endpoint DLP Metadata Feed is subject to a maximum monthly export amount as described in the Proofpoint quote or Order Form. Excessive ingestion of activities may lead to local caching on an Agent or throttling of transmission to the cloud.

Insider Threat Management (ITM). ITM SaaS is hosted on the Information and Cloud Security Platform and deploys software (an Agent) onto Customer managed desktops,

and store this data in Proofpoint's Information and Cloud Security Platform. ITM SaaS Metadata Feed allows Customer to export its captured User metadata. A licensed User of ITM SaaS is a unique individual with a unique access credential being monitored by Customer, regardless of whether the Agents are deployed on physical or virtual systems. If an individual has more than one access credential, then a separate User license for each of that individual's unique access credentials must be purchased. A licensed User of ITM SaaS may also be a unique Server (physical or virtual) with a unique access credential being monitored by the Customer. ITM SaaS Metadata Capture, and ITM SaaS Metadata Capture with Visual Capture, are subject to the activity ingestion rate(s) and retention time tiers described in the Proofpoint quote or Order Form. Additionally, both the ITM SaaS Metadata Capture with Visual Capture and ITM Additional Visual Capture are further subject to the aggregate data storage limit(s) described in the Proofpoint quote or Order Form. ITM SaaS Metadata Feed is subject to a maximum monthly export amount as described in the Proofpoint quote or Order Form. Excessive ingestion of User activities may lead to local caching on an Agent or throttling of transmission to the cloud. Proofpoint reserves the right to require that the Customer pay additional fees when any ingestion, storage, and/or export limit is exceeded. ITM On-Prem is deployed on customer-provided infrastructure (bare-metal, VMs or customer-managed cloud) and Proofpoint does not have access to the customer's deployment. Proofpoint licenses the On-Prem version based on the number of endpoints the Agent is installed on.

Intelligent Classification and Protection. Proofpoint Intelligent Classification and Protection AI engine automatically locates and identifies sensitive and business-critical data to enhance existing data protection solutions such as labeling, encryption, access control, data loss prevention, CASB and suggests protection rules and/or policies to the Customer.

Internal Mail Defense (IMD). IMD leverages Email Protection and TAP features to protect Customer's internal email communications against spam and malicious content.

Misdirected Email Protection. Misdirected Email Protection is a cloud-based email protection service that prevents accidental data loss from misdirected emails and misattached files, preventing sensitive information being inadvertently sent to an unintended recipient.

Nexus People Risk Explorer. Proofpoint Nexus People Risk Explorer leverages people centric security data from Proofpoint's Targeted Attack Protection, Security Awareness Training, Cloud Account Defense and Cloud Account Security Broker to provide insights into the types, severity and frequency of threats targeted at Customer and its employees.

PhishAlarm & PhishAlarm Analyzer. PhishAlarm allows end users to report phishing emails and other suspicious messages. PhishAlarm Analyzer delivers highly responsive identification of phishing attacks in real time. Emails reported via PhishAlarm & PhishAlarm

Proofpoint Archive. Proofpoint Archive is a cloud-based archiving solution designed for legal discovery, regulatory compliance and data access for Customer's end users, and it provides a central, searchable repository that supports a wide range of content types. 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") subject to payment of a pro-rata fee 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.

Proofpoint Automate. Proofpoint Automate uses machine learning to evaluate supported archived messages (such as email, social media, collaboration platforms, and mobile messages) flagged for Customer's review by Proofpoint Supervision. This helps Customer improve its regulatory supervision decision making and automate key parts of Customer's supervision workflow. Customer may configure its own data models in the supervision UI. As between Proofpoint and Customer, Proofpoint shall have no liability whatsoever with respect to such data models. If Proofpoint has reason to believe that a data model is malfunctioning, Proofpoint reserves the right to disable the data model.

Proofpoint Capture. Proofpoint Capture captures content from supported messaging and Cloud storage platforms and delivers it compliance services such as e-discovery, archive and supervision.

Proofpoint Discover. Proofpoint Discover is an add-on capability to Proofpoint's Archive service with case management features, advanced visualizations and Technology Assisted Review for classifying electronically stored information (ESI) for legal discovery.

Proofpoint Isolation. Proofpoint Isolation products establish an isolated remote web browser or web email environment to protect the Customer from potential threats when Users connect to the Internet or web-based email accounts on Customer owned or controller devices. Customer will not allow Users to transmit through (or post on) Isolation any infringing, defamatory, threatening or offensive material.

Proofpoint Patrol. Proofpoint Patrol allows Customers to monitor, remediate and generate compliance reports about their end users' activities on Customer controlled social media accounts. Proofpoint Patrol for Text is the limited version of Proofpoint Patrol exclusively for third-party text messaging applications. Proofpoint Patrol uses YouTube API Services, please see Google's Privacy Policy at http://www.google.com/policies/privacy.

threats such as Business Email Compromise (BEC), phishing, and malware; message quarantines for analysis and disposition of suspicious content; and functions to quarantine delivered messages with threats. Proofpoint PX is for use with normal external business messaging traffic flowing through a Microsoft O365 application instance only. Customer shall not use Proofpoint PX for the machine generated message delivery of bulk or unsolicited emails or emails sent from an account not assigned to an individual.

Proofpoint Shadow. Proofpoint Shadow detects attackers who have already gained access to Customer's network and prevents further access against Customer's critical assets. Shadow deploys believable, automatically customized, assets that mimic the data, credentials, and connections that attackers seek. Shadow triggers incidents and collects real-time forensics from compromised Customer endpoints to assist in triage and risk response.

Proofpoint Spotlight. Proofpoint Spotlight is an identity threat detection and response (ITDR) solution that automatically discovers, prioritizes, and remediates identity vulnerabilities through Customer's corporate network. Spotlight detects directory structure misconfigurations in Active Directory and Azure AD, searches for accounts unmanaged by PAM, and detects and eliminates exposed credentials on Customer's endpoint devices.

Proofpoint Supervision. Proofpoint Supervision is a cloud-based solution that helps Customer identify, review, address and maintain audit trails from the Customer's regulatory data archive, including all incoming, outgoing and internal correspondence captured by Customer's archive.

Proofpoint Track. Proofpoint Track acts as a central hub to filter and route message content to Customer's archive, supervision and analytic systems.

Secure Access. Proofpoint Secure Access is a people-centric, zero- trust alternative to VPN. It secures remote access to any enterprise application, regardless of location. Secure Access provides Users microsegmented secure access to hundreds of cloud instances. Customers can automate cloud-to-cloud connectivity and quickly deploy access from user devices to apps in both on-premises data centers and public clouds.

Secure Email Relay. Secure Email Relay (SER) is a hosted, multi-tenant solution that puts Customer in control of applications that send email using Customer's owned or controlled domains. It adds a layer of security to each application and distributes the email to the Internet in a DMARC-compliant fashion after Proofpoint AS/AV checks are performed. SER may only be used for delivery of emails that comply with applicable bulk or unsolicited message laws. The number of messages processed through SER is limited to the annual amount identified in the Proofpoint quote or Order Form and Proofpoint reserves the right to require that the Customer pay additional fees when such limit is exceeded. Additionally, any

SecureShare. SecureShare is a secure method for the sharing of files and temporary storage of such files, but is not a back-up service. SecureShare is limited to the number of Users, the maximum storage capacity and maximum retention period set forth in the Order Form or Proofpoint quote.

Security Training Modules. Security Training Modules enable Customer to send security awareness training to Users to teach Users secure behavior. Customer may include additional content in the Training Modules, and hereby represents and warrants that it has the right to distribute, reproduce, publish, upload and use any such additional content. If customized content is added to Customer's instance of Proofpoint's Security Training Modules, then, with the exception of Customer's logos and other property provided by Customer to Proofpoint for such customization, Proofpoint retains all ownership rights in and to its products, services, all work product resulting from the customizations, as well as all modifications and derivative works thereto. All such custom content must be deleted by the Customer at the end of the Customer's Security Training Modules subscription.

Social Discover. Social Discover scans the Internet to identify accounts using Customer's brands on social media networks, including unauthorized accounts.

Social Patrol. Social Patrol automatically scans Customer's social media account posts and comments for high-risk content such as malware, phishing links, hate speech, pornography and piracy.

Supplier Threat Protection. Designed to identify customer's suspected supplier and/or known third-party compromised email accounts. The customer is made aware of the potential suspicious account through the TAP Dashboard, allowing a customer to proactively investigate and/or take action to protect their environment from a supplier and/or known third-party compromised account.

TAP Account Takeover (TAP ATO). Optional addon to TAP. Designed to help protect end-users from email account takeover attacks. Customers are made aware of suspected account takeovers through the TAP Dashboard, allowing security teams to investigate and remediate mail threats and prevent further mailbox abuse in the cloud.

Targeted Attack Protection (TAP). TAP identifies and protects against malicious URLs and malicious attachments in emails using a dynamic malware analysis engine.

Threat Response. Threat Response is an incident management platform that leverages event source alerts, automation, reporting, threat intelligence and IOC agents to enable Customer to manage cybersecurity threats. Threat Response interoperates with certain supported: (i) third-party data sources ("*Event Source*"); (ii) quality and data enrichment sources ("Enrichment Sources"), and (iii) third-party security enforcement platforms (e.g. firewalls, and web proxy servers) ("*Enforcement Device*"). As between Proofpoint and

Customer may configure additional Event Sources and Enforcement Devices as needed by Customer in connection to Customer's use of Threat Response.

Threat Response Auto Pull (TRAP). TRAP is an incident management platform that includes automation to analyze and remove unwanted emails. Threat Response Auto Pull may only be integrated with Event Sources, (i) Enrichment Sources, or (ii) 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, Abuse Mailbox Monitor, 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.

ThreatSim. ThreatSim enables quick and easy sending of phishing simulation assessments and results tracking. Customer may only conduct simulated phishing emails to domains owned or controlled 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, and use the Customer Information.

Virtual TakeDown. Proofpoint Virtual TakeDown is an optional add-on to Domain Discover. Through it Customer can submit malicious and criminal domains, including domains engaged in phishing, propagation of malicious content, or engaged in criminal activity, to leading blocklists used by a wide array of ISPs, devices, web services and security products.

Web Security / Web Security OCR (add-on). Proofpoint Web Security protects Users against advanced threats when they browse the web. It supports a Customer's distributed workforce by ensuring secure internet access for all workers, whether they're inside or outside of Customer's perimeter. It applies monitoring and visibility, advanced threat protection and data-loss prevention (DLP) policies in a people-centric approach to security. Web Security does not support routing streaming media through the proxy. Web Security OCR technology automatically extracts and analyzes text content in images to identify sensitive information and is subject to the image limitation described in the quote or Order Form.

Last updated March 14, 2024.

Overview
Why Proofpoint
Careers
Leadership Team
News Center
Nexus Platform
Privacy and Trust

Threat Hub
Cybersecurity Awareness Hub
Ransomware Hub
Threat Glossary
Threat Blog

Products

Email Security & Protection
Advanced Threat Protection
Security Awareness Training
Cloud Security
Archive & Compliance
Information Protection
Product Bundles

Resources

White Papers
Webinars
Data Sheets
Events
Customer Stories
Blog
Free Trial

Connect

+1-408-517-4710

Contact Us
Office Locations
Request a Demo

Support

Support Login
Support Services
IP Address Blocked?

Terms and conditions

Privacy Policy