Symantec™ Data Loss Prevention Cloud Service for Email with Cloud Console and Symantec Endpoint Data Loss Prevention

Service Description

June 2019

This Service Description describes **Symantec Data Loss Prevention Cloud Service for Email with Cloud Console** and **Symantec Endpoint Data Loss Prevention** (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

Symantec™ Data Loss Prevention Cloud Service for Email with Cloud Console and Symantec Endpoint Data Loss Prevention

Service Description

June 2019

1: Technical/Business Functionality and Capabilities

Service Overview

Symantec Data Loss Prevention Cloud Service for Email with Cloud Console and **Symantec Endpoint Data Loss Prevention**[1] 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 recommended remediation actions from the Service.

The Service is licensed for use in the following ways:

Symantec Data Loss Prevention Cloud Service for Email with Cloud Console:	**Symantec Endpoint Data Loss Prevention**:
Symantec Data Loss Prevention Cloud Service for Email with Cloud Console provides DLP detection to outbound Email traffic by any of the following supported third-party enterprise email service providers: Microsoft Office 365 Exchange Online or Google G Suite Gmail. The Service can be used in conjunction with Symantec Email Security.cloud Safeguard to perform DLP detection on outbound emails from Microsoft Office 365 Exchange Online or Google G Suite Gmail (Note: A separate subscription to Email Security.cloud is required. The Service Description for Symantec Email Security.cloud service is located at https://www.symantec.com/about/legal/repository).	**Symantec Endpoint Data Loss Prevention** is used in conjunction with Symantec Endpoint Protection 15 with Symantec Integrated Cyber Defense Manager to add DLP detection to endpoint Devices to monitor and control sensitive data in use and in motion on those Devices (Note: A separate subscription to Symantec Endpoint Protection is required. The Service Description, End User License Agreement, and Product Use Rights for Symantec Endpoint Protection are located at https://www.symantec.com/about/legal/repository).
DLP Cloud Detection (Symantec Data Loss Prevention Cloud Service for Email with Cloud Console only) provides: • Content detection including Indexed Document Matching and 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 detecting 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.	**Endpoint DLP Agent** (Symantec Endpoint Data Loss Prevention only) 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 use or in motion on managed endpoint devices. • File type, size, and count detection for detecting files or file attachments in emails. • Contextual controls based on user, email sender/recipient, or domain information. • Automated remediation including blocking and notification. • Violation generation with Violation details that include contextual details, sensitive content matches, policy rule violations, and applied remediation actions.

[1] **Symantec Endpoint Data Loss Prevention** is only available to Customers who have a concurrent Subscription for Symantec Endpoint Protection.

Symantec™ Data Loss Prevention Cloud Service for Email with Cloud Console and Symantec Endpoint Data Loss Prevention

Service Description

June 2019

With either **Symantec Data Loss Prevention Cloud Service for Email with Cloud Console** or **Symantec Endpoint Data Loss Prevention**, the **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.
- Creation and modification of DLP policies for the Service. These policies are then applied to Email or files inspected by the Service.
- Ability to view Violations generated by DLP Cloud Detection and/or the Endpoint DLP Agent as a result of a policy violations.
- Integration with Customer premises directory services using 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 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.
- Ability to configure the Service to send automatic notification that is triggered when an Email or file violates the DLP policy. The recipient of this notification action is configurable and such notifications can be created, deleted and customized through the DLP Cloud Console.

Service Features

- Customer can access the Service through the **DLP Cloud Console**. Customer may configure and manage the Service, access reports, and view data and statistics, through the **DLP Cloud Console**, when available as part of the Service.
- 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.
- Should a Service be suspended or terminated for any reason whatsoever, Symantec will reverse all configuration changes made upon provisioning the Service and it is the responsibility of Customer to undertake all other necessary configuration changes when the Service is reinstated.

Service Level Agreement

- Symantec provides the applicable service level agreement ("SLA") for the Service as specified in Exhibit A.

Supported Platforms and Technical Requirements

- Supported platforms for the Service are defined at
    - (1) http://www.symantec.com/docs/INFO4144 for the Symantec Data Loss Prevention Cloud Service for Email with Cloud Console; and
    - (2) https://help.symantec.com/cs/CLOUD_DLP/CDLP/v132281600_v132124660/System-requirements-and-support-for-Symantec-Endpoint-Data-Loss-Prevention?locale=EN_US for Symantec Endpoint Data Loss Prevention.

Hosted Service Software Components

- The Service includes the following software components:
    - The DLP Cloud Console provides a Directory Synchronization Tool that enables Administrators to synchronize users and groups within a directory residing on the Customer's premises to the DLP Cloud Console for use in DLP detection policies. The Directory Synchronization Tool must be installed on a server residing in Customer's premises.

- The DLP Cloud Console provides an Indexed Document Matching (IDM) Remote Indexer and Bridge that enables Administrators to generate and maintain indices of sensitive documents for use in DLP detection policies. The IDM Remote Indexer and Bridge must be installed on a server residing in Customer's premises.
- The Endpoint DLP Agent is deployed on managed devices and enables Administrators to enforce DLP detection policies on these devices. The Endpoint DLP Agent is only applicable to Symantec Endpoint Data Loss Prevention.

- The use of any software component is governed by the Agreement and, if applicable, any additional terms published with this Service Description on www.symantec.com/about/legal/repository.

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.

- Service Activation: Customer must follow required steps to activate the Service:
  - Customer must use the *DLP Cloud Console as the management console for Symantec Data Loss Prevention Cloud Service for Email with Cloud Console* and/or *Symantec Endpoint Data Loss Prevention*, including all policy management and violation investigation and remediation.
  - Installation of the following software is required for enabling certain features of the Service, as applicable.
    - 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.
    - Customer must install the Indexed Document Matching (IDM) Remote Indexer and Bridge on a server in the Customer's premises in order to generate and maintain indices of sensitive documents for use in DLP detection policies.
    - Customer must install the Endpoint DLP Agent on managed devices in order to enforce DLP detection policies on those devices.
- Setup Enablement: Customer must provide information required for Symantec to begin providing the Service.
- 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 DLP Cloud 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 liable for Customer's use of the Service, nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.

The following conditions and limits apply to the **Symantec Data Loss Prevention Cloud Service for Email with Cloud Console** only:

- Customer must route Emails scanned by the Service to Symantec Email Security.cloud for delivery to recipients. Customer must have a concurrent subscription to the Symantec Email Security.cloud Safeguard service in order for Symantec to deliver the Service.

- Maximum Email size = configurable up to fifty megabytes (50 MB) with a default size limit of thirty megabytes (30 MB). Any Emails that are received by the Service that exceed the limit will be scanned up to configured size limit and evaluated against the DLP detection policy configured by Customer. If the portion of a received Email within the configured size limit violates the policy, automated remediation actions will be applied to the entire Email (including portions of the email beyond the configured threshold). Otherwise, if the portion of a received Email within the configured size limit does not violate any policy, such Email will be passed along to Symantec Email Security.cloud without application of any automated remediation action based on routing configurations chose by Customer.

- 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 Service 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. Further, Symantec reserves the right to purge all Violations recorded since provisioning 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 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.

The following conditions and limits apply to **Symantec Endpoint Data Loss Prevention** only

- It is the Customer's, not Symantec's, responsibility to ensure that the Endpoint DLP Agent is installed on Devices. The Endpoint DLP Agent must be installed and enabled on Devices in order to enforce DLP detection policies.

- Customer Devices running the Endpoint DLP Agent must have connectivity to the Internet and remain in communication with the Service in order to:

    - Obtain DLP detection policies and policy updates
    - Obtain agent configurations
    - Report Violations back to the DLP Cloud Console
    - Obtain agent updates via Live Update.

Customer must make any required firewall and/or proxy changes to allow unfettered agent communication with the Service. Note that policy updates, agent configuration changes, and Violation reporting can take up to 30 minutes to propagate from the DLP Cloud Console to the Endpoint DLP Agent running on Devices maintaining regular communication with the Service.

- Customer must manage Devices, DLP detection policies, agent configurations, and other configuration options through the DLP Cloud Console.

- Maximum file or Email size = thirty megabytes (30 MB). Any files or Emails that are inspected by the Endpoint DLP Agent that exceed the specified limit will not be scanned or evaluated against DLP detection policy configured by Customer.

- 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 Devices, 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 files and Emails.

- Should a Service be terminated for any reason whatsoever, Customer's account will be deleted and Customer will not have access to the Service. Further, Symantec reserves the right to purge all Violations recorded since provisioning the Service.

The following conditions and limits apply to use of DLP Cloud Console (with either **Symantec Data Loss Prevention Cloud Service for Email with Cloud Console** or **Symantec Endpoint Data Loss Prevention**)

- Violation retention limit = configurable up to seven (7) years with a default retention limit of one (1) year. Symantec reserves the right to purge Violations older than the Violation retention limit.

- Total Violation count limit = two hundred (200) Violations per User or Device per Service, but not to exceed one million (1,000,000) Violations regardless of the number of Users, Devices, or Services. 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 or Device per Service, but not to exceed five hundred gigabytes (500 GB) regardless of the number of Users, Devices, or Services. 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.

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 purchase 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 DLP Cloud Service for Email, "Cloud Application" means a supported third-party enterprise email service providers including Microsoft Office 365 Exchange Online or Google G Suite Gmail.

- **"Device"** means an individual device (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 uses any portion of the Service. Each subscription purchase for the Service may only be used by a single Device.

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 email service 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 Page. Customers can also receive notifications via SMS, email or Twitter by subscribing to Symantec Status Page.
- **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 the Symantec Status Page. 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 Page. 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.
- Symantec may modify the Online Services and/or the corresponding Service Descriptions at any time: (a) due to changes in applicable laws or industry standards; and (b) for any other reason, if the modification does not materially reduce the level of performance, functionality, security or availability of the Online Services during the Subscription Term.

6: Definitions

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

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

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

"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.

"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 for 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".

"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 number of days that are added to Customer's current Subscription Term.

"Spam" means unsolicited commercial Email.

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

"Violation" means a persistent artifact generated by DLP Cloud Detection or the Endpoint DLP Agent 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 file and/or 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 file or Email including attachments.

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.

Inline Service Availability	
DLP Cloud Detection (as applicable to Symantec Data Loss Prevention Cloud Service for Email with Cloud Console only)	**>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. management console or reporting tools used by the Administrator).

Non-Inline Service Availability	
DLP Cloud Console	**>99.5%**

3.0 AVAILABILITY CALCULATION

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

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

**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