ONLY THE SERVICE DESCRIPTION(S)/SLA SCHEDULES BELOW THAT CORRESPOND TO THE SERVICES PURCHASED UNDER THE AGREEMENT APPLY

SCHEDULE 1
DEFINITIONS AND GENERAL SERVICES OVERVIEW

1. Symantec Services

1.1. Symantec provides each Internet-hosted and managed Service as defined in each appendix in Schedule 2, Service Descriptions, with applicable service levels defined in Schedule 3, Service Level Agreement.
1.2. Each Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis. Each Service is monitored for hardware availability, service capacity and network resource utilization. Each Service is regularly monitored for service level compliance and adjustments are made as needed.
1.3. Each Service requires information from Customer for successful provisioning and performance of the Service.
1.4. Customer must apply renewal credential(s) accompanying the Subscription Instrument (defined below), to their account, upon receipt. Renewal credentials are required to maintain account information and Customer data during any post termination retention period, if any, as set forth in each applicable Service appendix, below. Otherwise, account access and data may be permanently deleted.

2. Definitions

2.1. The capitalized terms, below, shall have the following meanings for the purposes of the Agreement. Other capitalized terms shall have their plain meaning.

"**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.

"**Connection Manager**" means the detection methods which sit at the SMTP handshake stage.

"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;

"Domain Level Settings" means domain settings that are customizable for a particular domain within the SMC (defined below) for the Email Security Services.

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

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

"**Email Security Services**" are the Email AntiVirus.cloud, Email AntiSpam.cloud, Email Content Control.cloud, Email Image Control.cloud, Email Boundary Encryption.cloud, and Policy Based Encryption.cloud Services as defined in Schedule 2, Service Descriptions.

"**Email Archiving Services**" are the Enterprise Vault.cloud, AdvisorMail on Symantec.cloud, Symantec Email Continuity Archive.cloud, Symantec Email Continuity Archive Lite.cloud, Email Continuity.cloud, and Archiving.cloud (P) Services as defined in Schedule 2, Service Descriptions.

"**Email Virus False Positive**" means a legitimate Email incorrectly identified as containing a Virus.

"Global Settings" means the actions within the SMC (defined below) which are applied to all domains and group levels for the Email Security Services.

"Group Level Settings" means group settings that are customizable for a particular group within the SMC (defined below) for the Email Security Services.

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

"Known Virus" means a 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 anti-Virus 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;

"**Non-Severable Service Bundle**" means a bundle of Services defined in the Non-Severable Service Bundle and Legacy Name Charts located at www.symanteccloud.com/documents.aspx .

"**Member**" means Customer and third parties with whom Customer creates an encrypted network by utilizing the Email Boundary Encryption.cloud Service (defined below).

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

"**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 Email Security Services.

"**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 "Spam relay" or "public relay".

"**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 Level" means each of the Service parameters defined in Schedule 3, Service Level Agreement, below.

"**Service Software**" means Software (defined below), as may be required by a 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, or this Schedule 1, Definitions and General Services Overview, as applicable, 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 AntiSpam.cloud Service.

"**Spam False Positive"** means an Email incorrectly identified as Spam by the Email AntiSpam.cloud Service.

"Spam Recommended Settings" means Symantec's recommended configuration guidelines for the Email AntiSpam.cloud Service as provided to Customer during the provisioning process or as published in the online help resource.

"**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 Tracker**" means a Symantec tool by which Service Availability and Latency, as described in Schedule 3, Service Level Agreement, are measured for the Email Security Services.

"**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 anti-Virus

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. For the Email Security Services and/or Email Archiving Services, the definition of "**User**" shall include all mailboxes that send and/or receive Email.

"**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.

"**Volume Mail**" means a group of more than five thousand (5000) Email messages sent or received by a Customer, with substantially similar content, in a single operation or series of related operations, to individuals or a distribution list, including, but not limited to marketing, alerting, newsletter, or other intended mass communication.

"Web Services" means the Web v2 Protect.cloud and Web v2 URL.cloud Services collectively.

3. Service Management Console (SMC)

3.1. Each Service Management Console, as applicable, is an Internet-based resource and tool available to Customer as part of a Service. Customer can access the SMC by using a secure password protected login. The SMC provides the ability for Customer to configure and manage the Service, access reports, and view data and statistics when available as part of the Service(s). A Customer may have access to multiple SMCs to manage different Services (e.g., ClientNet, CMES, or Manage).

4. Email Security Services Overview

4.1. Email Security Services are only available to a Customer who have their own Email domain name and have the ability to configure the MX records and/or DNS for that domain name.
4.2. Customer must route their inbound Email to Symantec by using the MX records provided at time of provisioning. Customer may optionally route their outbound Email through Symantec to receive the full benefit of the Email AntiVirus.cloud, Email Content Control.cloud and Email Image Control.cloud services. Policy Based Encryption.cloud requires Customer to route their outbound Email through Symantec. Customer should not route Email to a specific Tower or IP address. For the avoidance of doubt, Schedule 3, Service Level Agreements, shall not apply for domains that are not provisioned in accordance with this clause.
4.3. For successful performance of the Email Security Services, Customer must ensure that domains (including sub-domains) are provisioned on the applicable Service Infrastructure and subscribed to the applicable Service, as described in the applicable Schedule 2, Service Description, appendix. Customer accepts that Service features may not function correctly and Email delivery may be unavailable for domains that are not provisioned. For avoidance of doubt, Schedule 3, Service Level Agreements, shall not apply for domains that are not provisioned per this Clause.
4.4. Customer must ensure that they only accept inbound Email from the Symantec Email Security Services Infrastructure. For the avoidance of doubt, Service Level Agreements will only apply to inbound Email that has been scanned by the Symantec Email Security Services.
4.5. Customer must accept inbound Email from all required IP ranges, as provided by Symantec, to ensure continuity of service in the event that a portion of the Infrastructure is not available. For the avoidance of doubt, Service Level Agreements will only apply to Email that has been scanned by the Symantec Email Security Services.
4.6. For all inbound Email, the IP reputation of the sender is determined using available resources. Email originating from a disreputable source (such as a spammer) will be delayed to reduce the impact on network capacity.
4.7. In order to provide continuity of Service, if a Customer opts to route outbound Email through the Email Security Service, Symantec reserves the right to scan all Email for malicious content, such as Spam. Outbound Emails that are suspected of being Spam will not be accepted by the Email Security Service. When an outbound Email is detected as potential Spam, an SMTP permanent error response will be provided (5xx) to the Customer's MTA; the default behavior of most MTAs is to generate a Non Delivery Receipt (NDR) to inform the sender when a 5xx error response is received. Outbound Emails that are suspected of being Spam will not be included in Email Security Service reporting in the SMC. Track and Trace (defined below) will show that an outbound Email has been detected as Spam and not accepted. Spam Capture Rate and Spam False Positive Service Levels shall not apply to outbound Emails. SYMANTEC IS NOT 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 SPAM.

4.8. Any Customer using Email Security Services must specify the mail server IP address(es) or hostname(s) for the delivery of inbound Emails to their organization, and Customer may specify inbound delivery routes for all provisioned domains, or for specific domains, using the SMC. In addition, 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 provided by Symantec. CUSTOMER AGREES THAT SYMANTEC CANNOT ACCEPT ANY LIABILITY DUE TO THE NON DELIVERY OR MISROUTING OF EMAIL RESULTING FROM ERRORS IN OR OMISSIONS FROM THE PER USER ROUTING CONFIGURATION FILES. Provisioning of Per User Routing may take longer than for other Services, and Clause 8.2 below shall not apply.

4.9. Symantec will attempt to deliver to Customer's configured inbound IP addresses or hostname, as configured in the SMC, periodically for up to seven (7) calendar days. Sender will be notified if the Email could not be delivered. Any undelivered Email is then deleted from the queue.

4.10. The default maximum Email size for the Email Security Services is 50MB. Customer can specify a maximum Email size within the SMC. Any Emails that are received by the applicable Service that exceed the specified limit will be blocked and deleted, and a notification alert Email will be sent to the sender, intended recipient, and an Administrator.

4.11. Customer agrees to provide and maintain a list of specific Email addresses to receive the Service (the "**Validation List**"). It is Customer's responsibility to verify such Validation List prior to the Service being made available and throughout the term of the Agreement. Customer acknowledges that inbound Email sent to Email addresses not specified or incorrectly entered in the Validation List will be blocked automatically. Customer agrees that Symantec is not liable for the failure to deliver of such Email resulting from errors or omissions in the Validation List.

4.12. Customer shall not allow its systems to: (i) act as an Open Relay or Open Proxy; (ii) send or receive Volume Mail originating from Customer, unless Customer has purchased the Volume Mail Service (defined below), in which case Customer may send and receive Volume Mail strictly in accordance with the terms and conditions applicable to that Service; or (iii) send Spam. Symantec reserves the right at any time to review Customer's compliance with this Clause. For the avoidance of doubt, any breach of this Clause 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 Email Security Service.

4.13. Customer may configure a disclaimer message that will be appended to each inbound and outbound Email that is scanned by the Symantec Email Security Services. A default disclaimer will be applied from the time of provisioning the Service, the content of which may be edited by Customer using the SMC. Customer may configure a different disclaimer message for inbound Emails and outbound Emails, either for all Emails or for specific domains and user groups. Only SMC users with Edit Configuration permission for all provisioned domains on the account will be able to configure disclaimer messages.

4.14. Track and Trace. Symantec provides message tracing within the SMC, which allows Customer to locate a specific Email and determine if and when the Email Security Service processed the Email and the action taken. Emails may be available for search within 15 minutes of being accepted by the Email Security Services Infrastructure and remain searchable for thirty (30) calendar days. Email Security Services do not store copies of any Emails that pass through its Infrastructure. Track and Trace is provided as a troubleshooting tool, designed to trace specific Emails, and is not a reporting tool. There are limits to the number of results that can be returned by a single search. Only SMC users with the necessary permissions can access Track and Trace. An Administrator can grant a Track and Trace user role for specific portal users. Track and Trace access is available across all domains that are provisioned for Customer's account.

4.15. The End User Email Quarantine ("Spam Manager"), when requested by Customer and enabled by Symantec, allows Users to manage Emails which are quarantined by the Email AntiSpam.cloud Service. Users may delete or release Emails to the User's selected Email inbox. Users may choose whether the text content of these Emails may be viewed. The Emails in quarantine can be managed by individual Users or by other selected individuals. Users can choose to receive periodic notifications when Email is quarantined by the Service. Emails in quarantine are stored for fourteen (14) calendar days before being automatically deleted. Users can review these Emails without limit during that time. Customer may purchase extended storage if required. In the rare event that the User Quarantine system is not able to accept Email, the Emails will be stored until the End User Email Quarantine is operational. Thereafter Emails will be accessible via the quarantine and, if notification is enabled, will be reported in the next summary notification.

4.16. Customer may request the alternative Email Quarantine ("Message 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 the Email AntiSpam.cloud, Email Image Control.cloud and Email Content Control.cloud Services. 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 the Service to Symantec. An Email may be stored in Message Manager for a maximum of fourteen (14) days, after which it will be deleted automatically. Quarantine storage using Message Manager is limited to 5MB per User, averaged across all Users of Customer. Symantec will monitor usage and in the event that the Customer's quota is exceeded, Symantec may delete message(s), or release message(s) to recipient(s) or administrator. SYMANTEC EXPRESSLY EXCLUDES ANY AND ALL REPRESENTATIONS, CONDITIONS OR WARRANTIES, WHETHER EXPRESS OR IMPLIED, IN RELATION TO MESSAGE MANAGER. Schedule 3, Service Level Agreements, shall not apply to Message Manager.

5. Reporting

5.1. Reporting for each Service will be as available through the SMC for that Service and as defined in Schedule 2, Service Descriptions, below.

5.2. Reporting on the activity of the Email Security Services, Web Services, and the Instant Messaging Security.cloud Service (defined below) and statistics are available through the SMC. Customer may choose to generate reports, through the SMC, which can be configured to be sent by Email on a scheduled basis, or downloaded from the SMC.

6. Planned Maintenance

6.1. "**Planned Maintenance**" means periods of maintenance of which Customer has been given seven (7) calendar days prior notification, posted on the SMC, by Symantec and which may cause disruption of Service due to non-availability of the Service Infrastructure. Symantec will use commercially reasonable efforts to not perform Planned Maintenance between 8am and 6pm, Monday through Friday, in the time zone in which the Infrastructure is located.

6.2. Wherever possible, Planned Maintenance will be carried out without affecting the Service. Planned Maintenance will normally be performed during periods of anticipated low traffic and on part, not all, of the network. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance in order to minimize disruption to the Service.

6.3. Where emergency maintenance is necessary and is likely to affect the Service, Symantec will endeavor to inform the affected parties and will post an alert on the applicable SMC no less than one (1) hour of the start of the emergency maintenance.

6.4. Routine maintenance of SMCs will be performed during off-peak hours to minimize disruption to the availability of the SMC. Symantec will use commercially reasonable efforts to keep these maintenance periods to a maximum of thirty (30) minutes. Customer will not receive prior notification for these maintenance activities.

7. Technical Support

7.1. Technical 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 described in each appendix; and to resolve reported problems with the Service. Additional technical support information may be defined in Schedule 2, Service Descriptions, below.

8. Customer Service

8.1. Symantec will provide customer service during Symantec regional business hours to:

a) Receive and process orders for provisioning the Service;
b) Receive and process requests for modifications to the operational aspects of the Service; and
c) Respond to billing and invoicing questions.

8.2. Unless stated otherwise in the applicable appendix, on receipt of a fully completed and actionable order or Service Change Request, Symantec will use commercially reasonable efforts to provision the Service within five (5) business days, provided that Customer has provided any required information.

9. Service Software License

For each Service in which Service Software is provided to Customer, the EULA accompanying the Service Software shall apply. If no EULA is provided with the Service Software, then the following terms shall apply. This

Clause 9 does not apply to any software which is delivered to Customer as part of an on-premise option, when a Service includes the choice of a cloud-managed or on-premise deployment.

9.1. **Grant of License**. Subject to the terms and conditions of this Agreement, Symantec grants Customer the non-exclusive, non-transferable right to install and use the Service Software solely for Customer's own internal business operations. All intellectual property rights in the Service Software are and shall remain the property of Symantec and/or its suppliers. The Service Software is licensed by Symantec, not sold. Customer acknowledges that the Service Software and all related information, including without limitation Updates, are proprietary to Symantec and its suppliers. Customer shall be responsible and fully liable for each User's compliance with or breach of the terms of this Agreement. Customer shall promptly notify Symantec of any unauthorized use or violation of these terms.

9.2. **Copy and Use Restrictions**. Customer may download and install the Service Software subject to the following conditions:

a) Customer may not download or install the Service Software to more than the number of User licenses licensed by Customer.
b) Customer may copy the Service Software as reasonably necessary for backup, archival or disaster recovery purposes. Printed Documentation may be reproduced by Customer for internal use only. "**Documentation**" means the Symantec's user guides and/or manuals for operation of the Service Software that are included with the Service Software.
c) Customer may not, nor allow any third party to: (i) decompile, disassemble, or reverse engineer the Service Software, except to the extent expressly permitted by applicable law, without Symantec's prior written consent; (ii) remove any product identification or proprietary rights notices; (iii) lease, lend, or use the Service Software for timesharing or service bureau purposes; (iv) modify translate, adapt or create derivative works of the Service Software, or (v) otherwise use or copy the Service Software except as expressly provided herein.

9.3. **Transfer of Rights**. Customer may not transfer, assign or delegate this license under this Agreement without the prior written consent of Symantec. Any such transfer, assignment or delegation in violation of the foregoing shall be void.

9.4. **Limited Warranty and Disclaimer**

a) Symantec warrants that, the Service Software will conform in all material respects to Symantec's current Documentation.
b) The preceding warranty will not apply if: (i) the Service Software is not used in accordance with this Agreement or the Documentation; (ii) the Service Software or any part thereof has been modified by any entity other than Symantec; or (iii) a malfunction in the Service Software has been caused by any of Customer's equipment or third party software.
c) SYMANTEC DOES NOT WARRANT THAT THE OPERATION OF THE SERVICE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. Symantec expressly disclaims all warranties of any kind whether express, implied or otherwise, including but not limited to warranties of merchantability, satisfactory quality, or fitness for a particular purpose.

9.5. **Termination**. Upon termination of the applicable Service or the Agreement, all of Customer's right to use the Service Software granted herein shall immediately cease and Customer shall promptly return to Symantec or destroy all copies of the Service Software and Documentation.

10. Synchronization Tools and APIs

10.1. Schemus Tool. The Schemus Tool is Software that synchronizes data between Customer's directory server and certain Symantec Services. The Schemus Tool is licensed to Customer by Schemus Limited via the EULA accompanying the Schemus Tool download. Customer acknowledges and agrees that access to and use of the Schemus Tool is subject to Customer accepting and complying with the applicable EULA, a copy of which is also available from Symantec upon request. Symantec provides no additional warranties (whether express, implied, statutory or otherwise) with respect to the Schemus Tool. In the event of a failure in respect of the three (3) most current versions of the Schemus Tool, Symantec will use commercially reasonable efforts to help determine the source of the problem and, where applicable, escalate the problem to Schemus Limited. Symantec will use commercially reasonable efforts to provide Customer with thirty (30) calendar days notice through the SMC, or via Email, if Symantec will discontinue use and / or support of the Schemus Tool and the related API. If available, information regarding an alternative synchronization tool will be delivered at the same time. CUSTOMER AGREES THAT SYMANTEC'S MAXIMUM LIABILITY TO CUSTOMER IN RELATION TO THE SCHEMUS TOOL SHALL BE LIMITED TO A SUM EQUAL TO THE GREATER OF THE ACTUAL AMOUNT PAID BY CUSTOMER TO SYMANTEC FOR THE SCHEMUS TOOL OR USD$500.

10.2. Enterprise Vault.cloud CloudLink Option. The CloudLink Option is Software that synchronizes data between Customer's directory server and certain Symantec Services. The CloudLink Option is licensed to Customer under the Service Software License, above.

11. Additional Legal Terms and Conditions

The following terms and conditions are applicable to all Services, and Customer accepts and agrees that:

11.1. Each Service is intended to enable Customer to implement a valid and enforceable computer use policy, or its equivalent. Customer shall comply with all applicable laws with respect to use of the Service(s). 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, Symantec is not liable for Customer's use of the Service(s), nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.

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

11.3. Suggested word lists and template rules or policies supplied by Symantec contain words which may be considered offensive.

11.4. You 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.

11.5. 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.

11.6. Should a Service be suspended or terminated for any reason whatsoever, Symantec shall reverse all configuration changes made upon provisioning the Service and it shall be the responsibility of Customer to undertake all other necessary configuration changes when the Service is reinstated.

11.7. Symantec does not access, read or copy Emails, instant messages, web pages or their attachments other than by electronic methods for the purposes of providing the Service. However, Symantec reserves the right to utilize the Virus, Spam, malware, adware and spyware related content of such Emails, instant messages, web pages and their attachments 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. Where Symantec exercises the rights under this Clause, Symantec will use all commercially reasonable efforts to keep confidential all information received from Customer or sent to Customer in connection with the Service.

11.8. Service Levels will apply to the Services defined in Schedule 3, Service Level Agreement, below, and each predecessor Service, if applicable.

11.9. Symantec will invoice Customer for set-up charges, as applicable, when Customer increases the number of Users, or other incremental use of the Service(s), at the then-current rates.

11.10. Registered Usage may only be increased in increments of ten (10) Users.

11.11. In order to optimize each Service Symantec may, at its discretion and without notice, add, modify or remove features from each Service at any time. Symantec may, in its sole discretion and from time to time, establish or amend general operating practices to maximize the operation and availability of the Service and to prevent abuses. For the avoidance of doubt, such changes will not materially degrade the Service.

Symantec may update these Service Descriptions schedules from time to time to accurately reflect the Service being provided.

11.12. Customer acknowledges and agrees that the remedies set forth in the Agreement are the sole and exclusive remedy for the failure of any Service to perform in accordance with the Agreement.

11.13. Each Service, and any Service Software provided there with, may use open source and other third party materials that are subject to a separate license. Please see the applicable Third Party Notice at http://www.symantec.com/about/profile/policies/eulas/.

12. Renewal Opt-Out Process

The Service renews automatically as set forth in the Agreement referencing these Services Descriptions, unless such renewal is cancelled as follows:

12.1. Customer may opt-out of automatic renewal for Services listed in Appendices 1 – 20 of this Service Description by providing Symantec notice, at least three (3) months prior to the end of Customer's then-current Minimum Period or Renewal Period (each, a "Term"). Customer must submit such notice of opt-out by e-mail to

CLD_cancellations_MLABS@symantec.com, either directly or through the Customer's authorized channel partner. A notice of non-renewal takes effect upon the expiration of the then-current Term. Any notice given according to the above procedure shall be deemed to have been given when received. Cancellation for all other Services shall be as defined in the applicable Service Description appendix.

SCHEDULE 2
SERVICE DESCRIPTIONS

Appendix 1	Symantec Email AntiVirus.cloud
Appendix 2	Symantec Email AntiSpam.Cloud
Appendix 3	Symantec Volume Mail
Appendix 4	Symantec Email Image Control.cloud
Appendix 5	Symantec Email Content Control.cloud
Appendix 6	Symantec Email Boundary Encryption.cloud
Appendix 7	Symantec Policy Based Encryption.cloud
Appendix 8	Symantec Enterprise Instant Messenger.cloud
Appendix 9	Symantec Instant Messaging Security.cloud
Appendix 10	Symantec Web v2 Protect.cloud
Appendix 11	Symantec Web v2 URL.cloud
Appendix 12	Symantec Web v2 Smart Connect.cloud
Appendix 13	Symantec Enterprise Vault.cloud
Appendix 14	AdvisorMail on Symantec.cloud
Appendix 15	Symantec Email Continuity Archive.cloud and Symantec Email Continuity Archive Lite.cloud
Appendix 16	Symantec Email Continuity.cloud
Appendix 17	Symantec Email Archiving.cloud P
Appendix 18	Symantec Web Security Archiving.cloud
Appendix 19	Symantec Endpoint Protection Small Business Edition 2013
Appendix 20	Symantec Backup Exec.cloud

Appendix 1 – Symantec Email AntiVirus.cloud

A. Service Overview

A.1. The Symantec Email AntiVirus.cloud ("Email AV") Service scans inbound and outbound Email and associated attachments for Viruses and phishing Emails.

B. Service Features

B.1. Each Email is scanned by multiple anti-virus technologies.
B.2. For inbound Email, alert notifications may be set up by Customer, to be sent automatically to the intended recipient within Customer's organization, and to an Administrator, if the Service intercepts an Email.
B.3. For outbound Email, alert notifications may be set up by Customer, to be sent automatically to an Administrator, if the Service intercepts an Email.
B.4.. Certain Emails are eligible for automatic release through the SMC, and an Administrator may provide the unique identifier for that Email and release the Email. Certain Emails are not eligible for automatic release through the SMC if Symantec determines that the Email is significantly infectious or damaging. Customer may request release of ineligible Emails, to the intended recipient or to another Email address by contacting Technical Support and submitting a release form. Individual Users will not have access to this quarantine.
B.5. Eligible Emails intercepted by the Service are quarantined and will be available for release for a minimum of seven (7) calendar days. Release can be requested through the SMC.
B.6. Emails Intercepted by the Service will not be returned to the sender.
B.7. Emails intercepted by the Service will not be forwarded to any third party.

C. Customer Responsibilities

C.1. Customer must change configuration settings through the SMC or the Service default settings will apply.

D. Reporting. See Schedule 1, Definitions and General Services Overview.

E. Technical Support. See Schedule 1, Definitions and General Services Overview**.**

F. Additional Terms and Conditions.

F.1 SYMANTEC IS NOT LIABLE FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO INTERCEPT AN EMAIL OR FOR WRONGLY INTERCEPTING AN EMAIL.

Appendix 2 – Symantec Email AntiSpam.Cloud

A. Service Overview

A.1. The Symantec Email AntiSpam.cloud ("Email AS") Service is an inbound Email scanning service designed to detect and reduce Customer's exposure to unsolicited or unwanted Spam Email sent inbound to Customer's Email domain. This Service is only available to Customers who also use the Email AntiVirus.cloud Service.

B. Service Description

B.1. Each inbound Email is scanned using multiple detection methods. Most detection methods can be enabled or disabled by Customer within the SMC. However, certain detection methods within the Connection Manager are not configurable.
B.2. Customer can create private approved and/or blocked senders lists which will be applied to inbound Emails.
B.3. Actions will occur for each inbound Email, identified as Spam by the Service, based on the options set for each detection method within the SMC.
B.4. Customer may enable Sender Policy Framework ("SPF") checking of inbound Email through the SMC. If the sending domain publishes a hard-fail SPF policy and the Email fails the authentication check, the Email will be blocked and deleted. Such blocked and deleted Emails will not be received into the Symantec Email Security Services Infrastructure and cannot be retrieved or quarantined. If the sending domain publishes an SPF policy that is not a hard-fail, or does not publish an SPF policy at all, the SPF check result will be neutral and the Email will not be blocked or deleted.
B.5. For all other inbound Email AntiSpam.cloud detection methods the following options are available for Customer to specify the actions to be taken for inbound Email identified as Spam by the Service:

a) Tag Email within the header;
b) Tag Email within the subject line; (Customer can specify the text to add to Subject lines)
c) Redirect Email to a pre-defined Email address; (which must be on a domain being scanned by the Service)
d) Block and delete Email;
e) Quarantine the Email (if enabled).

B.6. If Customer selects to have the End User Email Quarantine enabled for this Service, Customer may select 'Quarantine the Email' as an action in the event an inbound Email is identified as Spam by the Service. The following options are available within the quarantine:

a) Delete Email;
b) Release Email to original recipient address;
c) Review text of Email.

B.7. Customer may link a number of individual Email addresses to one 'owner' Email address for the purpose of Email aliasing and delegated access. The maximum number of Email addresses that may be linked to a single Email address is fifty (50). Symantec reserves the right to remove Customer's account group or aliasing links in the event that this maximum is exceeded.

C. Customer Responsibilities

C.1. Customer can customize settings for inbound Email through the SMC, or the Service default settings will be enabled for each of Customer's selected domains.

D. Reporting. See Schedule 1, Definitions and General Services Overview.

E. Technical Support. See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions.

F.1. SYMANTEC IS NOT 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 SPAM.

Appendix 3 – Symantec Volume Mail

A. Service Overview

A.1. The Symantec Volume Mail ("Email VM") Service allows Customer to send and receive Volume Mail. Customer who routinely need to send Email to 500 or more recipients, or who routinely expect Email responses from 500 or more Email addresses, where the total of recipients in each thirty (30) calendar day period exceeds 5000 are required to use the Volume Mail Service. This Service is only available to Customer who also use the Email AntiVirus.cloud Service.

B. Service Features

B.1. The Volume Mail must be made up of confirmed, opt-in solicited recipients only.
B.2. The size of each Volume Mail including attachments must not exceed 500 kilobytes.
B.3. The number of recipient Email addresses must not exceed 500 Email addresses per Email.
B.4. Customer may not send or receive Volume Mail in batches of more than 250,000 recipients per calendar day.
B.5. Each Volume Mail Service Band has a maximum quota of permitted recipients per month. Such quotas are not transferable or accumulative and therefore unused recipients cannot be rolled over into subsequent months.

C. Customer Responsibilities.

C.1. Customer must operate an effective list management system including the prompt removal of invalid and subscription cancellation Email addresses.
C.2. Customer must ensure that the disclaimer message appended to outbound Emails shall notify the recipient that the Volume Mail has been Virus scanned.
C.3. Customer shall notify Symantec if at any time its actual Volume Mail usage exceeds the number of recipients per month permitted for Customer's current Band and Symantec shall increase or decrease the charge to the appropriate purchase band in accordance with Symantec's then current price list. Symantec will monitor usage and will inform Customer if limits have exceeded.
C.4. Symantec recommends that Customer select a separate domain from which to send Volume Mail.
C.5. Symantec recommends that Customer stagger the sending of Volume Mail and send Volume Mail outside of local business hours.
C.6. Customer shall, upon Symantec's request and subject to applicable legislation, provide evidence that the Volume Mail must be made up of confirmed, opt-in solicited recipients only and that the Email must not contain Spam.

D. Reporting. See Schedule 1, Definitions and General Services Overview.

E. Technical Support. See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions.

F.1. CUSTOMER AGREES THAT SYMANTEC WILL ENFORCE THAT CUSTOMER MIGRATE TO THE VOLUME MAIL SERVICE IF THE MAIL TRAFFIC PROFILE IS DEEMED DETRIMENTAL TO OTHER CUSTOMERS.
F.2. Customer recognizes and accepts that the sending of Volume Mail is likely to have a varying effect on the flow of Email traffic. Such effects are outside of the control of Symantec and for this reason the Service Availability and Latency Service Levels set out in the Service Level Agreement shall not apply to Volume Mail. The Email AntiVirus.cloud and Email AntiSpam.Cloud SLAs still remain.
F.3. 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 Appendix, 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.
F.4. Volume Mail is assessed on the number of recipients. A Customer which sends one Email to 1000 recipients is considered the same as a sending the same Email one thousand times - both are deemed as Volume Mail under this Service.
F.5. Volume Mail can be both outbound and inbound.
F.6. Where a Customer's Volume Mail usage is found to exceed their specified banding, a surcharge will be levied on their excess usage, per every additional 1,000 Email recipients.
F.7. The upper Service band has a maximum of 1,000,000 recipients per month. Where a Customer has requirements that exceed this usage then Symantec will need to further qualify the operational feasibility of supporting this usage.

F.8. The Volume Mail Service is billed quarterly in advance.
F.9. There is no minimum term applicable to the Volume Mail Service and either party may cancel at any time upon three (3) months notice.

Appendix 4 – Symantec Email Image Control.cloud

A. Service Overview

A.1. The Symantec Email Image Control.cloud ("Email IC") Service is a scanning service which scans Customer's inbound and outbound Email to detect pornographic images. This Service is only available to a Customer who also use the Email AntiVirus.cloud Service.

B. Service Features

B.1. The Service will be enabled for each Customer's chosen domains.
B.2. Email will be scanned using image composition analysis technology for pornographic images.
B.3. The Service can only scan for pornographic images in certain file types which are defined in the administration guide and the online help provided with the Service.
B.4. Actions and notifications will occur per each Email identified by the Service, as containing a pornographic image, based on the options set by Customer through the SMC.
B.5. The following options are available for Customer to specify the actions to be taken when the Service identifies an Email as containing a pornographic image. These options may be set independently for inbound and outbound Email:

a) Log Email (provides statistics viewable via the SMC;
b) Tag Email within the header (for inbound Email only);
c) Tag suspected Email in the subject line (for inbound Email only);
d) Copy Email to a pre-defined Email address;
e) Redirect Email to a pre-defined Email address;
f) Block and delete Email.

B.6. Customer may identify approved Email senders or recipients for the administration of the Service, through the SMC, and the Email of such senders and recipients will not be scanned by the Service.
B.7. Customer may identify specific approved or blocked images, through the SMC. Approved images will not be blocked by the Service.

C. Customer Responsibilities

C.1. Customer must set the configuration options for each domain receiving the Service, through the SMC, or the default settings for the Service will apply.

D. Reporting. See Schedule 1, Definitions and General Services Overview.

E. Technical Support. See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions

F.1. Customer acknowledges that the identification of a pornographic image is subjective based on the automated scanning technology.
F.2. The Service may not be able to scan attachments with content which is under the direct control of the sender, such as, password protected and/or encrypted attachments.
F.3. Under no circumstances should illegal images be sent to Symantec. Customer should contact their local law enforcement agency for advice on dealing with such images.
F.4. SYMANTEC IS NOT LIABLE FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO IDENTIFY A PORNOGRAPHIC IMAGE OR FOR WRONGLY IDENTIFYING AN IMAGE AS PORNOGRAPHIC.

Appendix 5 – Symantec Email Content Control.cloud

A. Service Overview

A.1. The Symantec Email Content Control.cloud ("Email CC") Service is a scanning Service that allows Customer to configure its own rule-based Email filtering strategy. This Service is only available to a Customer who also use the Email AntiVirus.cloud Service.

B. Service Features

B.1. Customer can build a set of rules upon which incoming and outgoing Email is filtered by the Service.
B.2. A rule is an instruction set up by Customer which is used to identify a particular format of message/attachment or content within an Email. The rule will determine the action to be taken when that format is present in an Email.
B.3. Customer may configure rules on a 'global', 'per domain' or 'per group' basis.
B.4. The Service works on an exact match of Customer rules and will apply all rules until it determines an exit event and completes the scanning..
B.5. The Service can only scan for content in certain file types which are defined in the administration guide and the online help provided with the Service.
B.6. The following options are available for Customer to specify the actions to be taken when the Service identifies an Email as matching a Customer defined rule. These options may be set independently for inbound and outbound Email:

a) Block and delete Email (exit event);
b) Tag (if inbound) and redirect Email to a specified administrator (exit event);
c) Tag (if inbound) and copy Email to a specified administrator;
d) Tag (if inbound) header of Email;
e) Compress Email attachments;
f) Log only to the SMC statistics;
g) Tag in the subject line;
h) Route to a specific IP address or host name;
i) Log and Exit (exit event).

B.7. Customer can activate, deactivate and modify notifications configured by Customer on a per rule basis through the SMC.

C. Customer Responsibilities

C.1. Customer is responsible for implementing the configuration options for the Service for each domain, through the SMC.
C.2. Customer must implement rules in a logical hierarchy, otherwise, a rule may not be applied before the Service reaches Customer selected exit event.

D. Reporting. See Schedule 1, Definitions and General Services Overview.

E. Technical Support. See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions

F.1. Customer recognizes that if the Service is used in conjunction with the quarantine action of the Email AntiSpam.Cloud Service, this may result in an Email being quarantined before it has been filtered by the Service.
F.2. SYMANTEC IS NOT LIABLE FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO CORRECTLY IDENTIFY CONTENT OR FOR WRONGLY IDENTIFYING CONTENT.

Appendix 6 – Symantec Email Boundary Encryption.cloud

A. Service Overview

A.1. The Symantec Email Boundary Encryption.cloud ("Email BE") Service provides encrypted communication channels for Customer to communicate with selected third parties. This Service is only available to Customer who also use the Email AntiVirus.cloud Service.

B. Service Features

B.1. The Service is based on the standard 'SMTP over TLS' (Simple Mail Transfer Protocol over Transport Layer Security).

B.2. Customer can form a Secure Private Email Network (SPEN) with selected third parties ("SPEN Partners"). This configuration is commonly known as "Enforced" encryption.

B.3. Customer may also configure its Email servers for the "Secure Connect" model of the Service, and the following shall apply:

a) Email exchanges between Symantec and Customer's Secure Connect mail servers shall be secured by TLS encryption. Whether onward routing will be performed in unencrypted or encrypted format will depend on (i) Customer specified TLS enforcements and (ii) destination server capability to receive Emails over Opportunistic TLS.

B.4. If Customer is using the Service in conjunction with the Policy Based Encryption.cloud Service, Customer must implement the Secure Connect model of the Service on all of its mail servers.

B.5. Certificates and Authentication:

a) Where Customer originates a TLS connection, the accepting mail server must provide its certificate for authentication. If the accepting mail server requests to authenticate the Service, then Symantec will supply its client certificate for authentication. If the accepting mail server cannot be authenticated, the Email will be returned to Customer.

b) Where an external mail server originates a TLS connection, the Service will supply its server certificate for authentication, but will not require that the external mail server supply its client certificate for authentication.

c) The validation of any certificate is based upon the Certificate Authority that has signed the certificate. For each certificate submitted by a remote mail server as part of a TLS connection, the Service will validate that a recognized Certificate Authority has signed the certificate. If a certificate cannot be validated against a recognized Certificate Authority the connection will be abandonded and the Email will be returned to the sender. A list of recognized Certificate Authorities is available upon request.

C. Customer Responsibilities

C.1. Customer must define SPEN Partners by domain. SPEN Partners do not have to be a Customer of the Email Boundary Encryption.cloud Service, however Symantec will not support non-Email Boundary Encryption.cloud Customer SPEN Partners directly.

C.2. Both Customer's and the SPEN Partner's mail server must support TLS to enable use of the Service.

C.3. Customer must add SPEN Partner domains to an approved senders list when also using the Email AntiSpam.Cloud Service. Otherwise, in certain circumstances involving unavailability of the local signaturing system, Email may be redirected to a remote signaturing system via a public network.

D. Reporting.

See Schedule 1, Definitions and General Services Overview.

E. Technical Support.

E.1. Customer Support response times defined in Schedule 1 shall not apply to provisioning of this Service.

F. Additional Terms and Conditions

F.1. Symantec is not liable for the failure of Customer or any third party (including without limitation any SPEN Partner) to fulfill their obligations with regard to registering certificates, or for the timeliness or accuracy of such information.

F.2. A CUSTOMER ACKNOWLEDGES THAT IF THE SECURE CONNECT MODEL IS APPLIED THEN ONLY SERVERS REGISTERED IN 'OUTBOUND ROUTES' WILL BE ENFORCED OVER TLS; SERVERS NOT CONFIGURED IN THIS SECTION MAY NOT HAVE TLS ENFORCED.

Appendix 7 – Symantec Policy Based Encryption.cloud

A. Service Overview

A.1. The Symantec Policy Based Encryption.cloud ("Email PBE") Service provides the ability to send and receive encrypted Emails. Email PBE is only available to Customer who also use both of the Email Boundary Encryption.cloud and Email Content Control.cloud Services. Each individual Policy Based Encryption.cloud User also must be an Email Content Control.cloud User.

B. Service Features

B.1. Customer must use Email Content Control.cloud to define outbound encryption policies for Emails.
B.2. Customer can configure the encryption method to be either Push or Pull. For Symantec Policy Based Encryption.cloud (Z) ("PBE Z"), the Email Content Control.cloud policy decides between Push and Pull. For Symantec Policy Based Encryption.cloud (E) ("PBE E"), the default encryption method is Pull but can be changed to Push by the recipient, if this configuration is selected by the sender.

a) The "PBE Push" variant of the Policy Based Encryption.cloud Service sends the recipient an Email notification with the original Email saved within it as an encrypted attachment. Following initial registration online, for the Policy Based Encryption.cloud (E) Service, the recipient is able to view the decrypted Email offline using a secure reader.
b) The "PBE Pull" variant of the Service sends the recipient an Email notification. The recipient is able to view the decrypted Email online via a secure SSL session in their browser when they log on to a secure web portal and enter their password.

B.3. Customer may customize a portion of the portal that recipients use to read the encrypted Emails, or the default Service settings will apply.
B.4. The recipient of an encrypted Email may also send an encrypted Email to any of Customer's Email PBE Users.
B.5. If Customer subscribes to the Service, a third party Microsoft Outlook® Plug-In can add an "encrypt" icon to the recipient's Microsoft Outlook® toolbar. Customer may choose to use this plug-in at its own discretion. Symantec does not directly support, nor accept any responsibility for the plug-in.
B.6. The following limitations apply to Email PBE:

a) The number of secure Emails Customer may send in any month using Policy Based Encryption.cloud (Z) may not exceed three hundred (300) times the number of Users of the Service.
b) The number of secure Emails Customer may send in any month using Policy Based Encryption.cloud (E) may not exceed four hundred and eighty (480) times the number of Users of the Service.
c) 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 month, Symantec reserves the right to invoice Customer accordingly.
d) Emails routed through the Policy Based Encryption.cloud (Z) Service are limited to a maximum size of fifty megabytes (50 MB) per Email when compressed. Emails routed through the Policy Based Encryption.cloud (E) Service are limited to a maximum size of fifty megabytes (50 MB) per Email post-encryption.

C. Customer Responsibilities

C.1. Customer is responsible for implementing the configuration options for the Service, through the SMC.
C.2. Customer may request customization of eligible portions of the portal, that recipients use to read the encrypted Email, a maximum of two times per 12 month period.

D. Reporting.

See Schedule 1, Definitions and General Services Overview.

E. Technical Support.

E.1. Customer Support response times defined in Schedule 1 shall not apply for provisioning of the Service.

F. Additional Terms and Conditions

F.1. The Email Latency service level in the Service Level Agreement shall not apply to this Service.
F.2. SYMANTEC IS NOT LIABLE FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM THE FAILURE OF THE SERVICE TO ENCRYPT EMAIL.

Appendix 8 – Symantec Enterprise Instant Messenger.cloud

A. Service Overview

A.1. The Symantec Enterprise Instant Messenger.cloud ("EIM") Service allows for administrative control, centralized storage, and domain management of instant messages.

B. Service Features

B.1. Each version of the Service described below allow the User to securely connect to the Service platform and to use the Service.

B.2. With the exception of MSI and Java versions, the Service client (the "POD" or "Service Software") is installed on each User's work station. The POD has the following functionality:

a) File sharing;
b) Secure instant messaging conferencing;
c) Interoperability with public instant messaging networks (with CONNECT package only).

B.3. The SMC allows defined Administrators to manage their domain structure and User base.

B.4. **Symantec Enterprise Instant Message.cloud Communicate.cloud ("COMMUNICATE") Option**

a) Integrated file sharing (100mb capacity per User);
b) Desktop back-up solution;
c) Ability to share information with Instant Messaging Security.cloud Users that are online or offline;
d) Access control lists;
e) Secure, 168-bit 3DES SSL encrypted POD-to-POD communications;
f) Web-based administration console;
g) Comprehensive user options interface;
h) Advanced presence detection and tracking;
i) Support for a wide variety of proxy servers;
j) HTTP tunneling capabilities;
k) Alert notifications for new files;
l) Object oriented file system with search capabilities.

B.5. **Symantec Enterprise Instant Message.cloud Connect.cloud ("CONNECT") Option**

All features in the COMMUNICATE package apply with the addition of the following:

a) Interoperable Instant Messenger (AOL®, MSN®, Yahoo! ®);
b) SMS messaging (2 messages per User, or "User Quota");
c) Instant Messaging log capabilities.

B.6. Customer may choose to log instant messages that pass through the Service.

B.7. Symantec retains logs for a period of 3 years, after which time the logs are permanently deleted. Customer may submit a written request to obtain (i) a copy of such logs or (ii) the deletion of such logs, at any time prior to the expiry of such 3 year retention period.

C. Customer Responsibilities

C.1. Customer is responsible for all uses of the administration web site, whether or not authorized by Customer and Customer is responsible for maintaining the confidentiality of Customer's account login and passwords. Customer agrees to notify Symantec immediately of any unauthorized use of Customer's account.

D. Reporting.

See Schedule 1, Definitions and General Services Overview.

E. Technical Support.

See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions.

F.1. Customer acknowledges that Symantec may charge an additional fee for instant message logs which are more than one (1) year old.

F.2. Customer acknowledges that the SMC permits Customer to disable logging by group or sub-group at any time and therefore the logs may not provide a complete record of its use of the Service.

F.3. Upon termination of the Service for any reason, Customer may request the return or deletion of its logs. If Customer does not determine its preference within ninety (90) calendar days of termination, Symantec shall permanently delete the logs.

F.4. Symantec cannot act as a third party downloader in any event for the purposes of US SEC regulations.

F.5. Customer will receive interoperability functionality as set forth in this appendix (see CONNECT package above). Symantec makes no warranties or guarantees around the ability of the Service to interoperate with any IM provider, including but not limited to, AOL®, MSN® and Yahoo!®.

F.6**. Acceptable Use Policy.** Customer agrees that it will not:

a) Transmit or store via the POD or the Service any data, text, video, audio, software, or other content that is illegal;
b) Transmit or store via the POD or the Service any content that infringes any patent, trademark, copyright, rights of publicity, or other intellectual property right;
c) Transmit or store any content that violates any applicable local, state, national, or international law that could give rise to civil or criminal liability;
d) Transmit or store any unsolicited promotional content, advertising materials, Spam, “spim,” chain-letters, or other such solicitation;
e) Use the POD or the Service to publicly broadcast, transmit, or display content other than for the purposes of company communications;
f) Use the POD or the Service to intentionally transmit content which includes a Virus, worm, cancelbot, time bomb, Trojan-horse, sniffer, or other code designed to acquire information about other users or disrupt the functionality or availability of any computer program, database, the Service or any other Internet host; or
g) Disguise the POD User’s identity by spoofing, forging headers, using third-party relayers, or otherwise obscuring the origin of transmitted content, including without limitation impersonating another person or entity.

F.7. CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA.

Appendix 9 – Symantec Instant Messaging Security.cloud

A. Service Overview

A.1. The Symantec Instant Messaging Security.cloud ("IMS") Service scans instant messages and attachments for malware, malicious URL links, and inappropriate content, and allows Customer to log each message.

B. Service Features

B.1. Once the Service has been configured by Customer, instant messages passing from supported UC and IM platforms are directed through the Service for scanning.
B.2. The Service is only able to scan certain versions of UC and IM clients. A list of currently supported versions can be obtained by contacting Technical Support. Customer acknowledges and accepts that Symantec may update and change this list without notice.
B.3. If an Instant Message:

a) Is deemed to contain a Virus or other malicious code, it shall be blocked;
b) Contains a URL for a webpage where a Virus or other malicious code has been detected, it shall be blocked.

B.4. Instant Messaging Security.cloud is able to scan attachments for malicious code.
B.5. **Instant Messaging Security.cloud Content Control ("IMS CC")**
B.5.1. Customer may configure its own rule based content filtering strategy for incoming and outgoing instant messages through the SMC.
B.5.2. Rules may be configured on a group or individual basis.
B.5.3. Options are available for defining the action to be taken upon detecting controlled content within an instant message. These options are detailed on the SMC and in the current version of the Administrator's guide.
B.5.4. The Service can scan attachment filenames, however, it is unable to scan the body of an attachment.
B.6. **Logs and Storage**
B.6.1. If Customer has enabled the logging functionality, Symantec shall compile daily logs of instant messages scanned. Each log shall include date and time stamps, content, and names of files transferred. Any logs that are unable to pass to Customer shall be stored for a period of thirty-one (31) calendar days and then destroyed.
B.6.2. Customer may also configure the Service to send a copy of each instant message to a designated Email address, through the SMC.
B.7. **Notifications**
B.7.1. Customer may configure the Service to send an automatic notification to the sender and intended recipient in the event that an instant message is blocked because it is deemed to contain a Virus, Phishing attack, malicious URL or controlled content.

C. Customer Responsibilities

C.1. Customer can customize setting options though the SMC, or the Service default settings will apply.
C.2. Customer is required to synchronize its user directory with Symantec in order to create a list of Active Directory usernames and corresponding instant message usernames within the SMC. An "Internal User" is either a supported public instant message User or a supported UC User who connects to Instant Messaging Security.cloud from a Customer provisioned IP address, or a roaming user who connects to Instant Messaging Security.cloud with a Customer's provisioned SIP domain. An "External User" is anyone who does not meet the above criteria.

D. Reporting. See Schedule 1, Definitions and General Services Overview.

E. Technical Support. See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions

F.1 SYMANTEC IS NOT LIABLE FOR ANY LOSS OR DAMAGE RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO DETECT SPIM, VIRUSES, PHISHING ATTACKS, MALICIOUS CODE, BLOCKED URLs OR CONTROLLED CONTENT, OR FOR THE SERVICE WRONGLY IDENTIFYING INSTANT MESSAGES AS CONTAINING SPIM, VIRUSES, PHISHING ATTACKS, MALICIOUS CODE, BLOCKED URLs OR CONTROLLED CONTENT.
F.2. CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA

Appendix 10 – Symantec Web v2 Protect.cloud

A. Service Overview

A.1. The Symantec Web v2 Protect.cloud ("Web v2 Protect") Service digitally examines Web pages and attachments for viruses, malicious code, spyware, and/or adware.

B. Service Features

B.1. Customer's external HTTP and FTP-over-HTTP requests, including all attachments, macros or executables, can be directed through the Service.
B.2. Access to the Service is restricted via Scanning IP (i.e. the IP address(es) from which Customer's web traffic originates). The Scanning IPs are also used to identify Customer and dynamically select Customer-specific settings.
B.3. The Service will scan relevant elements of the Web page and its attachments that may contain Viruses, malicious code, spyware, and/or adware. It may not be possible to scan certain Web pages, content or attachments (for example, an item that is password protected). Attachments specifically identified as unscannable will not be blocked. Streamed and encrypted traffic (i.e. streaming Media and/or HTTPS/SSL) cannot be scanned and will be passed through the Service without being scanned, unless Customer has enabled HTTPS scanning through the SMC.
B.4. If Customer's Web page, Web page component, or attachments are found to contain an item identified as a Virus, spyware or adware, then access to that Web page, or a portion of that Web page, is denied and the User will be redirected to an automatic alert Web page.
B.5. Roaming User Support is an optional feature which extends the Service to Users who are not located within the corporate network. Customer must install a PAC file onto the User's PC so that the User is pointed to Service web portal when the browser is accessed. To access the web portal, the User must enter a user name and password. A PAC file template can be downloaded from the SMC and modified by Customer.

C. Customer Responsibilities

C.1. Customer must direct selected domains through the Service, configured through the SMC.
C.2. Customer may select settings, configured through the SMC, or default settings for the Service will apply.
C.3. Customer is responsible for ensuring that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed through the Service.
C.4. Where Customer has Internet services that mandate a direct connection rather than via a proxy, it is the responsibility of Customer to make the necessary changes to its own Infrastructure to facilitate the Service.
C.5. Customer may edit a portion of the automatic alert Web page(s) through the SMC.

D. Reporting

D.1. Reporting on the activity of the Service is provided through the SMC.
D.2. To enable per User or group reporting, Customer will be required to install the relevant Service Software (the "Client Site Proxy") in accordance with the installation guidelines provided with the Service.
D.3. Detailed reporting data is only stored on the SMC for a maximum period of forty (40) calendar days. The summary reporting data is available for a maximum period of twelve (12) months.
D.4. Customer may purchase an extended reporting period for the detailed reporting data of up to a maximum of six (6) months.

E. Technical Support. See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions

F.1. Customer's web traffic when using the Service shall not exceed thirty megabytes (30MB) per User per calendar day (calculated as an average per User across Customer's total Registered Usage for the Service).
F.2. SYMANTEC IS NOT LIABLE FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO DETECT VIRUSES, MALICIOUS CODE, SPYWARE OR ADWARE.

Appendix 11 – Symantec Web v2 URL.cloud

A. Service Overview

A.1. The Symantec Web v2 URL.cloud ("Web v2 URL") Service allows Web pages and attachments to be digitally examined based on configuration settings selected by Customer.

B. Service Description

B.1. Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through the Service. HTTPS requests will be scanned through the Service if the HTTPS scanning is enabled by Customer through the SMC.
B.2. Access to the Service is restricted via Scanning IP (i.e. the IP address(es) from which Customer's web traffic originates). The Scanning IPs are also used to identify Customer and dynamically select Customer-specific settings.
B.3. Customer is able to configure the Service to create granular policy rules through the SMC.
B.4. If Customer's Web page, Web page component, or attachments are restricted by Customer selected policy, then access to that Web page, or a portion of that Web page, is denied and the User will be redirected to an automatic alert Web page.

C. Customer Responsibilities

C.1. Customer may select settings, configured through the SMC, or default settings for the Service will apply.
C.2. Customer must direct its external traffic through the Service, configured through the SMC.
C.3. Customer should ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed through the Service.
C.4. Where Customer has Internet services that mandate a direct connection rather than via a proxy, it is the responsibility of Customer to make the necessary changes to its own Infrastructure to facilitate the Service.
C.5. Roaming User Support is an optional feature which extends the Service to Users who are not within the corporate network. Customer must install a PAC file onto the User's PC so that the User is pointed to Symantec's Web portal when the browser is accessed. To access the Web portal, the User must enter a user name and password. A PAC file template can be downloaded from the SMC and modified by Customer.
C.6. Customers may edit a portion of the automatic alert Web page(s) through the SMC.
C.7. Customer's web traffic when using the Service shall not exceed thirty megabytes (30MB) per User per calendar day (calculated as an average per User across Customer's total Registered Usage for Web v2 URL.cloud Service). In the event such daily limit is exceeded, Symantec reserves the right to:

a) Withhold provision of or suspend all or part of the Service immediately and until such excess use is remedied; or
b) Require Customer to purchase additional Users to reflect Customer actual Web traffic usage for the applicable term of Service.

D. Reporting

D.1. Reporting on the results of a Customer's access restriction policy rules is provided through the SMC.
D.2. To enable per User or group administration and reporting, Customer will be required to install the relevant Service Software application (the "Client Site Proxy") in accordance with the installation guidelines provided with the Service.
D.3. Detailed reporting data is only stored on the SMC for a maximum period of forty (40) calendar days. The summary reporting data is available for a maximum period of twelve (12) months.
D.4. Customer may purchase an extended reporting period for the detailed reporting data of up to a maximum of six (6) months.

E. Technical Support.

See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions

F.1. SYMANTEC IS NOT LIABLE FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO DETECT BLOCKED URLs OR CONTENT.

Appendix 12 –Symantec Web v2 Smart Connect.cloud

A. Service Overview

A.1. The Symantec Web v2 Smart Connect.cloud ("SmartConnect") Service allows Users who are not directly connected to Customer network to use either, or both of the Web v2 Protect.cloud and Web v2 URL.cloud Services. This Service is only available to Customers who also use the Web v2 Protect.cloud, and/or the Web v2 URL.cloud Services.

B. Service Features

B.1. When the User connects to the Internet in designated 'in service' countries, Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through the Web v2 URL.cloud and Web v2 Protect.cloud Service(s), as applicable, as a result of being redirected by the Service Software ("Web Roaming Agent"). HTTPS requests will be scanned through the Service if the HTTPS scanning is enabled by Customer through the SMC.
B.2. Access to the Web v2 URL.cloud and Web v2 Protect.cloud Services is restricted to authorized systems that contain a valid version of the Service Software, as well as authorized Users who are activated for these Services in the SMC. The Service Software and authorized User information is used to identify Customer and dynamically select Customer-selected settings.
B.3. Policy rules for the Web v2 URL.cloud and Web v2 Protect.cloud Services will be the same when a User is connected via a configured network location.

C. Customer Responsibilities

C.1. Customer must determine and maintain the configuration settings required to direct this external web traffic to the Service Software, as well as to forward traffic outbound to the Web v2 URL.cloud and Web v2 Protect.cloud Services, as applicable.
C.2. Customer must install a PAC file onto each User's PC so that the browser is pointed to the Service Software when the browser is accessed. A PAC file template can be downloaded from the SMC and modified by Customer.
C.3. Customer is responsible for ensuring that the internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed to the Service Software.

D. Reporting. See Schedule 1, Definitions and General Services Overview.

E. Technical Support. See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions

F.1. Customer or Partner shall not, and shall not permit any third party to, sell, resell, export, re-export, transfer, divert, distribute, dispose of, disclose or otherwise deal with the Controlled Technology, directly or indirectly, to any of the following countries: Afghanistan, Angola, Armenia, Azerbaijan, Bosnia and Herzegovina, Burma, Burundi, China, Cuba, Democratic Republic of Congo, Eritrea, Ethiopia, Iran, Iraq, North Korea, Liberia, Libya, Nigeria, Rwanda, Sierra Leone, Somalia, Sudan, Syria, Tanzania, Uganda and Zimbabwe.
F.2. Customer shall not transfer the Service Software to any third party, or to any individual that is not an employee of Customer except that: (i) Customer may transfer to or enable the download of the Service Software by its third party subcontractors for use on Customer's behalf; provided that Customer makes such third parties aware of the obligations in this Clause.
F.3. Customer acknowledges that the Service Software will be provisioned with Symantec's default settings applied which includes using reasonable efforts to route the User's web traffic to an 'optimal' Service Infrastructure access point. This routing is based on an understanding of the User's location based on IP address. The routing is done independently of any assessment of the likely performance for the individual end User's connection and only for those countries which Symantec is deemed capable of providing an acceptable level of Service.
F.4. For any other country outside of the acceptable service countries, Customer acknowledges that Symantec will not be able to provide the Service capabilities. If Symantec determines that the User is located in a 'non-service' country, the Service will not be available to the User. A current list of acceptable service countries is located at: http://images.messagelabs.com/EmailResources/ServiceAdminGuides/WebRoamingAgent/SmartConnect_NoServiceCountries.pdf.
F.5. CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA.

Appendix 13 – Symantec Enterprise Vault.cloud

A. Service Overview

A.1. Symantec Enterprise Vault.cloud ("EV.cloud") Service is the collective name for the archiving services and options described in this appendix. Customers must purchase each Service and add-on Services separately.

B. Service Features

B.1. Each service within the Enterprise Vault.cloud Service offering are compatible only with approved versions of on-premise mail servers and hosted mail services set forth in the current Compatibility List. The Compatibility List is located at: http://www.symantec.com/docs/TECH191408.

B.2. Customers may export data from the Enterprise Vault Discovery.cloud Service. For an additional fee, Symantec will export data from Enterprise Vault.cloud and transfer that data to Customer via courier. Data will be transferred to Customer encrypted if requested.

B.3. The following applies to both the Symantec Enterprise Vault Personal.cloud and Symantec Enterprise Vault Discovery.cloud Services:

a) The maximum single Email size that can be ingested by Enterprise Vault Personal.cloud and Enterprise Vault Discovery.cloud is 50MB unless otherwise specified in this appendix.
b) Neither Service replaces Customer's need to backup Customer's mail server(s). In the event that Customer needs to rebuild a mail server, it should rebuild the mail server from backup data rather than from the archive.

B.4. **Services and Options**

B.4.1. **Symantec Enterprise Vault Personal.cloud**

The Enterprise Vault Personal.cloud Service is an Email archiving service designed to give a User access to their own personal Email archives.

a) The Service stores and indexes Emails and attachments, and BlackBerry® messages (SMS text, PIN-to-PIN, call log, if Symantec Enterprise Vault.cloud BlackBerry® Option is added) in the archive.
b) Users can also access the archive from Microsoft Outlook® or Microsoft Outlook® Web App (where supported), IBM Lotus Notes®, BlackBerry® devices and through a browser-based, secure website.

B.4.2. **Symantec Enterprise Vault Discovery.cloud**

The Enterprise Vault Discovery.cloud Service is an Email archiving service designed to expedite specific topic or discovery (eDiscovery) requests, enforce Email use policies and to retain data for customer defined periods.

a) The Service stores and indexes Emails and attachments, and BlackBerry® messages (SMS text, PIN-to-PIN, call log, if Symantec Enterprise Vault.cloud BlackBerry® Option is added) in the archive.
b) Users can access the archive through a browser-based, secure website.

B.4.3. **Symantec Enterprise Vault.cloud BlackBerry® Option**

The Enterprise Vault.cloud BlackBerry® Option is an add-on Service to the Enterprise Vault Personal.cloud Service that allows Users to access and search archived Emails, attachments, SMS, PIN-to-PIN messages and call log files from their BlackBerry® devices. The Enterprise Vault.cloud BlackBerry® Option can be deployed by Administrators to Users from a BlackBerry® Enterprise Server (BES) or by Users via BlackBerry® Desktop Manager. Download and installation of Service Software is required for the BlackBerry® Option.

B.4.4. **Symantec Enterprise Vault.cloud Import Option**

The Symantec Enterprise Vault.cloud Import Option is an add-on Service to the Enterprise Vault Personal.cloud or Enterprise Vault Discovery.cloud Services that allows Customer to migrate and ingest existing legacy Email data into Customer's archive. This add-on Service allows Customer to combine both ingested legacy Email and new Email streams within the archive.

a) This add-on Service requires active participation by Customer to plan, analyze and execute an ingestion plan.
b) Customer must transfer Email data to be ingested via courier. All data should be provided in an encrypted form and Customer must provide the decryption key, per instructions from Symantec.
c) Customer can extract the data and provide it in any compatible format from supported repositories.
d) With Customer's guidance, this add-on Service assigns Users to each Email imported. Email that cannot be directly assigned to a specific User are archived into a single mailbox within the archive.
e) All migration activity can be logged and audited to provide integrity of Customer's Email records.
f) The maximum size for an Email to be ingested is 50MB.
g) Symantec cannot guarantee the time it will take to import the data once received.
h) Symantec is not responsible for failure to import data that is corrupt when received from Customer.

B.4.5. **Symantec Enterprise Vault.cloud for Box®**

Symantec Enterprise Vault.cloud for Box® is an add-on Service to the Enterprise Vault Personal.cloud or Enterprise Vault Discovery.cloud Services for files stored on enterprise www.Box.com accounts. This add-on Service allows Customers to map Box® users to the archive by Email address. This add-on Service collects files and securely transmits them in Email to the archive. Files may then be searched and accessed during the eDiscovery process or for individual use. Administrators can select any combination of compatible file types.

B.4.6. **Symantec Enterprise Vault.cloud for Salesforce Chatter®**

Salesforce Chatter® is an add-on service to Enterprise Vault.cloud.Symantec Enterprise Vault.cloud for Salesforce Chatter® is a cloud-based service designed to archive posts from Salesforce Chatter®. Salesforce Chatter® captures and indexes Salesforce Chatter® content in Enterprise Vault Personal.cloud and Enterprise Vault Discovery.cloud. From either Enterprise Vault Personal.cloud or Enterprise Vault Discovery.cloud, Customer can search across content directly and from Enterprise Vault Discovery.cloud users can export search results for further review and analysis.

B.4.7. **Symantec Enterprise Vault.cloud for Microsoft SharePoint®**

Symantec Enterprise Vault.cloud for Microsoft SharePoint® is a cloud-based service designed to archive documents from Microsoft SharePoint® Server on-premise. Microsoft SharePoint® captures and indexes SharePoint® content in Enterprise Vault Discovery.cloud. From Enterprise Vault Discovery.cloud, Customer can search across content directly and export search results for further review and analysis. Microsoft SharePoint® is an add-on service to Enterprise Vault Discovery.cloud.

B.4.8. **Symantec Enterprise Vault.cloud Folder Sync Option**

The Symantec Enterprise Vault.cloud Folder Sync Option is an add-on Service to the Enterprise Vault Personal.cloud Service which enables a Customer to view Emails in Enterprise Vault Personal.cloud in a manner similar to the Email organization in the User's Microsoft Outlook® folders. As Users move Emails between Microsoft Outlook® folders and create and move the location of Microsoft Outlook® folders, the synchronization feature subsequently replicates the folder structure inside Enterprise Vault Personal.cloud. Download and installation of Service Software is required for the Folder Sync Option.

B.4.9. **Symantec Enterprise Vault Mailbox Continuity.cloud**

Symantec Enterprise Vault Mailbox Continuity.cloud is a Service that allows Users to access their Email via a dedicated folder in Microsoft Outlook® or a web-based User interface during a failure of the main Email server platform ("Continuity Event"). This Service requires Customer to use at least one of the Symantec Email Security Services.

a) Customer agrees to configure the Service as a failover delivery route with the SMC and to further inform Symantec of the delivery location (mailhost name or IP address) by domain of its mail servers at commencement of this Service. Customer acknowledges and agrees that it has an ongoing obligation to update Symantec, during its use of the Service, of any changes to such delivery location. Customer acknowledges that Customer's failure to make such configurations or to provide Symantec with such delivery information may adversely impact the performance of the Service.
b) IF SYMANTEC IS UNABLE TO ESTABLISH AN SMTP CONNECTION TO CUSTOMER, CUSTOMER'S EMAILS WILL BE ROUTED TO THE SERVICE ON BEHALF OF CUSTOMER. FOR THE AVOIDANCE OF DOUBT: (I) IF CUSTOMER'S FIREWALL ACTS AS A PROXY AND RESPONDS ON BEHALF OF THE MAIL SERVER, OR (II) IF CUSTOMER'S MAIL SERVER ISSUES ANY RESPONSE (INCLUDING WITHOUT LIMITATION ERROR CODES), THIS WILL CONSTITUTE AN SMTP CONNECTION AND WILL NOT BE A CONTINUITY EVENT.
c) The Service uses an opportunistic TLS connection when attempting Email delivery. ALL EMAIL BOUNDARY ENCRYPTION.CLOUD AND POLICY BASED ENCRYPTION.CLOUD SERVICE CUSTOMERS ALSO USING THE SERVICE ACKNOWLEDGE AND AGREE THAT A TLS CONNECTION WILL BE ATTEMPTED BUT MAY NOT BE ACHIEVED, THEREFORE EMAILS MAY NOT BE ENCRYPTED. CUSTOMER ACKNOWLEDGES AND AGREES THAT IT SHOULD NOT SEND OR RECEIVE SENSITIVE DATA VIA THE SERVICE OR CUSTOMER DOES SO ENTIRELY AT ITS OWN RISK.
d) During the Term of the Service, all Email retrieved or stored by the Service will be stored and accessible by Customer for ninety (90) days, and will subsequently be automatically deleted.
e) Customer acknowledges and agrees that (i) the Symantec Email Security Services do not scan all Emails that originally enter the archive and (ii) the Symantec scanning services (Email AntiVirus.cloud, Email AntiSpam.Cloud, Email Image Control.cloud and Email Content Control.cloud) may not scan Emails that are released from the archive for reinstatement to a User's mailbox. Accordingly, Symantec cannot be responsible for any Virus, spam, images or inappropriate content that such reinstated Emails may contain, and therefore, any Service Level Agreement will not apply to such reinstated Emails.

B.4.10. **Symantec Enterprise Vault.cloud IM Logging Option**
The Symantec Enterprise Vault.cloud IM Logging Option is only available to Customers who also use the Symantec Instant Messaging Security.cloud Service. The IM Logging Option is a cloud-based add-on Service to the Symantec Instant Messaging Security.cloud Service. The IM Logging Option utilizes the Enterprise Vault.cloud Service to archive instant message transcripts from Symantec Instant Messaging Security.cloud. This IM Logging Option captures and indexes instant message transcripts in Enterprise Vault Discovery.cloud. From Enterprise Vault Discovery.cloud, Customers can search across content directly and export search results for further review and analysis.

C. Customer Responsibilities.
C.1. Customer must configure each Service as applicable.

D. Reporting. See Schedule 1, Definitions and General Services Overview.

E. Technical Support.
E.1. Customer may review the current system status of the Services online.
E.2. Customer will have access to a self-service help and knowledgebase with the Service.

F. Additional Terms and Conditions.
F.1. All Customer data stored or archived by the Service by Symantec or its third party vendors is the sole property of Customer ("Customer Data"), and nothing herein conveys to Symantec or its vendors any legal or equitable right, title, or interest into Customer Data.
F.2. Customer Data shall be archived during the Term of the Service. Before the end of the Service term or upon termination of the Service, Customer shall make a written election for Symantec to: (i) delete Customer Data at no charge (unless prohibited by law or court order); or (ii) provide an offline copy in PST format via hard disk media at Symantec's then current rates. In the event Customer fails to provide written instruction to Symantec as provided in the preceding sentence, Symantec shall delete Customer Data (unless prohibited by law or court order).
F.3. CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA.

Appendix 14 – AdvisorMail on Symantec.cloud

A. Service Overview

A.1. AdvisorMail on Symantec.cloud™ ("AdvisorMail") is an Email archiving and compliance service. Customers must purchase the Service and add-on Services separately.

B. Service Features

B.1. **AdvisorMail on Symantec.cloud™**

Messages are captured, stored and indexed, auto-scanned and flagged based on Customer's specific policy selections. Emails or attachments containing specific keywords or phrases can be reviewed as required by Customer.

B.2. **AdvisorMail IM Option on Symantec.cloud™**

The AdvisorMail IM Option on Symantec.cloud™ is an add-on Service to the AdvisorMail on Symantec.cloud Service for supported instant message platforms. Instant messages are captured, stored and indexed, and auto-scanned and flagged based on Customer's specific policy selections. Instant messages containing specific keywords or phrases can be reviewed as required by Customer. AdvisorMail IM Option on Symantec.cloud™ interoperates with supported IM networks and clients which are currently defined in the AdvisorMail IM Option Compatibility List found at http://archive.onconfluence.com/display/~ptath/Supportive+IMs+and+Proxy+Settings.

B.3. **AdvisorMail Bloomberg Option on Symantec.cloud™**

The AdvisorMail Bloomberg Option on Symantec.cloud™ is an add-on Service to the AdvisorMail on Symantec.cloud Service for Instant Bloomberg® (instant messages) and Bloomberg® Email. Bloomberg® messages are captured, stored and indexed, and auto-scanned and flagged based on Customer's specific policy selections. This add-on Service captures Instant Bloomberg® and Bloomberg® Email into AdvisorMail on Symantec.cloud in their proprietary format. Bloomberg® messages containing specific keywords or phrases can be reviewed as required by Customer.

B.4. **Symantec Enterprise Vault.cloud Import Option**

The Symantec Enterprise Vault.cloud Import Option is an add-on Service to the AdvisorMail on Symantec.cloud Service that allows Customer to migrate and ingest existing legacy Email data into Customer's archive. This add-on Service allows Customer to combine both ingested legacy Email and new Email streams within the archive.

a) This add-on Service requires active participation by Customer to plan, analyze and execute an ingestion plan.
b) Customer must transfer Email data to be ingested via courier. All data should be provided in an encrypted form and Customer must provide the decryption key, per instructions from Symantec.
c) Customer can extract the data and provide it in any format defined in the Compatibility List from supported repositories.
d) With Customer's guidance, this add-on Service assigns Users to each Email imported. Email that cannot be directly assigned to a specific User are archived into a single mailbox within the archive.
e) All migration activity can be logged and audited to provide integrity of Customer's Email records.
f) The maximum size for an Email to be ingested is 40MB.
g) Symantec cannot guarantee the time it will take to import the data once received.
h) Symantec is not responsible for failure to import data that is corrupt when received from Customer.

C. Customer Responsibilities.

C.1. Customer must configure each Service as applicable.

D. Reporting.

See Schedule 1, Definitions and General Services Overview.

E. Technical Support.

E.1. Technical support is provided by telephone or online on a 24x7 basis.

E.2. Customer may review the current system status of the Services at http://support.liveoffice.com/system-status/lax.

E.3. Customer will have access to a self-service help and knowledgebase with the Service.

F. Additional Terms and Conditions.

F.1. All Customer data stored or archived hereunder by Symantec or its third party vendors is the sole property of Customer ("Customer Data"), and nothing in this appendix conveys to Symantec or its vendors any legal or equitable right, title, or interest into Customer Data.

F.2. Customer Data shall be archived during the Term of the Service. Before the end of the Service term or upon termination of the Service, Customer shall make a written election for Symantec to: (i) delete Customer Data at

no charge (unless prohibited by law or court order); or (ii) provide an offline copy in PST format via hard disk media at Symantec's then current rates. In the event Customer fails to provide written instruction to Symantec as provided in the preceding sentence, Symantec shall delete Customer Data (unless prohibited by law or court order).

F.3. CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA

Appendix 15 – Symantec Email Continuity Archive.cloud and Symantec Email Continuity Archive Lite.cloud

A. Service Overview

A.1. The Symantec Email Continuity Archive.cloud and Symantec Email Continuity Archive Lite.cloud Services are hosted Email storage systems which allow Customer's system administrators to set specific Email retention policies for the storage of historical Email for a set of designated Email mailboxes.

B. Service Features

B.1. **Symantec Email Continuity Archive.cloud Service** includes the following service features:

a) Email Capture and Storage: Email is captured as it is delivered to Customer's primary Email environment and transferred to an Email archive for indexing and storage. Email is encrypted and stored on the Service. Email retention policies can be set for Users to determine when Emails will be purged from the Service.
b) Recovery**:** Provides the capability to restore Email from the Email archive back to Customer's Exchange message stores.
c) E-Discovery: Provides the capability for Customer's system administrators to specify certain Users as "Reviewers", giving them the ability to review Email in mailboxes other than their own for electronic discovery and other purposes. Reviewers can create a discovery archive containing the results of a search across Users' mailboxes. The discovery archive can be exported to a single mailbox.
d) Windows Authentication: Allows a Customer that uses Microsoft Exchange® 2000, Microsoft Exchange® 2003 and/or Microsoft Exchange® 2007 to extend Customer's security policies for Microsoft Active Directory authentication to Users of the Service by enabling Users to log into the Service using their Active Directory password.
e) End User Archive: Enables Users who are part of a retention policy to access their personal archive containing Emails from their mailbox through a web-based interface. Customer's Email administrators can also specify whether or not Users can forward Emails from their personal archive.
f) Storage Management: Customer's system administrator can define a storage management policy which will move attachments from Customer's Exchange message stores to the Service.

B.2. **Symantec Email Continuity Archive Lite.cloud Service** includes the following service features (as each is further described above):

a) Email Capture and Storage
b) Recovery
c) E-Discovery
d) Windows Authentication

The Symantec Email Continuity Archive Lite.cloud Service does not include the End User Archive or Storage Management features. Customer may upgrade to include the End User Archive service feature by subscribing to the Symantec Email Continuity Archive Lite.cloud End User Pack.

B.3. **Data Import Option**.

Customer may import legacy data into the Service from .pst files by downloading and using an import tool, subject to payment of an import fee based on the amount of data required to be imported. In the event that the actual amount of legacy data exceeds the amount of import data purchased, Symantec reserves the right to charge for such additional data at its then current rates.

B.4. **Symantec Email Continuity.cloud Storage Option**

a) Customer's storage shall be measured by the raw amount of Email transferred to the Service and currently under storage.
b) If Customer subscribes to the Symantec Complete Email Safeguard.cloud, Symantec Complete Email & Web Safeguard.cloud or Symantec Ultimate Safeguard.cloud bundles:
c) The bundle includes a maximum of 0.7GB of new Email storage per User per year for the Symantec Email Continuity.cloud and Symantec Email Continuity Archive.cloud Services combined. In the event that Customer exceeds its storage allowance, Symantec shall charge for such additional storage at its then current rates.

B.5. **Service Termination & Data Extraction**

B.5.1.Upon termination of the Symantec Email Continuity Archive.cloud or Symantec Email Continuity Archive Lite.cloud Service, Symantec shall delete Customer's data from the archive.

B.5.2. Customer is able to extract its data from the archive at any time prior to termination.

C. Customer Responsibilities

C.1. Customer is responsible for the following actions in relation to the Service:

a) Providing and maintaining the necessary hardware and software (as identified in the provisioning form);
b) Ensuring that a dedicated technical resource with administrative rights is available for provisioning of the Service;
c) Designating which Users are entitled to receive the Service and the specified retention period for each such User;
d) Designating and protecting access privileges to the archive via Customer interface;
e) Setting and managing archiving retention policies;
f) Executing searches for retrieval of archived data.

C.2. In the event that Customer has failed to perform the actions required in order to provision the Service within thirty (30) days from the date of Customer's order, Symantec may commence charging for the Service.
C.3. The bundles listed above do not include storage for any legacy data imported and Customer is required to purchase sufficient additional storage to meet such requirements.
C.4. If Customer does not subscribe to one of the bundles listed above, no storage is included in the per User price and Customer is required to purchase sufficient storage for the Service.

D. Reporting. See Schedule 1, Definitions and General Services Overview.

E. Technical Support. See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions

F.1. NO EMAIL ARCHIVE SERVICE CAN GUARANTEE 100% ACCURACY AND THEREFORE SYMANTEC IS NOT LIABLE FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE EXCEPT FOR THE REMEDIES EXPRESSLY PROVIDED IN THE SERVICE LEVEL AGREEMENT IN SCHEDULE 3, BELOW.
F.2. Symantec shall not be responsible for any inability to provide the Service as set out in this appendix which is caused by (i) Symantec's inability to apply its standard practices in deploying and managing the Service to Customer, (ii) failure of Customer to follow the Symantec guidelines set forth in the user manual or the provisioning form, or (iii) failure of Customer to activate or use the Service.
F.3. CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA
F.4. Customer acknowledges and agrees that (i) the Symantec scanning services (Email AntiVirus.cloud, Email AntiSpam.Cloud, Email Image Control.cloud and Email Content Control.cloud) do not scan all Emails that originally enter the archive and (ii) the Symantec scanning services (Email AntiVirus.cloud, Email AntiSpam.Cloud, Email Image Control.cloud and Email Content Control.cloud) do not scan Emails that are released from the archive for reinstatement to a User's mailbox. Accordingly, Symantec cannot be responsible for any virus, spam, images or inappropriate content that such reinstated Emails may contain, and furthermore, the Service Level Agreement shall not apply to such reinstated Emails.
F.5. Customer acknowledges and agrees that Symantec cannot act as a third party downloader in any event for the purposes of US SEC regulations.

Appendix 16- Symantec Email Continuity.cloud

A. Service Overview

A.1. The Symantec Email Continuity.cloud ("EC") Service is a standby messaging system for Microsoft Exchange® and Lotus Notes® environments.

B. Service Features

B.1. Email Continuity.cloud will synchronize key system and User information including, but not limited to, the Email directory and individual Users' personal contacts. Customer can also configure Email Continuity.cloud to support BlackBerry® devices through wireless forwarding using the BlackBerry® Web Client or BlackBerry® Internet Service, and an integrated Microsoft Outlook® experience for Users on Microsoft Outlook® 2003 Cached Mode or Microsoft Outlook® 2007 Cached Mode through an installed Microsoft Outlook® Extension.
B.2. Supported Versions: Microsoft Exchange® 5.5, Microsoft Exchange® 2000, Microsoft Exchange® 2003, Microsoft Exchange® 2007, Lotus Notes® Version 6, Lotus Notes® Version 7.
B.3. Supported Versions for Microsoft Outlook® Extension: Microsoft Outlook® 2003 in Cached Mode; Microsoft Outlook® 2007 in Cached Mode.
B.4. Activation: Customer can request activation of Email Continuity.cloud via telephone to the Symantec support team or via the SMC. Upon activation of Email Continuity.cloud, Customer shall receive alerts via SMS to nominated mobile phones and personal Email addresses. At that time, Email Continuity.cloud will begin to receive and sort incoming Emails, filter them (subject to Clause F.1. below) in accordance with any other Symantec Email Services to which Customer has subscribed (e.g. the Email AntiVirus.cloud Service), and route them to the appropriate User mailboxes. Email Continuity.cloud will provide storage and retention of Email traffic sent and received during activation for up to thirty (30) calendar days after de-activation.
B.5. Retention: Customer is responsible for designating which Users' Emails are to be retained and the specified retention period for each User. The retained Emails will be deleted upon the earlier of (i) expiry of the designated retention period for such User or (ii) termination of Email Continuity.cloud.
B.6. Authentication Manager: Customer may extend Customer's security policies for Microsoft Active Directory authentication to Email Continuity.cloud by enabling Users to log into their Email Continuity.cloud mailboxes using their Windows password, thereby removing the need for a separate Email Continuity.cloud password. Windows authentication requires the availability of a Windows domain controller accessible by Authentication Manager at the time of Email Continuity.cloud activation which is able to authenticate Users attempting to log on to Email Continuity.cloud mailboxes. Supported Versions: Microsoft Exchange® 2000, Microsoft Exchange® 2003, Microsoft Exchange® 2007
B.7. The minimum number of Users of Email Continuity.cloud that may be purchased by Customer is the greater of (i) a number of Users equal to the number of mailboxes in Customer's Microsoft Exchange® organization or (ii) ten (10) Users.
B.8. Partial Activation: For certain Email systems/versions (e.g., Microsoft Exchange® 2000, 2003 and 2007 environments), Email Continuity.cloud is capable of being activated for subsets of Customer's environment (one or more individuals, servers and/or locations),in order to serve more localized Email outages.
B.9. Activation: The Email Continuity.cloud subscription entitles Customer to twenty four (24) activations per 12 month period, each lasting for a period of up to twelve (12) consecutive hours ("Included Activations"). Customer may purchase additional activations (each lasting for a period of up to twelve (12) consecutive hours) at Symantec's then current rates.
B.10. System Testing: System Testing shall include (i) one (1) quarterly test of Email Continuity.cloud for all Users, with such test lasting up to four (4) hours, and (ii) for Microsoft Exchange® 2000, Microsoft Exchange® 2003 or Microsoft Exchange® 2007 environments, unlimited partial testing of up to ten percent (10%) of Users. Customer must schedule these tests with Symantec no less than seven (7) business days prior to Customer's desired test date.
B.11. If Customer uses the Email AntiVirus.cloud, Email AntiSpam.Cloud, Email Content Control.cloud and/or Email Image Control.cloud Services, Symantec is able to configure the failover routing for Customer's Emails to the Email Continuity.cloud environment within the SMC. This failover routing will be used when the Email Continuity.cloud service is activated.
B.12. **Options**
B.12.1. **Symantec Email Continuity – .cloud Storage Option**

a) If Customer subscribes to the Symantec Complete Email Safeguard.cloud, Symantec Complete Email & Web Safeguard.cloud or Symantec Ultimate Safeguard.cloud bundles, then the bundle includes a maximum of 0.7GB of new Email storage per User per year for the Symantec Email Continuity.cloud and Symantec Email Continuity Archive.cloud Services combined. In the event that

Customer exceeds its storage allowance, Symantec shall charge for such additional storage at its then current rates.

b) If Customer does not subscribe to one of the bundles listed in Clause B.12.1.a, above, no storage is included in the per User price and Customer is required to purchase sufficient storage for the Service.

B.12.2. **Symantec Email Continuity – .cloud Wireless Option**

a) If Customer subscribes to Symantec Email Continuity - .cloud Wireless Option, system administrators may provision specific BlackBerry® devices managed by their corporate RIM BlackBerry® Enterprise Servers (BES). When Email Continuity.cloud is activated, provisioned BlackBerry® devices will continue to send and receive Email by communicating with EMS, via a secure channel established by the BES server.

b) Supported Versions: Microsoft Exchange® 2000, Microsoft Exchange® 2003 or Microsoft Exchange® 2007; BlackBerry® Enterprise Server version 4.0 (or above); BlackBerry® Handheld Devices firmware version 4.1 (or above).

C. Customer Responsibilities

C.1. Customer is responsible for providing and maintaining the necessary hardware and software (as identified in the provisioning form).

C.2. Customer is required to purchase sufficient storage for retention purposes.

D. Reporting. See Schedule 1, Definitions and General Services Overview.

E. Technical Support. See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions

F.1. Customer acknowledges and accepts that where Customer is in an activated state, and Customer then sends Emails to, or receives Emails from another organization that is also in an activated state, Emails will bypass the Symantec inbound and outbound scanning Services to which Customer subscribes.

F.2. If Customer does not use Email AntiVirus.cloud, Email AntiSpam.Cloud, Email Content Control.cloud or Email Image Control.cloud, it is Customer's responsibility to configure and test the failover routing for the Customer Emails to the Email Continuity.cloud environment. These failovers must be set up according to Symantec's instructions during the provisioning process and maintained thereafter. In the event that Customer fails to set up or maintain such failovers, Customer acknowledges and accepts that Emails cannot be routed to Email Continuity.cloud.

F.3. SYMANTEC IS NOT LIABLE FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO SYNCRONIZE EMAIL SYSTEMS.

Appendix 17 – Symantec Email Archiving.cloud P

A. Service Overview

A.1. The Symantec Email Archiving.cloud (P), Symantec Email Archiving.cloud Lite (P) and Symantec Email Archiving.cloud Premium (P) Services (collectively the "Archiving.cloud (P) Service") are hybrid managed services for archiving, storing and retrieving Emails.

B. Service Features

B.1. Symantec will contact Customer to schedule an initial teleconference.
B.2. The initial teleconference shall be carried out via WebEx®. In this call the parties shall:

a) Verify all actions in the Client Setup Document have been completed;
b) Install the archiving and other required Software using Symantec's current archiving installation procedures document;
c) Review Active directory setup;
d) Activate the Service;
e) Verify user interface accessibility;
f) Verify archiving (site-to-site);
g) Generate copies of encryption keys in accordance with Symantec's current key backup procedures document.

B.3. A training session is available on or after the initial teleconference and comprises sessions focused on: (i) IT, (ii) Policy, (iii) Supervision, and (iv) End user.
B.4. A post-review teleconference is scheduled for approximately one (1) week following activation. Following completion of the post-review teleconference, Customer will follow the standard technical support procedures if additional assistance is required.
B.5. For Customers with *500 Users or fewer*, the *Symantec Email Archiving.cloud Lite (P) Service* includes the following:

a) Standard features as described in Clause B.11. below;
b) 3 year retention period;
c) Maximum storage of 3GB per User (calculated as an average per User based on the total number of Users).

B.6. For Customers with *more than 500 Users*, the *Symantec Email Archiving.cloud Lite (P) Service* includes the following:

a) Standard features as described in Clause B.11. below;
b) 1 year retention period;
c) Maximum storage of 1.5GB per User (calculated as an average per User based on the total number of Users).

B.7. For Customers with *500 Users or less*, the *Symantec Email Archiving.cloud (P) Service* includes the following:

a) Standard features as described in Clause B.11. below;
b) 10 year retention period;
c) Maximum storage of 10GB per User (calculated as an average per User based on the total number of Users).

B.8. For Customers with *more than 500 Users*, the *Symantec Email Archiving.cloud (P) Service* includes the following:

a) Standard features as described in Clause B.11. below;
b) Unlimited retention period;
c) Maximum storage of 6GB per User (calculated as an average per User based on the total number of Users).

B.9. For Customers with *500 Users or less*, the *Symantec Email Archiving.cloud Premium (P) Service* includes the following:

a) Standard features as described in Clause B.11. below;
b) Premium features as described in Clause B.12. below;
c) 10 year retention period;
d) Maximum storage of 10GB per User (calculated as an average per User based on the total number of Users).

B.10. For Customers with *more than 500 Users*, the *Symantec Email Archiving.cloud Premium (P) Service* includes the following:

a) Standard features as described in Clause B.11. below;
b) Premium features as described in Clause B.12. below;
c) Unlimited retention period;

d) Maximum storage of 6GB per User (calculated as an average per User based on the total number of Users).

B.11. **Standard Features**

B.11.1. Address Resolution and Distribution List/Group Expansion. All Email addresses marked by Exchange as being internal addresses will be resolved to the corresponding User mailbox. For each distribution list referenced as a recipient of the message, a list of the then-current membership will be captured as additional metadata about the Email message.

B.11.2. Full-text Index. The Email Archiving Appliance can extract textual content from various types of attachments as well as common fields in the message in order to support the creation of a full-text index for searching within the Archiving.cloud (P) Service.

B.11.3. Encryption. Message content data and index data (with the exception of fields such as dates and other non personally identifiable information) are encrypted using industry standard encryption technologies based upon a customer-specific encryption key held by Customer only. Customer has sole possession of all passwords, encryption keys and configuration settings and accordingly Customer should ensure that they are maintained safely, and are kept in escrow or another suitable location.

B.11.4. Retention Policies. Customer can define and update retention policies via the user interface. Each retention policy can consider criteria including the parties involved, keywords/phrases in the content and file types attached. As each message is archived, it is evaluated against the then-active set of retention policies. If a message matches more than one retention policy, the policy with the longest retention period is applied. If no specific retention policy matches the message, the default retention policy is applied.

B.11.5. InfoTags (metadata). Customer can define and update InfoTags via the user interface. Each InfoTag can consider criteria including the parties involved, keywords/phrases in the content, and file types attached. As each message is archived, it is evaluated against the active set of InfoTags and is flagged with each one that applies.

B.11.6. Policy Tracking. Changes made to retention and supervision policies are maintained by the system in unalterable form for reference purposes. Customer may generate a PDF-format file of current or previous versions of policies via the user interface.

B.11.7. Historical User Tracking. A list of all Users that have a mailbox within Exchange is submitted to the system on a nightly basis in order to maintain a running list of all mailboxes that have existed since the Archiving.cloud (P) Service was implemented.

B.11.8. Attachment Stubbing. Customer may enable functionality that replaces attachment content within Customer's mail system ("Mailbox Data") with a pointer to the appropriate copy within the archive. Customer can define and update stubbing policies with different rules for each group of mailboxes, based upon the age and size of the message as well as the folder it resides in. To facilitate automatic restoration of the original attachment from the archive when Users forward mail, Customer may install the Attachment Stubbing custom form to its Organization Forms Library (a special public folder on the Exchange server). Microsoft Outlook® will then automatically install the custom form from the server. To facilitate access to retrieve attachments outside of Customer's network, Customer may install the Archive Proxy on their front-end (OWA) Exchange servers. By default, only Mailbox Data that has previously been archived will be stubbed. Customer can enable an option that stores a copy of attachments not previously archived to facilitate stubbing of the attachments contained in the mailbox. Customer can configure retention policies on a per-mailbox basis to define how long attachments stored in this way should be retained. If not so specified, the default retention policy will apply to these items. Attachments stored by this process are not searchable within the archive.

B.11.9. *End-User Access*. Customer may choose to provide individual Users with access to search the archive, either within the web user interface or directly within Microsoft Outlook®.

B.11.10. Discovery Access. Customer can perform searches against the entire archive within the user interface. Customer can create a "hold" which is a repository for messages relevant to a given matter. Customer can perform search activity within the hold in the same way that they can search through the active archive.

B.11.11. Ad-Hoc Holds. Customer can use the policy user interface to define and update ad-hoc holds. The hold can consider criteria including the parties involved, keywords/phrases in the content, and file types attached. As each message is archived, it is evaluated against the then-active set of holds. The message is associated with each hold that it matches. To capture existing archived data into an ad-hoc hold, Customer can perform a search with similar criteria, copy the results to a folder, then copy the contents of the folder to the hold. Each ad-hoc hold has an indefinite retention period – all messages in a given ad-hoc hold are retained until that hold is released.

B.11.12. People-based Holds. Customer can use the policy user interface to define and update people-based holds. Each people-based hold defines a set of Users. As each message is archived, if it involves one of the people listed on a given hold, it is associated with that hold. The system also automatically captures existing mail belonging to the Users currently referenced by the hold and creates a new copy of the messages into the

hold. When Users are removed from a people-based hold definition, messages that belong solely to those Users no longer listed will be automatically disposed of from the hold. Messages for currently listed Users covered by a hold are retained until that hold is released.

B.11.13. Data Export. Messages from the active archive or hold can be exported to PST files. The system will create multiple PST files if required due to file size constraints.

B.11.14. Reporting. Reports about the size and growth of the archive are available to Customer within the user interface for display in HTML or to export to PDF or CSV (data only).

B.11.15. Audit Trail. Search, message view, export, retrieval and supervision activities are tracked. The audit trail can be viewed as a property of any given message. An audit trail viewer across all messages allows for filtered views based upon the type of activity, the person that performed the activity and/or the date of the activity.

B.11.16. Integration with Active Directory. Access to the archive is managed by adding Users (or existing groups of Users) to a set of predefined security groups within Active Directory. Each of these groups has an associated set of privileges. A User can perform several roles by virtue of their membership in several of these security groups. Authentication is performed directly against Active Directory. Users may sign in using their standard Active Directory username and password. Disabled accounts do not have access rights to the archive. Active Directory groups may also be referenced by various other aspects of the system to facilitate easier administration of elements such as policies. A nightly synchronization process is used to capture changes in group membership.

B.11.17. Retention and Disposition Management. Based upon the retention policies defined by Customer within the SMC, the Archiving.cloud (P) Service will categorize messages and either assign a target disposition date or record the month that the message was archived for indefinite retention. Target disposition dates align to the beginning of each month. Once messages have reached their target disposition date, Customer's authorized User(s) can formally approve disposition for all messages associated with that target disposition date. For messages archived according to an indefinite retention period, Customer's authorized User(s) can formally approve disposition for all messages that were archived during a given month. Data that is designated for disposal cannot be restored in human readable form from any and all storage mediums (including without limitation backups).

B.12. **Premium Features**

The following features are included with the Symantec Email Archiving.cloud Premium (P) Service only:

B.12.1. Supervision:

a) Automatic Selection for Supervisory Review. Customer can define and update policies through the CMP that add messages to a review queue. Each policy can consider the parties involved, keywords/phrases in the content, and file types. In addition, random sampling policies can be configured for specific Users.

b) Supervisory Review. Customer can assign access rights for reviewers to read messages that have been added to the review queue and flag them as acceptable or not.

B.12.2. Bloomberg® Archiving:

a) The Symantec Email Archiving.cloud Premium (P) Service uses logging features of the Bloomberg® Professional Service that records Email and instant message conversations in XML files that are posted on a nightly basis to the Bloomberg® FTP site.

b) If Customer subscribes to the Bloomberg® Professional Service, the Email Archiving Appliance can be used to retrieve a copy of these XML files from the FTP site for conversion into HTML formatted messages and submission to the archive.

c) The FIRM format is supported, but not the ACCOUNT format or historical extract format of Bloomberg® logs.

d) The Bloomberg® archiving integration does not purge content from the Bloomberg® FTP site, but does track which files have been processed. As Bloomberg® purges content from its FTP site on a regular basis, and the Bloomberg® archiving integration process purges copies that it has made on the Email Archiving Appliances, Customer must monitor that the archiving integration is working on an on-going basis so that files are not deleted before the Bloomberg® archiving integration has been able to retrieve and fully process them.

e) A list of Bloomberg® FIRM identifiers is used to identify which users referenced in the XML are internal employees. The Bloomberg® archiving integration provides a web-based mapping user interface that allows an administrator to associate each of the Bloomberg® user accounts to the corresponding Active Directory user accounts. As the XML files are processed, if a message references an internal user that is not yet mapped, the address is added to the unmapped address list and the message is not processed. Once the administrator has mapped these addresses they

can trigger reprocessing of the associated messages. The resolved corporate Email addresses are used as the sender/recipients of the message.

f) An informational block within the message body provides additional information about the actual addresses/display names of the parties to the message/conversation including the user's Bloomberg® account information.

B.13. **Legacy Data Import**

B.13.1. Customer may import legacy data into the Archiving.cloud (P) Service subject to payment of the applicable fee based on the amount of data to be imported. In the event that the actual amount of legacy data exceeds the amount of import data purchased, Symantec reserves the right to charge for such additional data at its then standard rates.

B.13.2. Customer may elect to use independent third party software in order to facilitate the import of data to the archive at its own risk and expense.

C. Customer Responsibilities

C.1. Customer is required to purchase Email Archiving Appliance(s) in order to receive the Archiving.cloud (P) Service. The Email Archiving Appliance(s) (and accompanying documentation) will be shipped to Customer for installation and configuration. Customer is responsible for all shipping, duties, insurance and taxes on the Email Archiving Appliance.

C.2. Actions outlined in Symantec's Client Setup Document must be completed by Customer before the initial teleconference and include, but are not limited to:

a) Set up new active directory user account;
b) Set up additional active directory groups;
c) Add users to Exchange groups;
d) Firewall configuration (if required);
e) Enable Microsoft Exchange® Journaling (no earlier than 48 hours before installing the Email Archiving Appliance);
f) Install Email Archiving Appliance (in rack and booted up);
g) Ensure all mailboxes required for archiving are "mail enabled";
h) Configure remote access for Symantec.

C.3. Customer may call a Symantec Customer Service Manager if assistance is needed with the above actions.

C.4. Customer must configure the journaling feature of Exchange to deposit a copy of internal and external Emails into a local mailbox on the Exchange server. Appliance(s) which reside behind the firewall within Customer's corporate network (the "Email Archiving Appliance(s)") can then be used to pull data from this mailbox for submission to the Archiving.cloud (P) Service. Emails are not deleted from the journaling mailbox until storage within the Archiving.cloud (P) Service is confirmed.

D. Reporting. See Schedule 1, Definitions and General Services Overview.

E. Technical Support. See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions

F.1. Archived Emails cannot be deleted until the assigned retention period expires.

F.2. Symantec is unable to act as a third party downloader. If the event that Customer is required to select a third party downloader for compliance purposes, Customer must enter into an independent agreement with Symantec's third party service provider, for which there may be a separate fee that is not determined by Symantec.

F.3 CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA

F.4. Upon termination of the Archiving.cloud (P) Service, Symantec shall delete Customer's data from the archive. Prior to termination, Customer may extract its data from the archive, or Customer can request that Symantec's authorized third party transfers the archived data back to Customer in PST file format.

F.5. If Customer requests Symantec's authorized third party to transfer the archived data upon termination:

a) Customer must enter into a direct agreement with that third party. Symantec shall not be a party to such agreement.
b) As the data is stored in an encrypted format, Customer will need to provide the third party with an encryption key in order to decode the Email into a free format.

c) Customer will be responsible for the costs of transfer. Costs will be agreed upon in the agreement with the third party. Costs may be based on: (i) Amount of data; (ii) Format/medium of transfer; (iii) Costs of setting up transfer process; (iv) Time and materials used to complete the transfer.
d) Symantec reserves the right to charge its then current rates for storage if the data has not been exported and deleted from the archive upon the effective date of termination.

F.6. Symantec may, at its sole discretion, terminate the Archiving.cloud (P)Service immediately without notice and take such defensive action as it deems necessary:

a) If so directed by a court or competent authority;
b) In the event of an attack on the Archiving.cloud (P) Service or network; or
c) In the event that Customer or any of its Users is in breach of the Acceptable Use Policy defined below.

F.7. Customer shall be responsible for ensuring that it and all of its Users are aware of and comply with this Acceptable Use Policy:

Users must not under any circumstances whatsoever commit, nor attempt to commit, nor aid or abet any action that may threaten the Archiving.cloud (P) Service, whether deliberately, negligently or innocently. This shall include but is not limited to:

a) Any attempt to crash a service host or network;
b) “Denial of service” attacks or “flooding” attacks against a service host or network;
c) Any attempt to circumvent the user authentication or security of a service host or network;
d) The creation, transmission, storage, or publication of any kind of Virus or corrupting program or corrupted data;
e) Any other action that may adversely affect the Archiving.cloud (P) Service or its operation.

F.8. SYMANTEC IS NOT LIABLE FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE EXCEPT FOR THE REMEDIES EXPRESSLY PROVIDED IN THE APPLICABLE SERVICE LEVEL AGREEMENT.

F.9. Symantec is not liable for the loss of any passwords, encryption keys or configuration settings. Customer accepts and agrees that loss of passwords and encryption keys will result in the archive being inaccessible.

F.10. Customer is required to select the location of the archiving data centre at the time of the order and the charges are calculated based on such selection. CUSTOMER AGREES TO TAKE ALL NECESSARY STEPS TO (I) INFORM ANY OF ITS EMPLOYEES, AGENTS AND CONTRACTORS AS WELL AS THIRD PARTIES WHO USE THE COMMUNICATION SYSTEM COVERED BY THE ARCHIVING.CLOUD (P) SERVICE OF THE FACT THAT ANY INFORMATION, INCLUDING WITHOUT LIMITATION PERSONALLY IDENTIFIABLE INFORMATION OF INDIVIDUALS, MAY BE PROCESSED IN THE DATA CENTER COUNTRY LOCATION; AND, IF REQUIRED BY LAW (II) OBTAIN SUCH EMPLOYEES, AGENTS, CONTRACTORS AND THIRD PARTIES’ CONSENT TO SUCH PROCESSING PRIOR TO THE OPERATION OF THE ARCHIVING.CLOUD (P) SERVICE BY CUSTOMER.

F.11. Customer acknowledges and accepts that, if purchased, (i) the Symantec scanning services (Email AntiVirus.cloud, Email AntiSpam.Cloud, Email Image Control.cloud and Email Content Control.cloud) do not scan all Emails that originally enter the archive and (ii) the Symantec scanning services (Email AntiVirus.cloud, Email AntiSpam.Cloud, Email Image Control.cloud and Email Content Control.cloud) do not scan Emails that are released from the archive for reinstatement to a User’s mailbox. Accordingly, Symantec cannot be responsible for any Virus, spam, images or inappropriate content that such reinstated Emails may contain, and furthermore, the Service Level Agreement(s) shall not apply to such reinstated Emails.

Appendix 18 –Symantec Web Security Archiving.cloud

A. Service Overview

A.1. The Symantec Web Security Archiving.cloud Service is a cloud based archiving service for retaining User web browsing history from the Symantec Web Services.

B. Service Features

B.1. Customer may choose the Basic or Premium Service:

B.1.1. The Basic Service includes;

a) A default of 6 months,
b) Allows up to 12 months of archiving.

B.1.2. The Premium Service includes;

a) A default of 3 years,
b) Allows up to 7 years of archiving,
c) A SMC which allows each User to directly access items in their own archive. Users can search their full archive but do not have access to the advanced features available to the archive Administrator. Users cannot access any information in the archive that is not generated by them.

B.2. Archiving of the following information is available through the Service:

a) Date URL was requested
b) User requesting the URL
c) Full URL requested
d) RuleSpace category as defined by the Web Security Service

B.3. The information is collected from, and limited to, the logs produced from the Web Services and is ingested, indexed and stored within the Symantec Infrastructure. All URL's will be stored except those that have been added to the bypass list in the Symantec Web Services.

B.4. The E-Discovery feature allows data to be searched using multiple search fields and options.

B.5. Data holds are available to allow logs to be grouped, named and stored. The selected data is then retained for an indefinite period, until the data hold is removed, or the Service terminated by Customer.

B.6. Records can be exported in HTML format for external review and/or storage.

B.7. Encryption technologies are used to ensure that all communication between the Service and the archive will be encrypted. Data is also fully encrypted when stored within the archive and is not accessible unencrypted to anyone other than Customer.

C. Customer Responsibilities

C.1. Customer is responsible for configuring the log retention period within the SMC.

C.2. Customer is required to upload required information for all authorized Users of the Service.

D. Reporting.

D.1. Reporting metrics available to the Service Administrator for number of users, total disk space used, and disk space used per calendar day.

E. Technical Support. See Schedule 1, Definitions and General Services Overview.

F. Additional Terms and Conditions.

F.1. Archived Web records cannot be deleted from the system until Customer-selected retention period has been reached.

F.2. Customer acknowledges that Symantec is not able to retrieve any data encrypted by the Service.

F.3. The Service Level Agreement in Schedule 3, below, will not operate for the Basic Service.

F.4. SYMANTEC IS NOT LIABLE FOR ANY DAMAGE OR LOSS OF DATA RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO ARCHIVE DATA.

Appendix 19 –Symantec Endpoint Protection Small Business Edition 2013

A. Service Overview

A.1. The Symantec Endpoint Protection Small Business Edition 2013 service is an antivirus and anti-malware service that lets Customer choose a cloud-managed service or on-premise deployment option. This appendix applies to the cloud-managed deployment option only. The on-premise option is governed by the Subscription Instrument and accompanying EULA.

B. Service Features

B.1. The Service is intended to:

a) Protect the computer from detected malwares based on known methods.
b) Block known malicious attacks from the network on the computer.
c) Provide available anti-phishing functionality on the supported browsers which will block suspected phishing attacks.
d) Symantec will publish the current list of supported computer operating systems for the agent and supported browser for the SMC.
e) Block or allow access from USB storage devices based on Customer configuration.

B.2. Changes made to the policies are visible on the SMC and are batched to push down to the agents. Effective policy setting on individual agents can be viewed on the SMC, or on the agent running on the end-user computer.
B.3. Customer may configure the Service to send an automatic notification to configured Email recipients based on the alerts rule, configurable in the SMC. Notifications can be created, deleted and customized through the SMC.

C. Customer Responsibilities

C.1. Installation of a Service Software is required for each affected end–user computer receiving the Service.
C.2. Customer must manage the Service Software through the SMC.
C.3. Customer must manage computers, policies, alerts and reports and other configuration options through the SMC.
C.4. Customer must make any required firewall changes to allow the agent to communicate and operate with the Service.
C.5. Customer must designate any Local Update Hosts through the SMC.

D. Reporting

D.1. During the Term, all logs and reports based on data reported by the agent are stored on, viewable and downloadable from the SMC for ninety (90) days, and will be automatically deleted at the end of that ninety (90) day period.
D.2. All logs and reports will be deleted upon termination or expiration of the Term.

E. Technical Support

E.1. Support includes:

a) Walk through of the SMC including a service description and Q&A session. (This does not include assistance with the set up of policies or analysis of the effectiveness of the policies);
b) Online help content;
c) User Guide.

F. Additional Terms and Conditions

F.1. Instances: Notwithstanding anything to the contrary contained in this appendix, each running instance (physical and/or virtual) of the Service Software must be licensed. An “instance” of Service Software is created by executing the Service Software’s setup or install procedure. An “instance” of Service Software is created by duplicating an existing instance. References to the Service Software include “instances” of the Service Software. Customer “runs an instance” of software by loading it into memory and executing one or more of its instructions. Once running, an instance is considered to be running (whether or not its instructions continue to execute) until it is removed from memory.
F.2. Terminal Servers: If the Service Software is for use on a hardware device/server that provides endpoints with a common connection point to a local or wide area network (a “Licensed Terminal Server”), and such Licensed Terminal Server(s) is/are accessed by endpoints that do not have installed copies of the Service Software (“Thin Clients”), then every Thin Client accessing a Licensed Terminal Server is considered an “instance” and must have a valid license to

the Service Software. In the event that the Licensed Terminal Server(s) is/are accessed by endpoints which have authorized copies of the Service Software already installed ("Thick Clients"), such access of the Licensed Terminal Server(s) by Thick Clients shall not be considered additional "instances" and Customer is not required to purchase additional licenses to the Service Software.

F.3. CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA

F.4. As indicated in the applicable Subscription Instrument, Customer may choose to deploy either the cloud-managed or on-premise option at any time during the applicable License Term, but not both at the same time. All Users of the Service, regardless of when the Service was purchased, must use the same deployment option. If Customer is changing from one deployment option to the other, Customer will have a grace period of sixty (60) calendar days to complete such change. If Customer chooses to deploy the on-premise option, Customer must upgrade to the most current version within ninety (90) calendar days of availability of such upgrade.

F.5. When Customer is using the cloud-managed Service, Customer may deploy the on-premise option to protect an environment for which the cloud-managed Service is not yet available. Any deployment of the on-premise option must be included in the total User count. Customer will have sixty (60) calendar days to synchronize the deployment of all Users, once the cloud-managed Service becomes available for that environment.

Appendix 20 –Symantec Backup Exec.cloud

A. Service Overview

A.1. The Symantec Backup Exec.cloud Service provides online backup and recovery of Customer selected data.

B. Service Features

B.1. Customer data is automatically routed by the Service to Symantec's data centers.
B.2. Customer may configure the Service to back up Customer data directly to onsite storage locations (the "Onsite Backup) through the SMC. Onsite Backup is only available to Users directly connected (physically or virtually) to the Customer environment. Storage capacity for Onsite Backup is based on the available storage in the Customer environment. Onsite Backup can synchronize data automatically to Symantec data centers per Customer's configuration.
B.3. Customer data is encrypted during transmission and at rest.
B.4. Symantec shall publish a list of supported computer operating systems for the use and installation of the agent as well as supported browsers for the use of the SMC. Customer acknowledges and accepts that Symantec may update and change this list on a regular basis without notice.
B.5. The Service Software installed on the applicable User computer shall backup the data to Symantec data centers and/or the Onsite Backup based on the files/folders selected through the SMC.
B.6. Customer selected changes made through the SMC are visible immediately on the SMC. User configurations are then batched to be pushed down to the Service Software when the endpoints are online and available.
B.7. Customer may configure the Service to send an automatic notification to configured Email recipients based on predetermined alerts, configurable by Customer in the SMC.
B.8. Customer can create, delete and customize notifications through the SMC.

C. Customer Responsibilities

C.1. Customer must install the Service Software on applicable User computers and assign appropriate policies through the SMC to use the Service.
C.2. Customer may have to make some basic firewall changes to allow the Service Software to communicate and operate with the Service Infrastructure.
C.3. Customer must use the SMC to manage the Service Software.

D. Reporting

D.1. All logs and reports generated by the agent are stored on, viewable and downloadable from the SMC for ninety (90) days, after which time the logs and reports will be deleted.

E. Technical Support

E.1. Support includes:

a) A teleconference walk through of the SMC including a service description and Q&A session. (This does not include assistance with the set up of policies or analysis of the effectiveness of the policies);
b) Access to the Administrator's Guide and the User Guide, both of which may be obtained from the SMC.

F. Additional Terms and Conditions

F.1. All Customer data stored or archived hereunder by Symantec or its third party vendors is the sole property of Customer ("Customer Data"), and nothing under this appendix conveys to Symantec or its vendors any legal or equitable right, title, or interest in Customer Data.
F.2. Customer is solely responsible for Customer's conduct related to the Service, including control over the content of any Customer Data stored on the Service. Customer specifically agrees that it will not use the Service:

a) In violation of any laws or regulations, including without limitation, uploading, transmitting, storing or otherwise backing up any obscene, indecent, or pornographic content;
b) In any manner that would infringe the intellectual property or rights of third parties; or
c) To transmit any material that contains Viruses or other harmful computer code or files such as Trojan horse, worms or time bombs.

F.3. Customer may upload, store or otherwise backup Customer Data up to the total amount of storage or allocated quota Customer has purchased from Symantec ("Maximum Storage"). In the event Customer exceeds the Maximum

Storage, Symantec reserves the right to restrict Customer's ability to backup data until Customer reduces its storage usage or subscribes to a storage plan with higher quotas.

F.4. Customer may access Customer Data during the Term for a period of ninety (90) days. Following termination or expiration of the Term, Customer Data will no longer be available for access by Customer and Customer will not be able to add to the backups or restore Customer Data. However, Symantec will continue to store and maintain Customer Data ("Stored Data") for a period of sixty (60) calendar days following the date of expiration or termination of the Term ("Post-Termination Retention Period"). During the Post-Termination Retention Period, Customer may elect to renew the Term and pay the applicable fees, which will allow Customer to regain access to the previously Stored Data again. Following expiration of the Post-Termination Retention Period, Customer Data will be deleted by Symantec and will no longer be accessible by Customer or Symantec in the event Customer does not renew the Service.

F.5. Customer may only direct the Onsite Backup to Customer owned and/or controlled environment. Customer may not direct the Onsite Backup to a managed service provider or service bureau server.

F.6. CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA.

SCHEDULE 3
SERVICE LEVEL AGREEMENT

1. General

1.1. In the event that Customer believes it is entitled to a remedy in accordance with this Service Level Agreement, Customer must submit a Credit Request within ten (10) business days of the end of the calendar month in which the suspected breach of the service level 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.
1.2. All Credit Requests will be subject to verification by Symantec in accordance with the applicable provisions of this Service Level Agreement.
1.3. This Service Level Agreement will not operate: (i) during periods of Planned Maintenance or emergency maintenance, periods 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 or (iii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (iv) Customer has not configured the Service in accordance with the Agreement.
1.4. 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.
1.5. 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 the affected Service(s).
1.6. Where the affected Service is part of a Non-Severable Service Bundle:

a) For the purpose of calculating Service Credits, the Monthly Charge for such affected Service shall be calculated as the total monthly charge for the Non-Severable Service Bundle divided by the number of separate Services included in the bundle; and
b) if Customer terminates the affected Service in accordance with this Service Level Agreement, the revised charge for the Non-Severable Service Bundle shall be calculated as the original total Monthly Charge for the Non-Severable Service Bundle, divided by the original number of separate Services included in the bundle, and multiplied by the number of remaining constituent Services in that bundle.

2. Exceptions to Service Level Agreement for Email Security Services and Web Services.

2.1. 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) or in respect of any inbound or outbound Emails that were initially sent to Symantec containing more than 500 recipients per SMTP session.
2.2. The Service Levels for the Email Security Services do not apply to the Email Continuity.cloud Service and therefore the Service Levels for the Email Security Services in Clauses 3 to 5 inclusive below shall be suspended during any period in which the Email Continuity.cloud Service is in an activated state.

3. 100% Service Availability

3.1. This Service Availability Service Level will only operate if Customer utilizes one or more of the Email Security Services or Web Services.
3.2. In relation to the Email Security Services, this Service Availability Service Level means the ability to establish a SMTP session on port 25 of the Designated Tower Cluster, as measured by Symantec Tracker. This Service Level shall only apply if the Designated Tower Cluster is able to:

a) receive Customer's inbound Email on behalf of Customer's domain on a 24x7 basis; and
b) accept Customer's outbound Email from a correctly configured Customer SMTP host on behalf of Customer's domain(s) on a 24x7 basis.

3.3. In relation to the Web Services, this Service Availability Service Level means the availability of the Web Services to accept Customer's outbound Web requests and shall only apply if Customer host, gateway devices or proxy(s) are correctly configured on a 24x7 basis.
3.4. If in any calendar month Service Availability is below one hundred percent (100%), Customer may submit a Credit Request and may receive a Service Credit for the following percentage credit:

Percentage Service Availability Per Calendar Month	Percentage credit of Monthly Charge
< 100% but >= 99%	25

< 99% but >= 98.0%	50
< 98.0%	100 and termination of affected Service at Customer's discretion

3.5. In the event Service Availability falls below ninety eight percent (98%) in any calendar month, Customer shall be entitled to terminate the affected Service and receive a pro rata refund of charges paid in advance for the affected Service for the period after termination.

4. 100% Email Delivery

4.1. This Email Delivery Service Level will only operate if Customer utilizes one or more of the Email Security Services.

4.2. Symantec will deliver 100% of all Email sent to or from Customer subject to the following:

a) the Email must have been received by Customer's Designated Tower Cluster; and

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

4.3. Subject to Clauses 4.1 and 4.2 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 Email Security Services upon thirty (30) calendar days prior written notice.

5. Email Latency – 60 Seconds

5.1. Subject to Clause 5.2, this Email Latency Service Level will only operate if Customer utilizes one or more Email Security Services.

5.2. This Email Latency Service Level shall not apply to the Policy Based Encryption Service.

5.3. If in any calendar month the average roundtrip time (as measured by the Symantec Tracker) for Emails sent every 5 minutes to and from every Email Security Services Tower within Customer's Designated Tower Cluster exceeds the delays stated in the table below, Customer may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Average roundtrip time of 100% of measurements (in minutes and seconds)	Percentage credit of Monthly Charge
> 1 min but <= 1min 30 secs	25
> 1min 30secs but <= 2 mins	50
> 2 mins but <= 2mins 30 secs	75
> 2 mins 30 secs	100

5.4. This Email Latency Service Level will not operate:

a) If Customer has not supplied Symantec with a Validation List and Customer suffers a Denial of Service attack;

b) During periods of delay caused by a mail loop from/to Customer's systems.

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

6. Web Latency – 0.1 Seconds

6.1. This Web Latency Service Level will only operate if Customer utilizes one or more Web Services.

6.2. This Web Latency Service Level shall only apply to objects of 1MB or less.

6.3. If the average scanning time of Web content, measured from when Symantec receives the content to the point of Symantec's attempted transmission of the content, calculated over the course of a calendar month is less than 100% in accordance with the table below, Customer may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Average percentage of web content scanning within 100 milliseconds	Percentage credit of Monthly Charge
< 100% but >= 99%	25
< 99% but >= 98%	50
< 98% but >= 97%	75
< 97%	100 and termination of affected Service at Customer's discretion

7. Spam – False Positives 0.0003%

7.1. This Spam False Positive Service Level will only operate if Customer uses the Email AntiSpam.Cloud Service and implements the Symantec Spam Recommended Settings. Furthermore, this Service Level will apply to inbound E mails only.

7.2. Where the average Spam False Positive capture rate rises above 0.0003% of Customer's Email traffic in any calendar month Customer may be submit a Credit Request and may receive a Service Credit in accordance with the table below:

Percentage Spam False Positive capture rate during the calendar month	Percentage credit of Monthly Charge
>0.0003 but <= 0.003	25
> 0.003 but <= 0.03	50
>0.03 but <= 0.3	75
>0.3	100

7.3. The following Emails will not constitute Spam False Positive Emails for the purposes of this Service Level:

a) Emails which do not constitute 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 which are sent from a compromised machine;
e) Emails which are sent from a machine which is on a third party block-list;
f) Emails which have at least 80% of the same content.
g) Emails intercepted by outbound spam scanning.

8. 99% Spam Capture Rate

8.1. This Spam Capture Service Level will only operate if Customer uses the Email AntiSpam.Cloud Service and implements the Spam Recommended Settings. The provisions of this Service Level correspond to the number of Spam False Negatives measured in a calendar month. Furthermore, this Service Level will apply to inbound Emails only.

8.2. Where Symantec has not met the Spam Capture rate in any calendar month Customer may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Percentage Spam Capture rate during the calendar month	Percentage Credit of Monthly Charge
>98% - <= 99%	25
> 97% - <= 98%	50
> 96% - <= 97%	75
< 96%	100

8.3. This Spam Capture Service Level will not operate where the Email was not sent to a legitimate address.

8.4. 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 shall be entitled to a Service Credit equal to 100% of the Monthly Charge.

9. Spam Service Credit Requests

9.1. In order to be eligible for credit under Clauses 7 and 8 Customer must report and send suspected False Positive or 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 Positive or Spam False Negative and will record the finding. At the end of the calendar month, Customer must submit a Credit Request if it is seeking a Service Credit.

10. Email Virus Protection – 100% Known and Unknown

10.1. This Email Virus Protection Service Level will only apply if Customer uses the Email AntiVirus.cloud Service.

10.2. If Customer's systems are infected by one or more Known or Unknown Viruses, by an Email that passed through the Email AntiVirus.cloud Service, in any calendar month, Customer may be entitled to a Service Credit in the amount stated below. Customer must notify Symantec and such notification must be logged and validated by Symantec's support call records to confirm that a Virus has been passed to Customer through the Email AntiVirus.cloud Service. Customer must submit a Credit Request, and if validated, will receive a Service Credit equal to 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) whichever is the lower. The remedy set out in this Clause shall be the sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise in respect of any infection by a Virus passed to Customer or a third party through the Service. For the avoidance of doubt, the remedy set out in this Clause shall not apply in cases of deliberate self-infection.

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

10.4. In the event that Symantec detects, but does not stop a Virus-infected Email, Symantec will promptly notify Customer's designated Support Contact(s), providing sufficient information to enable Customer to identify and delete the Virus-infected Email. If such notification results in a prevention of infection the remedy set out above shall not apply. If Customer fails to promptly act upon the notification from Symantec, the remedy set out above shall not apply.

10.5. The Email AntiVirus.cloud Service will scan as much of the Email and its attachments as possible. It may not be possible to scan attachments with content which 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.

10.6. This Email Virus Protection Service Level shall not operate in relation to Viruses that have been intentionally released by Customer.

10.7. This Email Virus Protection Service Level shall not apply with respect to other types of malware, including, but not limited to; Trojans; Phishing; Spyware; Adware; or URL links to websites hosting malicious content.

11. Email Virus False Positives 0.0001%

11.1. This Email Virus False Positive Service Level will only operate if Customer uses the Email AntiVirus.cloud Service.

11.2. Where the Email Virus 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:

Percentage Email Virus False Positive capture rate during the calendar month	Percentage credit of Monthly Charge
>0.0001 but <= 0.001	25
> 0.001 but <= 0.01	50
>0.01 but <= 0.1	75
>0.1	100

12. Web Virus Protection – 100% Known

12.1. This Web Virus Protection Service Level will only apply if Customer uses the Web v2 Protect.cloud Service.

12.2. If Customer's systems be infected by one or more Known Viruses, by a URL that passed through the Web v2 Protect.cloud Service, in any calendar month Customer may be entitled to a Service Credit in the amount stated below. Customer must notify Symantec and such notification must be logged and validated by Symantec's support call records to include details of the URL from which the item was downloaded, confirming that a Known Virus has been passed to Customer through the Web v2 Protect.cloud Service, Customer must submit a Credit Request and, if validated, will receive a Service Credit equal to 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) whichever is the lower. The remedy set out in this Clause shall be the sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise. For the avoidance of doubt, the remedy set out in this Clause shall not apply in cases of deliberate self-infection or deliberate download of known malicious code by Customer.

12.3. Customer's systems are deemed to be infected if a Known Virus contained in a web transaction received through the Web v2 Protect.cloud Service has been activated within Customer's systems either automatically or with manual intervention.

12.4. In the event that Symantec detects but does not stop a Known Virus as part of a URL which passed through the Symantec Web v2 Protect.cloud Service, Symantec will promptly notify Customer, providing sufficient information to enable Customer to identify and delete the item. If such notification results in a prevention of infection the remedy set out in the Clause above shall not apply. If Customer fails to promptly act upon the notification from Symantec, the remedy set out above shall not apply.

12.5. The Web v2 Protect.cloud Service will scan as much of the Web item downloaded as possible. It may not be possible to scan items that are encapsulated or tunneled for communication purposes via the supported Web Protocols (HTTP, and FTP over HTTP), conveyed over HTTPS, compressed or modified from their original form for distribution, product license protection, download or update, or content which is under the direct control of the sender (for example,

password protected and/or encrypted items). Such items and/or attachments are excluded from the Service Level and the remedy set forth above shall not apply.

13. 24x7 Technical Support and Fault Response

13.1. Symantec will on a twenty-four (24) hours/day by seven (7) days/week basis:

a) provide technical support to Customer for problems with the Service; and
b) liaise with Customer to resolve such problems.

13.2. Whenever a Customer raises a problem, fault or request, for service information via telephone or Email with Symantec, its priority level is determined and it is responded to as defined in the table below:

Priority Level	Definition	Response Target	Percentage Credit of Monthly Charge for Failure to Meet Target
Severity 1	Loss of Service	95% of calls responded to within 2 hours	15
Severity 2	Partial loss of Service or Service impairment	85% of calls responded to within 4 hours	10
Severity 3	Potentially Service affecting or non-Service affecting information request	75% of calls responded to within 8 hours	5

13.3. 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 Service Level.

13.4. Subject to Clause above, if Customer believes that it has experienced a delay in Symantec response to a request (outside the parameters defined in Clause 13.2 above) it may be entitled to a Service Credit in accordance with the table above. Credit Requests must state the time, date and the log number of the incident.

14. Archiving.cloud (P) Service Availability

14.1. The provisions of the Clauses 14 and 15 shall apply to the Archiving.cloud (P) Service only.

14.2. The Archiving.cloud (P) Service will be Available 99.9% of each calendar month, exclusive of Planned Maintenance and emergency maintenance windows. In this case, "Available" is defined as the Symantec hosted Infrastructure being ready to accept and archive Email. For the purposes of calculating non-availability the following criteria will apply: (i) the measurement will be performed by Symantec's monitoring systems (such measurement may be provided to Customer upon written request), (ii) monitoring will occur in 5 minute intervals with two successive failures required to be an outage, (iii) only the Symantec hosted Infrastructure will be measured and such measurement excludes any non-availability as a result of an Email Archiving Appliance outage, a Customer network outage, or an Internet outage.

14.3. For each one (1) percent or part thereof of non-availability beyond the availability target of 99.9% under this Clause 14 in the calendar month in question, Customer will be entitled to a Service Credit equivalent to 10% of the monthly charges due to Symantec for the Service, subject to a maximum of 100% of the Monthly Charge. Customer may terminate the Archiving.cloud (P) Service, at its sole option, if at any time this Availability falls below ninety percent (90%) in any calendar month.

15. Archiving.cloud (P) Service - Appliance Service Level

15.1. If an Email Archiving Appliance fails during the warranty period for reasons covered by the Symantec Limited Warranty (as defined in documentation received with the Email Archiving Appliance), Symantec will, at no cost to Customer, work with Customer to trouble-shoot the Email Archiving Appliance (which may require VPN access to the Email Archiving Appliance) within four (4) hours of receiving notification of the problem from Customer during regional business hours and within eight (8) hours of receiving notification of the problem outside of regional business hours. Within two (2) business days of receiving notification of the problem, Symantec will either:

a) notify Customer that the Email Archiving Appliance is functioning properly and that the problem does not originate with the Email Archiving Appliance or the Software; or
b) repair the Email Archiving Appliance by means of hardware and/or software; or
c) notify Customer that a replacement Email Archiving Appliance is required; or

d) if Symantec is unable to repair or replace the Email Archiving Appliance, refund the monthly charges for the Archiving.cloud (P) Service for the current Term and terminate the Archiving.cloud (P) Service.

15.2. Should Symantec be obligated under Clause 15.1.c. above to provide a replacement Email Archiving Appliance, Symantec shall deliver such replacement Email Archiving Appliance to Customer's site within four (4) business days from the time Symantec notifies Customer that a new Email Archiving Appliance is needed.

15.3. Should Symantec be obligated under Clauses 15.1.b. and 15.1.c. above to repair or replace the Email Archiving Appliance or Software and fail to do so within the time-frames set out in Clauses 15.1. and 15.2. Symantec will refund Customer 5% of the Monthly Charge for the Service for every calendar day in delay past such time frame, up to a maximum of 100% of the Monthly Charge.

15.4. The foregoing terms in this Clause 15 shall be Customer's sole and exclusive remedy with respect to any defect or breach of warranty with respect to the Email Archiving Appliance.

16. Email Continuity.cloud Service

16.1. The provisions of this Clause 16 shall apply to the Email Continuity.cloudService only.

16.2. Email Continuity.cloud will be Available 99.9% of each calendar month, exclusive of Planned Maintenance and emergency maintenance windows. In this case, "Available" is defined as the Symantec hosted Infrastructure being ready to synchronize key system and User information. For the purposes of calculating non-availability the following criteria will apply: (i) the measurement will be performed by Symantec's monitoring systems (such measurement may be provided to Customer upon written request), (ii) only the Symantec hosted Infrastructure will be measured and such measurement excludes any non-availability as a result of a Customer network outage, a third party outage, or DNS issues outside of the direct control of Symantec.

16.3. For each one (1) percent or part thereof of non-availability beyond the availability target of 99.9% under this Clause 16.1. in the calendar month in question, Customer will be entitled to a credit equivalent to ten per cent (10%) of the monthly charges due to Symantec in relation to the Email Continuity.cloud Service, subject to a maximum of 100% of the Monthly Charges for the Service. Customer may terminate the Email Continuity.cloud Service, at its sole option, if at any time this Availability falls below ninety percent (90%) in any calendar month.

17. Symantec Email Continuity Archive.cloud or Symantec Email Continuity Archive Lite.cloud Service

17.1. The provisions of this Clause 17 shall apply to Symantec Email Continuity Archive.cloud Service and Symantec Email Continuity Archive Lite.cloud Service only.

17.2. The Symantec Email Continuity Archive.cloud Service and Symantec Email Continuity Archive Lite.cloud Service shall be available 99.95% of each calendar month. Availability shall be calculated by dividing the total number of hours that the Symantec Email Continuity Archive.cloud Service or Symantec Email Continuity Archive Lite.cloud Service (as applicable) was unavailable (excluding any periods of Customer network outages, maintenance, or DNS issues outside of the direct control of Symantec) by the total number of planned available hours of the Symantec Email Continuity Archive.cloud Service or Symantec Email Continuity Archive Lite.cloud Service (as applicable) in the calendar month in question.

17.3. For each one (1) percent of non-availability beyond the availability target of 99.95% under this Clause 16 in the calendar month in question, Customer shall be entitled to a Service Credit equivalent to the charges paid to Symantec in relation to the Symantec Email Continuity Archive.cloud Service or Symantec Email Continuity Archive Lite.cloud Service (as applicable) for one (1) calendar day of the Symantec Email Continuity Archive.cloud Service or Symantec Email Continuity Archive Lite.cloud Service.

18. Symantec Enterprise Vault.cloud Service or AdvisorMail on Symantec.cloud Service

18.1. The provisions of this Clause 18 shall apply to Symantec Enterprise Vault.cloud Service and AdvisorMail on Symantec.cloud Service.

18.2. Symantec shall provide 99.99% availability for Symantec Enterprise Vault.cloud Service and AdvisorMail on Symantec.cloud Service. If availability for a full calendar month falls below 99.99%, subject to Clause 18.3 below Customer will be entitled to a Service Credit in accordance with the table below.

Availability	Percentage Credit of Monthly Charge
<99.99% but ≥99.9%	5% of Monthly Charge
<99.9% but ≥98.0%	10% of Monthly Charge

<98.0% but ≥95.0%	15% of Monthly Charge
<95.0% but ≥89.9%	25% of Monthly Charge
<89.9%	2.5% of Monthly Charge for every 1% of lost availability up to a maximum of 100% of the Monthly Charge

18.3. Credit Requests must include the dates and times of unavailability. Symantec will compare the information provided by Customer with availability monitoring data maintained by Symantec. In response to a Credit Request, a Service Credit shall be issued if the unavailability triggers a credit pursuant to the table in Clause 18.2 above. The Service Credit described in this Clause 18.3 shall be Customer's sole and exclusive remedy in connection with any unavailability. Unavailability for Planned Maintenance or emergency maintenance is excluded from availability calculations.

19. Symantec Web Security Archiving.cloud

19.1. The provisions of this Clause 19 shall apply to the Symantec Web Security Archiving.cloud Premium Service only.

19.2. The Symantec Web Security Archiving.cloud Premium Service shall be available 99.9% of each calendar month. Availability shall be calculated by dividing the total number of hours that the Symantec Web Security Archiving.cloud Premium Service (as applicable) was unavailable (excluding any periods of Customer network outages, maintenance, or other issues outside of the direct control of Symantec) by the total number of planned available hours of the Symantec Web Security Archiving.cloud Premium Service (as applicable) in the calendar month in question.

19.3. For each 1% of non-availability beyond the availability target of 99.9% under this Clause 19.3. in the calendar month in question, Customer will be entitled to a Service Credit equivalent to 10% of the Monthly Charge due to Symantec in relation to the Symantec Web Security Archiving.cloud Premium Service (as applicable), subject to a maximum of 100% of the Monthly Charge in any calendar month. Customer may terminate either the Symantec Web Security Archiving.cloud Service at its sole option if at any time this availability falls below 90% in any calendar month.

19.4. The Service Credit described in Clause 19.3. shall be Customer's sole and exclusive remedy in connection with any unavailability of the Service.

20. Symantec Endpoint Protection Small Business Edition 2013

20.1. The provisions of this Clause 20 shall apply to the Symantec Endpoint Protection Small Business Edition 2013 Service only.

20.2. The Service will be Available 100% of each calendar month, exclusive of Planned Maintenance and emergency maintenance windows. In this case, "Available" is defined as the Symantec hosted Infrastructure being ready to synchronize policy information. For the purposes of calculating non-availability the following criteria will apply: (i) the measurement will be performed by Symantec's monitoring systems (such measurement may be provided to Customer upon written request), (ii) only the Symantec hosted Infrastructure will be measured and such measurement excludes any non-availability as a result of a Customer network outage, a third party outage, or DNS issues outside of the direct control of Symantec.

20.3. For each one (1) percent or part thereof of non-availability beyond the availability target of 100% under this Clause 20.3 in the calendar month in question, Customer will be entitled to a Service Credit equivalent to 10% of the Monthly Charges due to Symantec for the Service, subject to a maximum of 100% of the Monthly Charge. Customer may terminate the Service, at its sole option, if at any time this availability falls below 90% in any calendar month.

20.4. The Service Credit described in this Clause 20.3. shall be Customer's sole and exclusive remedy in connection with any unavailability of the Service.

21. Symantec Backup Exec.cloud

21.1. The provisions of this Clause 21 shall apply to the Symantec Backup Exec.cloud Service only.

21.2. Symantec Backup Exec.cloud will be Available 100% of each calendar month, exclusive of Planned Maintenance and emergency maintenance windows. In this case, "Available" is defined as the Symantec hosted Infrastructure being ready to synchronize policy information. For the purposes of calculating non-availability the following criteria will apply:

a) the measurement will be performed by Symantec's monitoring systems (such measurement may be provided to Customer upon written request),

b) b) only the Symantec hosted Infrastructure will be measured and such measurement excludes any non-availability as a result of Customer network outage, a third party outage, or DNS issues outside of the direct control of Symantec.

21.3. For each one (1) percent or part thereof of non-availability beyond the availability target under this Clause 21.3 in the calendar month in question, Customer will be entitled to a Service Credit equivalent to 10% of the Monthly Charge due to Symantec for the Service, subject to a maximum of 100% of the Monthly Charge. Customer may terminate the Symantec Backup Exec.cloud Service, at its sole option, if at any time this availability falls below ninety percent (90%) in any calendar month. The Service Credit described in this Clause 21.3 shall be Customer's sole and exclusive remedy in connection with any unavailability for the Symantec Backup Exec.cloud Service.

END OF SCHEDULES