Symantec™ Data Loss Prevention Cloud

Data Loss Prevention Cloud Detection Service, Data Loss Prevention Cloud Service for Email Standalone, and Data Loss Prevention Cloud Service for Email with Email Safeguard

Service Description

August 2019

This Service Description describes Symantec's Data Loss Prevention Cloud Detection Service, Data Loss Prevention Cloud Service for Email Standalone, and Data Loss Prevention Cloud Service for Email with Email Safeguard (individually and collectively, the "Service"). All capitalized terms in this description have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section.

This Service Description, with any attachments included by reference, is part of and incorporated into Customer's manually or digitally-signed agreement with Symantec which governs the use of the Service, or if no such signed agreement exists, the Online Services Terms and Conditions published with the Service Description at www.symantec.com/about/legal/repository (hereinafter referred to as the "Agreement").

Table of Contents

1: Technical/Business Functionality and Capabilities

Service Overview

Symantec™ Data Loss Prevention Cloud Detection Service, Data Loss Prevention Cloud Service for Email Standalone, and Data Loss Prevention Cloud Service for Email with Email Safeguard (individually and collectively, the "Service") are hosted services that provide content inspection capabilities through the use of advanced content aware detection technologies. Application of user configured Data Loss Prevention ("DLP") policies to content submitted to the Service enables the identification of sensitive information contained within the submitted content.

Other Symantec or third party services integrating with the Service (each, an "Integrating Service") can send content for scanning of sensitive data to the Service. In return, the Integrating Service receives DLP policy violations and recommended remediation actions from the Service.

- **DLP Cloud Detection Service** with a Symantec certified partner application (available under a separate license from Symantec) or with a Custom Integration (defined below). Customers may license a REST API of the DLP Cloud Detection Service from Symantec for purposes of adding DLP functionality to Customer's internally used application or service ("Custom Integration"), which DLP functionality can be invoked from such internally used application or service to perform DLP detection on data sent to the Service. Please contact your Symantec representative for more information about licensing Service's REST API for development of a Custom Integration.

- **DLP Cloud Detection Service with Symantec CloudSOC™ CASB service**: The Service is used in conjunction with the Symantec CloudSOC™ CASB service to add Symantec DLP detection to cloud application data monitored by the CASB service. (Note: A separate subscription to CloudSOC™ CASB service is required. The Service Description for the Symantec CloudSOC™ CASB service is located at https://www.symantec.com/about/legal/repository.)

- **DLP Cloud Detection Service with Symantec Web Security Service**: The Service is used in conjunction with the Symantec Web Security Service (WSS) cloud-proxy to add Symantec DLP detection to outbound web traffic monitoring by the cloud-proxy. (Note: A separate subscription to WSS is required. The Service Description for the Symantec WSS service is located at https://www.symantec.com/about/legal/repository.)

- **DLP Cloud Service for Email Standalone**: The Service provides Symantec DLP detection to outbound email traffic by any of the following supported third-party enterprise email service providers: Microsoft Office 365 Exchange Online, Microsoft Exchange Server, or Google G Suite Gmail.

  Note: A separate subscription to Email Security.cloud may be required, depending on implementation. For more details, please refer to the *Symantec Data Loss Prevention Implementation Guide* at https://www.symantec.com/docs/doc9008.html. The Service Description for Symantec Email Security.cloud service is located at https://www.symantec.com/about/legal/repository.)

- **DLP Cloud Service for Email with Email Safeguard:** The Service is used in conjunction with the Symantec Email Safeguard service to add Symantec DLP detection to email scanned by the Email Safeguard service. (Note: A separate subscription to Email Safeguard is required. The Service Description for Email Safeguard is located at https://www.symantec.com/about/legal/repository, under Email Security.cloud.)

Service Features

- **"Enforce Server"** is an administration console that is a centralized, web-based interface for deploying detection servers, cloud services, authoring policies, remediating incidents, and managing the system. Customer can configure and manage the Service, access reports, and view data and statistics, through the Enforce Server administration console.
- The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for hardware availability, service capacity and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.
- The Service is intended to enable Customer to implement a valid and enforceable computer use policy, or its equivalent.

Service Level Agreement

- Symantec provides the applicable service level agreement ("SLA") for the Service as specified in Exhibit-A. These SLAs do not apply to any Integrating Service.

Supported Platforms and Technical Requirements

- Supported platforms for the Service are defined at: https://support.symantec.com/en_US/article.DOC9414.html

Service Enabling Software

- This Service includes Enabling Software (including the Symantec Enforce Server administration console), which should be used only in connection with Customer's use of the Service during the Subscription Term. Use of the Enabling Software is subject to the license agreement accompanying such software ("Software License Agreement"). If no Software License Agreement accompanies the software, it is governed by the terms and conditions located at http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf. In the event of conflict, the terms of this Service Description prevail over any such Software License Agreement. Customer must remove Enabling Software upon expiration or termination of the Service.

2: Customer Responsibilities

Symantec can only perform the Service if Customer provides required information or performs required actions, otherwise Symantec's performance of the Service may be delayed, impaired or prevented, and Customer may lose eligibility for any Service Level Agreement.

- Symantec can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, Symantec's performance of the Service may be delayed, impaired or prevented, and/or eligibility for Service Level Agreement benefits may be voided, as noted below.
  - Service Activation: Customer must follow required steps to activate the Service.
  - On-premise installation and use of administration console: Customer must install and use an on-premise version of the Enforce Server administration console.
  - Customer Configurations: Customer must configure features of the Service through the Enforce Server administration console.
  - Connecting Applications: If the service is used by Customer with their Integrating Service, the Integrating Service must comply with the API specification for the REST API when calling the Service.
- Setup Enablement: Customer must provide information required for Symantec to begin providing the Service.
- Customers developing Custom Integrations must specify the name of the internally used application or service to be integrated with the Service using a Custom Integration request form provided by Symantec. Symantec reserves the right in its sole discretion to decline any proposed Custom Integration with the Service, and shall notify Customer promptly upon such determination
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Symantec in delivery of the Service.
- Renewal Credentials: If applicable, Customer must apply renewal credential(s) provided in the applicable Order Confirmation within its account administration, to continue to receive the Service, or to maintain account information and Customer data which is available during the Subscription Term.
- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the Console if applicable, or default settings will apply. In some cases, default settings do not exist, and no Service will be provided until Customer chooses a setting. Configuration and use of the Service(s) are entirely in Customer's control, therefore, Symantec is not responsible for Customer's use of the Service. Should a Service be suspended or terminated for any reason, Customer configurations will be lost and cannot be saved.
- The foregoing restrictions apply whether Customer has purchased a Sandbox subscription in addition to a Service subscription, or a Sandbox-only subscription for testing.
- The following conditions apply to **DLP Cloud Service for Email** *(Standalone or combined with Email Safeguard)*:

- Customer may choose to route emails scanned by the Service to Symantec Email Security.cloud or Microsoft Office 365 Exchange Online for delivery to recipients. Customer that chooses to route emails scanned by the Service to Symantec Email Security.cloud must have a concurrent subscription to the Symantec Email Security.cloud Safeguard service in order for Symantec to deliver the Service. Customer that chooses to route emails scanned by the Service to Microsoft Office 365 Exchange Online for delivery to recipients must have a concurrent subscription to the Microsoft Office 365 Exchange Online, maintain a valid certificate provided by Symantec for the Service, and designate the Symantec-provided certificate as trusted by Customer's Microsoft Office 365 Exchange Online service. Customer, and not Symantec, is solely responsible for any failure of the Service to function due to lack of valid certificate unless Symantec fails to provide such certificate.
- Default maximum email size = thirty megabytes (30MB). Customer can specify any maximum email size up to fifty megabytes (50MB). Any emails that are received by the Service that exceed the specified limit will be scanned for the first fifty megabytes (50MB) of a received email against detection policy configured by Customer. If the first fifty megabytes (50MB) of a received email violates the policy, automated remediation actions will be applied to the entire email (including portions of the email beyond the 50MB threshold). Otherwise, if the first 50MB of a received email does not violate any policy, such email will be passed along to either Symantec Email Security.cloud or Microsoft O365 Exchange Online without application of any automated remediation action based on routing configurations chosen by Customer.
- Customers must route their outbound email through the Service using the routing information provided by Symantec.
- Customer must ensure that all domains (including sub-domains) requiring the Service are provisioned. Customer accepts that Service features may not function correctly, and email delivery may be unavailable for domains that are not provisioned.
- In the event that continued provision of the Service to Customer would compromise the security of the Service, including, but not limited to, hacking attempts, denial of Service attacks, mail bombs or other malicious activities either directed at or originating from Customer's domains, Customer agrees that Symantec may temporarily suspend Service to Customer. In such an event, Symantec will promptly inform Customer and will work with Customer to resolve such issues. Symantec will reinstate the Service upon removal of the security threat.
- Should the Service be suspended for any reason whatsoever, the Service will not be applied to Customer's emails, and emails will not be routed through Symantec's Infrastructure. Customer is responsible for redirecting their email during suspension and confirming that all configurations are accurate if the Service is reinstated.
- Should a Service be terminated for any reason whatsoever, Customer's account will be deleted, and Customer will not have access to the Service.
- Customer will not allow its systems to: (i) act as an Open Relay or Open Proxy or (ii) send Spam. Symantec reserves the right at any time to review Customer's compliance with this restriction. For the avoidance of doubt, any breach of this restriction will constitute a material breach of the Agreement and Symantec reserves the right to suspend all or part of the Service immediately and until the breach is remedied or terminate the Agreement with respect to the affected Service.
- If at any time (i) Customer's email systems are blacklisted, or (ii) Customer causes the Symantec systems to become blacklisted due to the sending of Spam, or (iii) Customer fails to meet any of the obligations set out in this Service Description, Symantec shall inform Customer and reserves the right at its sole discretion to immediately withhold provision of, suspend or terminate all or part of the Service.
- The Service is only available to a Customer who has its own email domain name and has the ability to configure the MX records and/or DNS for that domain name.
- Customer must specify the mail server IP address(es) or hostname(s) for the delivery of inbound emails to their organization.
- Customer agrees to provide and maintain a list of valid email addresses (the "Validation List") to receive the Service. It is Customer's responsibility to verify the Validation List prior to the Service being made available and throughout the Term. Emails with email addresses not on the Validation List, or incorrectly entered, will be rejected by the Service. If Customer is unable to provide such Validation List and requests, Symantec will review each such request on a case-by-case basis and reserves the right to decline requests, in Symantec's sole and absolute discretion.

3: Entitlement and Subscription Information

Charge Metrics

The Service is available under one of the following Meters as specified in the Order Confirmation:

"**User**" means an individual person (i) authorized to use the Service, (ii) benefitting from use of the Service, (iii) on behalf of whom Customer derives benefit from the use of the Service, or (iv) that actually uses any portion of the Service. Each subscription purchased for the Service may only be used by a single User in conjunction with a single Cloud Application. As used herein and for purposes of determining the applicable User count for the Service, "Cloud Application" means the target application or hosted service scanned by an Integrating Service. Where Symantec™ CloudSOC™ CASB service is the Integrating Service, each Securlet for a target application constitutes one Cloud Application and all Gatelets taken together constitute one Cloud Application. Where Symantec Web Security Service (WSS) is the Integrating Service, WSS constitutes one Cloud Application that requires a DLP Cloud Detection Service subscription for each User licensed to WSS otherwise as a stand-alone service. In the case of AWS S3 as the Integrating Service, AWS S3 constitutes one Cloud Application whereby Customer must purchase a maximum User count of Service subscriptions (i.e., a Service subscription for each individual person within Customer's organization) for such Cloud Application.

4: Customer Assistance and Technical Support

Customer Assistance

Symantec will provide the following assistance as part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service;
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions.

Technical Support

If Symantec is providing Technical Support to Customer, Technical Support is included as part of the Service as specified below. If Technical Support is being provided by a reseller, this section does not apply.

- Support is available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of the Service features and to resolve reported problems with the Service. Support for Services will be performed in accordance with the published terms and conditions and technical support policies published at https://support.symantec.com/en_US/article.TECH236428.html.
- Once a severity level is assigned to a Customer submission for Support, Symantec will make every reasonable effort to respond per the response targets defined in the table below. Faults originating from Customer's actions or requiring the actions of other service providers are beyond the control of Symantec and as such are specifically excluded from this Support commitment.

Problem Severity	**Support (24x7) Response Targets***
Severity 1: A problem has occurred where no workaround is immediately available in one of the following situations: (i) Customer's production server or other mission critical system is down or has had a substantial loss of service; or (ii) a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption.	Within 30 minutes
Severity 2: A problem has occurred where a major functionality is severely impaired. Customer's operations can continue in a restricted fashion, however long-term productivity might be adversely affected.	Within 2 hours
Severity 3: A problem has occurred with a limited adverse effect on Customer's business operations.	By same time next business day**

Severity 4: A problem has occurred where Customer's business operations have not been adversely affected.	Within the next business day; Symantec further recommends that Customer submit Customer's suggestion for new features or enhancements to Symantec's forums

The above Support Response Targets are attainable during normal service operations and do not apply during Maintenance to the Service and/or supporting infrastructure as described in the Maintenance section below.

** Target response times pertain to the time to respond to the request, and not resolution time (the time it takes to close the request)*.

*** A "business day" means standard regional business hours and days of the week in Customer's local time zone, excluding weekends and local public holidays. In most cases, "business hours" mean 9:00 a.m. to 5:00 p.m. in Customer's local time zone*.

Maintenance to the Service and/or supporting Service Infrastructure

Symantec must perform maintenance from time to time. For information on Service status, planned maintenance and known issues, visit https://status.symantec.com/ and subscribe to Symantec Status via email, SMS, or Twitter to receive the latest updates. The following applies to such maintenance:

- **Planned Maintenance:** Planned Maintenance means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, Symantec will provide seven (7) calendar days' notification posted on Symantec Status.
- **Unplanned Maintenance**: Unplanned Maintenance means scheduled maintenance periods that do not allow for seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. Symantec will provide a minimum of one (1) calendar day notification posted on Symantec Status. During Unplanned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. At times Symantec will perform Emergency Maintenance. Emergency Maintenance is defined as maintenance that must be implemented as quickly as possible to resolve or prevent a major incident. Notification of Emergency Maintenance will be provided as soon as practicable.
- **Note:** For Management Console Maintenance, Symantec will provide fourteen (14) calendar days' notification posted on Symantec Status. Symantec may perform minor updates or routine maintenance to the Management Console with no prior notification as these activities do not result in Service disruption.

5: Additional Terms

Any templates supplied by Symantec are for use solely as a guide to enable Customer to create its own customized policies and other templates.

6: Definitions

"**Administrator**" means Customer's designated personnel to manage the Service on behalf of Customer.

"**Service Credit**" means the number of days that are added to Customer's current Subscription Term.

"**Service Infrastructure**" means any Symantec or licensor technology and intellectual property used to provide the Services.

"**Symantec Online Services Terms and Conditions**" means the terms and conditions located at or accessed through https://www.symantec.com/about/legal/repository.

Exhibit-A

Service Level Agreement

1.0 GENERAL

These Service Level Agreements ("SLA(s)") apply to the Online Service that is the subject matter of this Service Description only. If Symantec does not achieve these SLA(s), then Customer may be eligible to receive a Service Credit. Service Credits are Customer's sole and exclusive remedy and are Symantec's sole and exclusive liability for breach of the SLA.

2.0 SERVICE LEVEL AGREEMENT(S)

a. **Availability.** Availability is the amount of time that the Service is operational in minutes, expressed as a percentage per calendar month, excluding Excused Outages. Availability SLAs may exist for i) Inline (Data Plane) Service, and ii) Non-Inline (Control Plane) Service, separately:

- **Inline Service Availability** means access to the core features of the Service that impact the data in transit to and from Customer to the Internet. *Examples of Inline features of each Service include:*
  - *DLP Cloud Detection Service with CloudSOC (CASB) (if using Gatelet), and DLP Cloud Detection Service with WSS:*
    - *Inspect content;*
    - *Enforce sensitive data policies;*
    - *Quarantine files;*
    - *Apply identity-based encryption and digital rights policies.*
  - *DLP Cloud Service for Email:*
    - *Message blocking and/or modification;*
    - *Enforce sensitive data policies;*
    - *Quarantine files;*
    - *Apply identity-based encryption and digital rights policies.*

Inline Service Availability	**≥99.9%**

- **Non-inline Service Availability** is access to the controls that govern the features of the Service that do not impact data in transit to and from the end-user to the Internet (e.g., reporting tools used by the Administrator). Examples of Non-Inline features for each Service include*:*
  - *DLP Cloud Detection Service and DLP Cloud Detection Service with CloudSOC (CASB) (if using Securlet):*
    - *Setting policies;*
    - *Reporting;*
    - *Incident remediation;*
    - *System management;*
    - *Remote API calls to scan content.*

Non-Inline Service Availability	**≥99.5%**

3.0 AVAILABILITY CALCULATION

Availability is calculated as a percentage of 100% total minutes per calendar month as follows:

$$\frac{\underline{\text{Total Minutes in Calendar Month – Excused Outages – Non-Excused Outages*}}}{\text{Total – Excused Outages}} \quad \text{X} \quad 100 \quad > \quad \text{Availability Target}$$

**Non-Excused Outages = Minutes of Service disruption that are not an Excused Outage*

Note: The availability calculation is based on the entire calendar month regardless of the Service start date.

4.0 SERVICE CREDIT

If a claim is made and validated, a Service Credit will be applied to Customer's account.

Symantec will provide a Service Credit equal to two (2) days of additional service for each 1 hour or part thereof (aggregated) that the service is not available in a single 24-hour period, subject to a maximum of seven (7) calendar days for all incidents occurring during that 24 hour period. A Customer may only receive up to twenty-eight (28) days maximum, for up to four (4) Service Credits, over twelve (12) months. The maximum is a total for all claims made in that twelve (12) month period.

Service Credits:

- May not be transferred or applied to any other Symantec Online Service, even if within the same account.
- Are the only remedy available, even if Customer is not renewing for a subsequent term. A Service Credit is added to the end of Customer's current Subscription Term.
- May not be a financial refund or credit of any kind.
- Do not apply to failure of other service level SLAs if such failure relates to non-availability of the Service. In such cases Customer may only submit a claim for the Availability SLA.

5.0 CLAIMS PROCESS

Customer must submit the claim in writing via email to Symantec Customer Support at ServiceCredit_Request@symantec.com. Each claim must be submitted within ten (10) days of the end of the calendar month in which the alleged missed SLA occurred for Symantec to review the claim. Each claim must include the following information:

(i) The words "Service Credit Request" in the subject line.
(ii) The dates and time periods for each instance of claimed outage or other missed SLA, as applicable, during the relevant month.
(iii) An explanation of the claim made under this Service Description, including any relevant calculations.

All claims will be verified against Symantec's system records. Should any claim be disputed, Symantec will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide a record of service availability for the time period in question to Customer.

6.0 EXCUSED OUTAGES AND EXCLUSIONS TO CLAIMS

The following are minutes of downtime that are defined as Excused Outages:

- Planned Maintenance and Unplanned Maintenance as defined in the Service Description.
- Force Majeure as defined in the Agreement.
- Any downtime that results from any of the below listed exclusions to a claim.

If any of the following exclusions apply, a claim will not be accepted:

- Any Service provided on a provisional basis, including but not limited to: trialware, evaluation, Proof of Concept, Not for Resale, pre-release, beta versions.
- Customer has not paid for the Service.
- Third party, non-Symantec branded products or services resold with the Service.

- Hardware, software or other data center equipment or services not in the control of Symantec or within the scope of the Service.
- Any item that is not a Service Component that is provided for use with the Service.
- Technical support provided with the service.
- Failure of Customer to correctly configure the Service in accordance with this Service Description.
- Hardware or software configuration changes made by the Customer without the prior written consent of Symantec.
- Unavailability of a specific web page or a third party's cloud application(s).
- Individual data center outage.
- Unavailability of one or more specific features, functions, or equipment hosting locations within the service, while other key features remain available.
- Failure of Customer's internet access connections.
- Suspension and termination of Customer's right to use the Service.
- Alterations or modifications to the Service, unless altered or modified by Symantec (or at the direction of or as approved by Symantec
- Defects in the Service due to abuse or use other than in accordance with Symantec's published Documentation unless caused by Symantec or its agents.
- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.

END OF EXHIBIT A