Symantec™ Data Loss Prevention Cloud Service for Email with Email Safeguard with Cloud Console

Service Description

February 2017

TABLE OF CONTENTS

A. SERVICE OVERVIEW

The Symantec Data Loss Prevention Cloud Service for Email with Email Safeguard with Cloud Console (the "Service") is a hosted service that:

- Protects sensitive data loss through email by applying data loss prevention policies
- Protects organizations from malware, phishing, spam and other email-borne threats

The Service provides data protection features to help control sensitive information sent outbound by email and offers advanced encryption options and advanced threat protection as choices of add-ons.

This Service Description, with any attachments included by reference, is part of (i) any signed agreement between Symantec and Customer that is intended to govern this Service Description; or (ii) if no such signed agreement exists, the Symantec Online Services Terms and Conditions or the Symantec Hosted Services Terms, as applicable to Customer's use of the Service (each, an "Agreement"). Capitalized terms shall have the meaning set forth in the Definitions section set forth below or the agreement which incorporates this Service Description.

B. TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

The Service is intended to enable Customer to implement a valid and enforceable computer use policy, or its equivalent. The Service is managed on a twenty-four (24) hour/day by seven (7) day/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.

Service Features

The Service is comprised of the following features:

- **DLP Cloud Detection** provides:
  - Content detection including Described Content Matching with support for keyword, Data Identifier, and regular expression matching, providing highly accurate detection of sensitive data in emails sent from an organization to external recipients.
  - File type, size, and count detection for controlling file attachments in emails sent from an organization to external recipients.
  - Email contextual controls based on email sender, recipient, domain, or header information.
  - Automated remediation including email blocking, modification, and notification.
  - Violation generation with Violation details that include contextual details, sensitive content matches, policy rule violations, and applied remediation actions.
- **DLP Cloud Console** provides:
  - A hosted management console providing DLP policy management, Violation investigation and remediation, report generation, and dashboard functionality. Customer can access the DLP Cloud Console by using a secure, password-protected login.
  - Using the DLP Cloud Console, the policies for the DLP Cloud Detection Service can be created and modified. These policies are then applied to Email inspected by the DLP Cloud Detection Service.
  - Violations generated by the DLP Cloud Detection Service as a result of a policy violation may be viewed in the DLP Cloud Console.
  - Integration with Customer premises directory services is provided by the Directory Synchronization Tool. The Directory Synchronization Tool must be installed on a server residing in Customer's premises.
  - Sample policy templates and in-built Data Identifiers may be supplied by Symantec. Please note that some policy templates may contain words which may be considered offensive. Symantec reserves the right to periodically update policy templates and in-built Data Identifiers to improve detection coverage and accuracy.
  - Customer may configure the Service to send configured Email recipients an automatic notification that is triggered when an Email violates the DLP policy. This action is configurable and such notifications can be created, deleted and customized through the DLP Cloud Console.
- **Email Security.cloud with Email Safeguard ("Email Security")**provides:
  - Email antimalware: Malware protection including phishing and targeted attack protection with real-time link following
  - Email antispam: Spam and bulk mail protection
  - Email data protection: Customizable content filtering policy controls

- Email image control: Offensive image detection
- Outbound filtering
- Enforced TLS encryption
- Opportunistic TLS encryption
- User and groups LDAP synchronization tool
- Message tracing
- Reporting dashboard
- Summary (PDF) and detailed (CSV) reporting
- End-user spam quarantine portal and notifications
- Disclaimer management
- Policy-based encryption essentials
- Optional add-on: Advanced Threat Protection Email
- Optional add-on: Policy-Based Encryption Advanced
- Customer administrations can access the Email Security management console by using a secure password-protected login. The management console provides the ability for Customer to configure and manage Email Security, access reports, and view data and statistics when available as part of Email Security.
- Reporting for Email Security is available through the management console. Reporting may include activity logs and/or statistics. Using the management console, Customer may choose to generate reports, which can be configured to be sent by email on a scheduled basis or downloaded from the management console.
- Suggested word lists and template rules or policies may be supplied by Symantec. Please note that such lists may contain words which may be considered offensive.

Additional information on individual Email Security features is available in the online help at http://help.symanteccloud.com/.

Supported Platforms and Technical Requirements

Supported platforms and technical requirements are defined at: (1) http://www.symantec.com/docs/INFO4144 for DLP Detection and (2) http://help.symanteccloud.com/ for Email Security.

Hosted Service Software Components

The Service includes the following software Service Components available upon activation of DLP Cloud Detection, DLP Cloud Console and Email Security:

- The DLP Cloud Console provides a Directory Synchronization Tool that synchronizes users and groups within a directory residing on the Customer's premise to the DLP Cloud Console for use in DLP Cloud Detection policies

- Email Security includes the software Services Components available in the management console which may be accessed upon payment of any applicable fee.

Customer Use and Responsibilities

Customer may use the Service only in accordance with the use Meter or model under which Customer has obtained use of the Service: (i) as indicated in the applicable Subscription Instrument or Order Confirmation; and (ii) as defined in this Service Description or the Agreement.

Symantec can only perform the Service if Customer provides required information and performs required actions. If Customer does not provide or 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 DLP Cloud Detection, DLP Cloud Console, and Email Security.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec.
- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the DLP Cloud Console, Email Security management console, as well as configure its mail server to appropriately route outbound email through the Service 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 are entirely in Customer's control.
- Customer must use the DLP Cloud Console as the management console for DLP Cloud Detection, including all policy management and violation investigation and remediation.
- Customer must install the Directory Synchronization Tool on a server in Customer's premises in order to integrate with directory services residing on Customer's premises.
- Symantec Availability Monitor: Customer must allow monitor email sent by the Symantec Availability Monitor to flow through the Service and must not set up detection or data protection policies to block or flag the email.
- Installation of Service Software may be required for enabling certain features of the Service.

Assistance and Technical Support

Customer Assistance Team. Symantec will provide the following assistance as part of the Service:

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

Technical Support Team. The following technical support is included with the Service:

- Support available on a twenty-four (24) hour/day by seven (7) day/week basis to:
  a) provide technical support to Customer for problems with the Service; and
  b) communicate with Customer to resolve such problems.

If Customer contacts the Technical Support Team via telephone or email, the severity level or the request is determined by, and response time defined by, the table below:

Severity Level	Definition	Response Target
1	Loss of Service	Calls responded to within 2 hours
2	Partial loss of Service or Service impairment	Calls responded to within 4 hours
3	Potentially Service affecting or non-Service affecting information request	Calls responded to within 8 hours

Maintenance

Symantec must perform maintenance on the Service Infrastructure in order to provide the Service. The following applies to such maintenance:

- *Planned Maintenance*. Symantec will use commercially reasonable efforts to give Customer seven (7) calendar days of notification (a) via email for DLP Cloud Detection or DLP Cloud Console Planned Maintenance and (b) via posting on the management console for Email Security Planned Maintenance. Symantec will use commercially reasonable efforts to perform Planned Maintenance at times when collective customer activity is low, in the time zone in which the affected Infrastructure is located, and only on part, not all, of the network. If possible, Planned Maintenance will be carried out without affecting the Service. During Planned Maintenance, the Service may be diverted to sections of the Service Infrastructure not undergoing maintenance in order to minimize disruptions of the Service.
- *Emergency Maintenance*. Where Emergency Maintenance is necessary and is likely to affect the Service, Symantec will endeavor to inform the affected Customers in advance by posting an alert on the management console or by delivering an alert via email no less than one (1) hour prior to the start of the Emergency Maintenance.
- *Routine Maintenance*. Symantec will use commercially reasonable efforts to perform maintenance on DLP Cloud Detection, the DLP Cloud Console, and the Email Security management console at times when collective Customer activity is low, to minimize disruption to the availability of the Service and management console, respectively. Customers will not receive prior notification for these routine maintenance activities.

C. SERVICE CONDITIONS

- The following limits apply to the Service:

  - Inbound and outbound messages, per User per calendar month = ten thousand (10,000). This limit is not inclusive of Spam and Malware directed at Customer. Symantec reserves the right to invoice Customer for additional Users, upon notification, for the remaining months on the Service contract where usage exceeds the message limit.
  - Maximum email size = thirty megabytes (30 MB). Any Emails that are received by the Service that exceed the specified limit will not be subject to inspection or guaranteed delivery to the intended recipient.
- Customer 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 a 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 Infrastructure. In addition, Symantec reserves the right to reverse all configuration changes made upon provisioning the Service and it is the responsibility of Customer to undertake all other necessary configuration changes if the Service is reinstated. Further, Symantec reserves the right to purge all Violations recorded since provisioning the Service. 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 following limits apply to DLP Cloud Console

  - Violation retention limit = up to seven (7) years. Symantec reserves the right to purge Violations older than the Violation retention limit.
  - Total Violation count limit = two hundred (200) Violations per User, but not to exceed one million (1,000,000) Violations regardless of the number of Users. In the event that Customer generates Violations that cause the Service to exceed the total Violation count limit, Symantec reserves the right to purge excess Violations beginning with earliest Violations first, even if those Violations still fall within the Violation retention limit. Customer may manually purge Violations from the DLP Cloud Console to avoid reaching the total Violation count limit.
  - Aggregate Violation size limit = one hundred megabytes (100 MB) per User, but not to exceed five hundred gigabytes (500 GB) regardless of the number of Users. In the event that Customer generates Violations that cause the Service to exceed the aggregate Violation size limit, Symantec reserves the right to purge excess Violations beginning with earliest Violations first, even if those Violations still fall within the Violation retention limit. Customer may manually purge Violations from the DLP Cloud Console to avoid reaching the aggregate Violation size limit.
- The following limits apply to Email Security:
  - Inbound mail retry schedule = seven (7) calendar days.
  - Message Tracing = data is available for troubleshooting searches for 30 days; additional limits apply to the number of results that can be returned by a single search.
  - Malware Quarantine = Emails are automatically deleted after thirty (30) days.
  - Spam Quarantine = Emails are automatically deleted after fourteen (14) days.
  - Dashboard reporting data availability = twelve (12) months.
  - Summary (PDF) reporting data availability = twelve (12) months.
  - Detailed (CSV) reporting data availability = forty (40) days.
- The following limitations apply to Policy Based Encryption:
  - Policy Based Encryption (Z) outbound Emails per User per month = three hundred (300)
  - Policy Based Encryption Essentials/Advanced outbound Emails per User per month = four hundred and eighty (480)
  - When sending to multiple recipients, each unique address will be counted as a secure Email. In the event that Customer exceeds the number of permitted secure Emails in any calendar month, Symantec reserves the right to invoice Customer for actual usage.
  - Emails routed through the Policy Based Encryption Service are limited to a maximum size of thirty megabytes (30 MB).
  - If using Pull encryption with Policy Based Encryption (Z) service, by default, Emails will be stored for 90 days in the secure pickup portal before expiring.
  - If using Pull encryption with Policy Based Encryption (E) service, by default, Emails will be stored for 30 days in the secure pickup portal before expiring.
  - The Availability and Latency Service Levels do not apply to this Service.

- To ensure that messages are secured at all points during transmission, Symantec recommends that Customer configure domains that will be used for Policy Based Encryption such that TLS encryption is enforced on all outbound and inbound messages to and from the Service Infrastructure.
- Customer must route their inbound Email through Symantec using the routing information provided by Symantec and must not route Email to a specific Tower or IP address.
- 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 accept inbound Email from all required IP ranges to ensure continuity of the Service in the event that a portion of the Infrastructure is not available.
- 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 to receive the Service (the "Validation List"). It is Customer's responsibility to verify the Validation List prior to the Service being made available and throughout the Term. Emails sent to Email addresses not on the Validation List, or incorrectly entered, will be rejected by the Service. Customer accepts that SLAs will not apply to Emails sent to invalid addresses. For the avoidance of doubt, Customers using the Spam Quarantine system must maintain a Validation List and have the Address Registration capability enabled. If Customer is unable to provide such a Validation List and requests that the Address Registration capability is disabled, 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.
- If Customer chooses, it may request the alternative Email Quarantine ("Message Manager") to replace Spam Manager, and Symantec will assess each such request on a case-by-case basis and reserves the right to decline to enable Message Manager for any Customer, in Symantec's sole and absolute discretion. Message Manager allows Users to employ certain functionality to manage Emails which are quarantined by inbound Spam protection, Email Data Protection and Email Image Control. The current version of Message Manager is a limited availability release provided to Customer "as is." Customer has sole responsibility to ensure that the functionality of Message Manager meets their needs prior to submitting a request for provisioning of this alternative feature.
- Customer may request and Symantec may enable, only in its sole and absolute discretion, "Per User Routing" to allow Customer to route inbound Emails to a mail server IP address for specified Users. Any Customer receiving Per User Routing is solely responsible for providing and maintaining the configuration files as described by the Per User Routing Administration Guide. CUSTOMER AGREES THAT SYMANTEC IS NOT RESPONSIBLE FOR, OR LIABLE DUE TO, THE NON-DELIVERY OR MISROUTING OF EMAIL RESULTING FROM ERRORS IN OR OMISSIONS FROM THE PER USER ROUTING CONFIGURATION FILES.
- Customer may release Emails that have been categorized as containing a Virus, or request that Symantec release such Email, within Customer's domain. CUSTOMER AGREES THAT SYMANTEC

IS NOT RESPONSIBLE FOR, OR LIABLE DUE TO, THE RELEASE OF SUCH EMAILS ON CUSTOMER'S REQUEST.

- Symantec is not responsible or liable for any damage or loss resulting directly or indirectly from any failure of the Service to identify Spam or for wrongly identifying an email as being Malware or Spam. Symantec reserves the right to scan all outbound Emails.
- A default disclaimer message will be applied to Emails that are scanned by the Service from the time of provisioning the Service, the text of which may be edited by Customer via the management console. Symantec reserves the right to update the default disclaimer message at any time.
- Symantec does not access, read, or copy mails, their attachments or linked content other than by electronic methods for the purposes of providing the Service. However, Symantec reserves the right to utilize the Malware and Spam related content of such Emails, their attachments and linked content solely for the purposes of: (i) maintaining and improving the performance of the Service; and (ii) making available to licensors of the Service any information passing through the Service which may be of interest to the licensors solely for the purpose of further developing and enhancing the Service.

D. SERVICE LEVEL – DLP CLOUD DETECTION

Service Availability

- Service Availability for DLP Cloud Detection, for any month, will be no less than ninety-nine and nine-tenth percent (99.9%) uptime. "Service Availability" for DLP Cloud Detection means the ability to send email through DLP Cloud Detection as measured by the Symantec Availability Monitor that sends email through Customer's detection server instances at Symantec. This Service Availability shall only apply if DLP Cloud Detection is able to accept Customer's outbound email from a correctly configured Customer email host on behalf of Customer's domain(s) on a 24x7 basis.
- The foregoing Service Availability will not apply: (i) during periods of Planned Maintenance, Emergency Maintenance, or of non-availability due to force majeure or acts or omissions of either Customer or a third party; (ii) during any period of suspension of Service by Symantec in accordance with the terms of the Agreement; (iii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); (iv) if Customer has not configured the Service in accordance with the Agreement; or (v) during trial Service periods.

SERVICE LEVEL – DLP CLOUD CONSOLE

Service Availability

- Service Availability for DLP Cloud Console, for any month, will be no less than ninety-nine percent (99%) uptime. "Service Availability" for DLP Cloud Console means the ability to access the DLP

Cloud Console using a using a secure, password-protected login. This Service Availability shall only apply if the User accessing the DLP Cloud Console: (i) freely has access to the Internet (ii) is using a supported web browser to access the DLP Cloud Console and (iii) is unfettered by upstream firewalls and proxy servers that may block or control access to specific destinations on the Internet.

- The foregoing Service Availability will not apply: (i) during periods of Planned Maintenance, Emergency Maintenance, or of non-availability due to force majeure or acts or omissions of either Customer or a third party; (ii) during any period of suspension of Service by Symantec in accordance with the terms of the Agreement; (iii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); (iv) if Customer has not configured the Service in accordance with the Agreement; or (v) during trial Service periods.

SERVICE LEVEL – EMAIL SECURITY

General

- Customer may be entitled to Service Credit if Symantec does not meet the defined Email Security service level. If Customer believes it is entitled to Service Credit, Customer must submit a Credit Request within ten (10) business days of the end of the calendar month in which the suspected service level non-compliance occurred. Customer recognizes that logs are only kept for a limited number of calendar days and therefore any Credit Request submitted outside of the provided timeframe will be deemed invalid.
- A Credit Request is made by sending an email to support.cloud@symantec.com with the subject line “Credit Request” indicating the affected Service Level Agreement, the date/time of the failure, any technical support ticket information related to such failure, and any other relevant information.
- All Credit Requests will be subject to verification by Symantec in accordance with the applicable provisions of this Service Level Agreement. Symantec may request additional information from Customer to validate the Credit Request.
- The remedies set out in this Service Level Agreement shall be Customer’s sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise, with respect to this Service Level Agreement.
- For the purpose of calculating Service Credits, the Monthly Charge for Email Security shall be deemed to be half of the total monthly charge for the Service. The maximum accumulative liability of Symantec under this Service Level Agreement in any calendar month shall be no more than one hundred percent (100%) of the Monthly Charge payable by Customer for Email Security.

Exceptions to Service Level Agreement for Email Security Services

This Service Level Agreement will not operate: (i) in respect of any Emails that have not passed through the Service (including without limitation if Customer has not taken appropriate steps to ensure that it will only accept inbound Email from the Symantec Infrastructure); (ii) in respect of any inbound or outbound Emails that were initially sent to Symantec containing more than 500 recipients per SMTP session, (iii) for any Customers provisioned on any Tower designated as a Bulk Cluster Tower, (iv) in respect of any inbound or outbound Emails for Customer domains that are not provisioned for the Service, (v) during periods of Planned Maintenance, Emergency Maintenance, or of non-availability due to force majeure or acts or omissions of either Customer or a third party; (vi) during any period of suspension of Service by Symantec in accordance with the terms of the Agreement; (vii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); (viii) if Customer has not configured the Service in accordance with the Agreement; or (ix) during trial service periods.

Service Availability

The Service Availability service level is defined by the ability to establish a SMTP session on port 25 of the Designated Tower Cluster, as measured by Symantec Tracker. The Service Availability Service Level does not apply to the management console or Spam Quarantine system. This Service Level shall not apply if Customer has incorrectly configured the Service.

If Service Availability is below one hundred percent (100%) in any calendar month, Customer may submit a Credit Request and may receive a Service Credit for the following percentage credit:

Percentage Available Per Calendar Month	Percentage Credit Of Monthly Charge
Below 100% and above of equal 99%	25%
Below 99% and above or equal 98%	50%
Below 98%	100%

If Service Availability falls below ninety eight percent (98%) in any calendar month, as confirmed by Symantec, Customer shall be entitled to terminate the affected Service and receive a pro-rata refund of fees paid in advance for the portion of the term after such termination is effective.

Email Delivery

The Email Delivery service level is defined by Symantec's ability to deliver 100% of all email sent to or from Customer subject to the following conditions:

a) The Email must have been received by Symantec; and

b) The Email must not contain a Virus, Spam or other content which has caused it to be intercepted by the Service.

Subject to the conditions above, in the event Symantec fails to deliver an email to or from Customer and Customer is not in breach of the terms of the Agreement, Customer is entitled to terminate the Service upon thirty (30) calendar days prior written notice.

Email Latency

The Email Latency service level is defined by whether the average round-trip time, as measured by the Symantec Tracker, for emails sent every five (5) minutes to and from every tower within Customer's Designated Tower Cluster exceeds the delays stated in the table below, in a calendar month. If Customer believes that the Email Latency service level has not been met, Customer may submit a Credit Request and may receive a Service credit in accordance with the table below:

Average Round-Trip Time (seconds)	**Percentage Credit of Monthly Charge**
Above 60 and below or equal 90	25%
Above 90 and below or equal 120	50%
Above 120 and below or equal 180	75%
Above 180	100%

This Latency service level will not apply if:

a) Customer has not supplied Symantec with a Validation List and Customer suffers a denial of service attack;

b) Periods of delay are caused by a mail loop from/to Customer systems;

c) Customer's primary email server is unable to accept Email on the initial attempted delivery.

Spam False Positive

The Spam False Positive service level defines the maximum Spam False Positive Capture Rate. The Spam False Positive service level will only apply if Customer implements the Antispam Best Practice Settings as provided in the Online Help resource.

If the average Spam False Positive capture rate rises above 0.0003% of Customer's inbound email traffic in any calendar month, Customer may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Spam False Positive Capture Rate %	**Percentage Credit Of Monthly Charges**
Above 0.0003 and below or equal 0.003	25%
Above 0.003 and below or equal 0.03	50%
Above 0.03 and below or equal 0.3	75%
Above 0.3	100%

The following emails do not constitute Spam False Positive emails for the purposes of this service level:

a) Emails that are not legitimate business email;

b) Emails containing more than 20 recipients;

c) Emails where the sender of the email is on Customer's blocked senders list, including without limitation, those defined by the individual user if Customer has enabled user-level settings;

d) Emails that are sent from a compromised machine;

e) Emails that are sent from a machine which is on a third-party block list;

f) Emails that have at least eighty percent (80%) of the same content;

g) Emails intercepted by outbound Spam scanning;

In order to be eligible for a Service Credit, Customer must report and send suspected Spam False Positive Emails to support.cloud@symantec.com within five (5) calendar days of receipt of the email. Symantec will investigate and confirm whether or not the Email is a Spam False Positive and will record the finding.

Spam Capture Rate

The Spam Capture Rate service level defines the minimum Spam Capture Rate. This service level will only apply if Customer implements the Antispam Best Practice Settings as provided in the Online Help resource. The service level corresponds to the number of Spam False Negatives measured in a calendar month.

Customer may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Spam Capture Rate %	Percentage Credit of Monthly Charge
Above 98 and below or equal 99	25%
Above 97 and below or equal 98	50%
Above 96 and below or equal 97	75%
Below 96	100%

This Spam Capture Rate Service Level will not apply if the Email was not sent to a valid email address.

A lower Spam Capture Rate of 95% shall apply to emails containing more than 50% double-byte character sets. In the event that such Spam Capture Rate falls below 95%, Customer shall be entitled to a 25% Service Credit of the monthly charge. In the event that the Spam Capture Rate falls below 90%, Customer may be entitled to a Service Credit equal to 100% of the monthly charge.

In order to be eligible for a Service Credit, Customer must report and send suspected false negative emails to support.cloud@symantec.com within five (5) calendar days of receipt of the email. Symantec will investigate and confirm whether or not the email is a Spam False Negative and will record the finding.

Malware and Virus Protection

If Customer systems are infected by one or more Known Malware, Known Virus or Unknown Virus, by an Email that passed through the Service, in any calendar month, Customer may be entitled to a Service Credit in the amount defined below. Customer must notify Symantec and such notification must be logged and validated by Symantec's support call records to confirm that a Malware or Virus has been passed to Customer through the Service. Customer must submit a Credit Request, and if validated, will receive a Service Credit equal to the lower of 100% of the Monthly Charge or ten thousand dollars/five thousand pounds sterling/ten thousand euro ($10,000/£5,000/€10,000) (depending on the currency in which Customer is invoiced). The remedy set out in this section shall be the sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise in respect of any infection by a Malware or Virus passed to Customer or a third party through the Service. For the avoidance of doubt, the remedy set out in this section shall not apply in cases of deliberate self-infection.

Customer systems are deemed to be infected if a Malware or Virus contained in an Email received through the Service has been activated within Customer's systems either automatically or with manual intervention.

In the event that Symantec detects, but does not stop a Malware- or Virus-infected Email, and notifies Customer's designated support contact(s), providing sufficient information to enable Customer to identify and delete the infected Email, the remedy set out above shall not apply.

The Service will scan as much of the Email and its attachments as possible. It may not be possible to scan attachments with content that is under the direct control of the sender (for example, password protected and/or encrypted attachments). Such email and/or attachments are excluded from the Service Level and the remedy set out above shall not apply.

This Malware and Virus Protection Service Level shall not operate in relation to Malware or Viruses that have been intentionally released by Customer or by Symantec on request of Customer.

This Malware and Virus Protection Service Level shall only apply to Malware and Virus as defined in this Service Description, and will not apply to the following, including, but not limited to; phishing; spyware; adware; or URL links to websites hosting malicious content.

Malware False Positive

The Malware False Positive service level defines the maximum Malware False Positive Capture Rate. If the Email Malware False Positive capture rate rises above 0.0001% of Customer's Email traffic in any calendar month, Customer may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Malware False Positive Capture Rate %	Percentage Credit of Monthly Charge
Above 0.0001 and below or equal 0.001	25%
Above 0.001 and below or equal 0.01	50%
Above 0.01 and below or equal 0.1	75%
Above 0.1	100%

F. MISCELLANEOUS

Service Renewal

- Notwithstanding anything to the contrary in the Agreement, the Service does not renew automatically. To renew the Service, Customer must submit a renewal order at least sixty (60) days prior to expiration of the Service.
- Customer must provide reasonable assistance to Symantec to complete the processing of the Renewal Order and must apply required renewal credentials to renew the Service and maintain account information and data available during the Service Term.

General

- Symantec may update the Service at any time in order to maintain the effectiveness of the Service. Symantec may update this Service Description from time to time to accurately reflect the Service being provided.
- The Service may be accessed and used globally, subject to applicable export compliance limitations and technical limitations in accordance with the then-current Symantec standards.
- Customer is permitted to use the Service solely for Customer's own business purposes. Customer agrees not to resell, sublicense, lease, or otherwise make the Service and associated documentation available to any third party. Customer agrees not to use the Service for the purposes of building a competitive product or service or copying its features or user interface, performing Service evaluations, benchmarking or other comparative analysis intended for publication outside Customer organization without Symantec's prior written consent.
- Customer shall comply with all applicable laws with respect to use of the Service. In certain countries, it may be necessary to obtain the consent of individual personnel. Configuration and use of the Service(s) is entirely in Customer’s control, therefore, Customer is solely responsible for, and Symantec is not liable for, Customer’s use of the Service(s), nor is Symantec liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.
- Customer may not disclose the results of any benchmark tests or other tests connected with the Service to any third party without Symantec’s prior written consent.
- The use of any Service Component in the form of software shall be governed by the license agreement accompanying the software. If no EULA accompanies the Service Component, it shall be governed by the terms and conditions located at http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf. Any additional rights and obligations with respect to the use of such Service Component shall be as set forth in this Service Description.
- Except as otherwise specified in the Service Description, the Service (including any Hosted Service Software Component provided therewith) may use open source and other third party materials that are subject to a separate license. Please see the applicable Third Party Notice, if applicable, at http://www.symantec.com/about/profile/policies/cloud-services-agreements.jsp.

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

G. DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement or this Services Description, have the meaning given below:

"Address Registration" is a mandatory feature of the Email Security Service that rejects inbound emails sent to Email addresses that are not included in Customer's list of valid Email addresses (the "Validation List").

"Administrator" means a Customer User with authorization to manage the Service on behalf of Customer. Administrators may have the ability to manage all or part of a Service as designated by Customer.

"Antispam Best Practice Settings" means Symantec's recommended configuration guidelines for the Email Security Service as provided to Customer during the provisioning process or as published in the online help resource.

"Credit Request" means the notification which Customer must submit to Symantec by Email to support.cloud@symantec.com with the subject line "Credit Request" (unless otherwise notified by Symantec).

"Designated Tower Cluster" means two (2) or more Towers designated to provide Email Security Services to Customer.

"Email" means any inbound or outbound SMTP message passing through the Service.

"Emergency Maintenance" means unscheduled maintenance periods during which the Service may be disrupted or prevented due to non-availability of the Service Infrastructure or any maintenance for which Symantec could not have reasonably prepared for the need for such maintenance, and failure to perform the maintenance would adversely impact Customer.

"End User License Agreement (EULA)" means the terms and conditions accompanying Software (defined below).

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

"Known Malware/Known Virus" means a Malware or Virus for which at the time of receipt of the content by Symantec: (i) a signature has already been made publicly available for a minimum of one (1) hour for configuration by antivirus technologies used by Symantec; or (ii) is included in the "Wild List" held at http://www.wildlist.org and identified as being "In the wild" by a minimum of 2 Wild List participants.

“Malware” means “malicious software”. This term is used generically to describe software that intentionally causes harm including but not limited to “Viruses”, “Worms”, “Trojans”, “Email bombs”, “Cancelbots” or other similar destructive computer programming routine.

“Malware False Positive” means a legitimate Email incorrectly identified as containing a Malware.

“Meter” means the applicable unit(s) of measurement by which Symantec prices and sells a Subscription to an Online Service, in effect at the time of the Order Confirmation.

“Monthly Charge” means the monthly charge for the affected Service(s) as defined in the Agreement.

“Online Help” means additional information available at http://help.symanteccloud.com/.

“Open Proxy” means a proxy server configured to allow unknown or unauthorized third parties to access, store or forward DNS, web pages or other data for the Service.

“Open Relay” means an Email server configured to receive Email from an unknown or unauthorized third party and forward the Email to one or more recipients that are not users of the Email system to which that Email server is connected. Open Relay may also be referred to as a “Spam relay” or “public relay”.

“Planned Maintenance” means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure.

“Service Component” means certain enabling software, hardware peripherals and associated documentation which may be separately provided by Symantec as an incidental part of a Service.

“Service Credit” means the amount of money that will be credited to Customer’s next invoice after submission of a Credit Request and validation by Symantec that a credit is due to Customer.

“Service Software” means Software (defined below), as may be required by the Service, which must be installed on each Customer computer, in order to receive the Service. Service Software includes the Software and associated documentation that may be separately provided by Symantec as part of the Service.

“Software” means each Symantec or licensor software program, in object code format, licensed to Customer by Symantec and governed by the terms of the accompanying EULA, including without limitation new releases or updates as provided hereunder.

“Spam” means unsolicited commercial Email.

“Spam False Negative” means a Spam Email that is not identified as Spam by the Email Security Service.

“Spam False Positive” means an Email incorrectly identified as Spam by the Email Security Service.

“Subscription Instrument” means one or more of the following applicable documents which further defines Customer’s rights and obligation related to the Service: a Symantec certificate or a similar document issued by Symantec, or a written agreement between Customer and Symantec, that accompanies, precedes or follows the Service.

“Symantec Hosted Services Terms” means the terms and conditions located at or accessed through https://www.symantec.com/about/legal/service-agreements.jsp.

“Symantec Online Service Terms and Conditions” means the Online Services Terms and Conditions located at or accessed through https://www.symantec.com/about/legal/service-agreements.jsp.

“Symantec Tracker” means a Symantec tool by which Service Availability and Latency are measured for the Service.

“Tower” means a cluster of load balanced Email servers.

“Unknown Virus” means a Virus for which at the time of receipt of the content by Symantec: (i) a signature has not already been made publicly available for a minimum of one (1) hour for configuration by antivirus technologies used by Symantec; or (ii) was not included in the "Wild List" held at http://www.wildlist.org and identified as being "In the wild" by a minimum of 2 Wild List participants.

“User” means an individual person and/or device authorized to use and/or benefits from the use of the Service, or that actually uses any portion of the Service.

“Violation” means a persistent artifact generated by DLP Cloud Detection and accessible from the DLP Cloud Console that contains details about a DLP policy violation including (but not limited to) contextual details about the violating Email (for example, sender, recipient, subject, list of attachments, etc.), policy rule violations and associated content matches, and applied remediation actions. Violations may contain excerpts of the violating content as well as a copy of the original Email and its attachments.

“Virus” means a piece of program code, including a self-replicating element, usually disguised as something else, which is designed so that it may infect other computer systems.

END OF SERVICE DESCRIPTION

Exhibit A

EULA for Service Software to Directory Synchronization Tool

SYMANTEC SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") IS WILLING TO LICENSE THE LICENSED SOFTWARE (AS DEFINED BELOW) TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT ("LICENSE AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY CLICKING THE "I AGREE" OR "YES" BUTTON, OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING OR OTHERWISE USING THE LICENSED SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE LICENSED SOFTWARE.

1. License Rights. Subject to Your compliance with the terms and conditions of this License Agreement, Symantec grants to You a non-exclusive, non-transferable license to use a reasonable number of copies of the Licensed Software solely in support of Your use of the Symantec DLP Cloud Service for Email with Cloud Console. "Licensed Software" means the Symantec software program, in object code form, accompanying this License Agreement, including any associated program documentation included in, or provided for use with, such software.
2. License Restrictions. You may not, without Symantec's prior written consent, conduct, cause or permit the: (i) use, copying, modification, rental, lease, sublease, sublicense, or transfer of the Licensed Software except as expressly provided in this License Agreement; (ii) creation of any derivative works based on the Licensed Software, except as expressly provided in this License Agreement; (iii) reverse engineering, disassembly, or decompiling of the Licensed Software (except that You may decompile the Licensed Software for the purposes of interoperability only to the extent permitted by and subject to strict compliance under applicable law); (iv) use of the Licensed Software in connection with service bureau, facility management, timeshare, service provider or like activity whereby You operate or use the Licensed Software for the benefit of a third party; or (v) use of the Licensed Software by any party other than You, except as expressly provided in this License Agreement.
3. Ownership/Title. The Licensed Software is the proprietary property of Symantec or its licensors and is protected by copyright and patent laws. Symantec and its licensors retain any and all rights, title and interest in and to the Licensed Software, including in all copies, improvements, enhancements, modifications and derivative works of the Licensed Software. Your rights to use the Licensed Software shall be limited to those expressly granted in this License Agreement. All rights not expressly granted to You are retained by Symantec and/or its licensors.

4. Updates. Any updates to the Licensed Software provided by Symantec at its sole discretion ("Updates") shall be subject to any terms and conditions provided with such Updates. If no terms and conditions are provided, then Updates are subject to this License Agreement.
5. Third Party Programs. This Licensed Software may contain third party software programs ("Third Party Programs") that are available under open source or free software licenses. This License Agreement does not alter any rights or obligations You may have under those open source or free software licenses. Notwithstanding anything to the contrary contained in such licenses, the disclaimer of warranties and the limitation of liability provisions in this License Agreement shall apply to such Third Party Programs.
6. Warranty and Limitation of Liability.

   6.1. Warranty Disclaimer. THE LICENSED SOFTWARE IS PROVIDED "AS IS," EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ANY OTHER WARRANTY, WHETHER EXPRESSED OR IMPLIED.

   6.2. Limitation of Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY DIRECT, SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA, ARISING OUT OF THE USE OR INABILITY TO USE THE LICENSED SOFTWARE, EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

   SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

7. No Support or Maintenance. Notwithstanding any other terms contained in this License Agreement, Symantec does not offer support or maintenance for the Licensed Software.
8. Data Collection. To the extent that Symantec processes any Personal Information in accordance with Your use of the Licensed Software and/or Maintenance/Support, Symantec will be the Data Processor and You will be the Data Controller. "Personal Information" means personal data as defined by applicable data protection law, which may include without limitation names, e-mail address, contact details of designated users and contacts, IP addresses, etc., as may be provided by You to Symantec during Your, or Your users, use of the Licensed Software and Maintenance. You undertake to obtain all necessary consents, permits or licenses, and to comply with all applicable data protection legislation, in particular the Data Protection Directive (95/46/EC) or any successor legislation, with regards to the provision of Personal Information to Symantec in accordance with this License Agreement. Symantec shall process Personal Information as is necessary to (i) enable, optimize and provide the Licensed Software and/or Maintenance/Support to You and Your users, (ii) to administer and enforce its License Agreements with You, (iii) to make recommendations regarding usage of the Licensed Software, Maintenance/Support and other Symantec products and services, (iv) to improve and develop Symantec's products and services including, without limitation, for security research and

development, or threat detection and security reporting purposes, and (v) to generate statistical reports and analysis about use of the Licensed Software and/or Maintenance/Support (including analysis related to security trends and data patterns, and comparisons in Symantec's aggregated install base) (collectively "Reports"). Symantec shall implement and maintain appropriate technical and organisational measures to protect the Personal Information processed under this License Agreement against accidental loss, destruction, damage, alteration or disclosure. You hereby consent for Symantec to transfer Personal Information, as maybe required to provide the Licensed Software and/or Maintenance/Support pursuant to this License Agreement, to the United States or other countries that may have different data protection laws than the region in which You are located and may be accessed by Symantec employees, contractors, partners and vendors for the purposes described above. Where transfers of Personal Information are made from the European Economic Area to outside the European Economic Area, You agree that Symantec will execute Standard Contractual Clauses on your behalf. In the event of a conflict between the clauses of this License Agreement and the Standard Contractual Clauses with respect to data processed under this License Agreement, the terms of the Standard Contractual Clauses will prevail to the extent of the conflict. Your acceptance of this License Agreement shall be treated as Your signature of the Standard Contractual Clauses.

9. Export Regulation. You acknowledge that the Licensed Software and related technical data and services (collectively "Controlled Technology") are subject to the import and export laws of the United States, specifically the U.S. Export Administration Regulations (EAR), and the laws of any country where Controlled Technology is imported or re-exported. You agree to comply with all relevant laws and will not to export any Controlled Technology in contravention to U.S. law nor to any prohibited country, entity, or person for which an export license or other governmental approval is required.
10. Term and Termination. This License Agreement will continue as long as You are in compliance with its terms. In the event You breach this License Agreement, it will automatically terminate. Upon termination, You must immediately stop using and destroy all copies of the Licensed Software within Your possession or control. The Ownership/Title, Warranty and Limitation of Liability and General sections of this License Agreement will survive termination of the Agreement.
11. General. You may not assign the rights granted hereunder or this License Agreement, in whole or in part and whether by operation of contract, law or otherwise, without Symantec's prior express written consent. Symantec may audit Your use of the Licensed Software. If You are located in North America or Latin America, this License Agreement will be governed by the laws of the State of California, United States of America. If You are located in China, this License Agreement will be governed by the laws of the Peoples Republic of China. Otherwise, this License Agreement will be governed by the laws of England. Such governing laws are exclusive of any provisions of the United Nations Convention on Contracts for Sale of Goods, including any amendments thereto, and without regard to principles of conflicts of law. If any provision of this License Agreement is found partly or wholly illegal or unenforceable, such provision shall be enforced to the maximum extent permissible, and remaining provisions of this License Agreement shall remain in full force and effect. A waiver of any breach or default under this License Agreement shall not constitute a waiver of any other subsequent breach or default. This License Agreement is the complete and exclusive agreement

between You and Symantec relating to the Licensed Software and supersedes any previous or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter.

GLB TECHNOLOGY EULA TEMPLATE v.4.0_Directory Synchronization Tool_26Jan2017