Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Schedule 1
General Service Description

THOSE SERVICE DESCRIPTIONS AND/OR SLAs LISTED IN SCHEDULES 2 AND 3 BELOW NOT ORDERED BY CUSTOMER IN SECTION B OF THE AGREEMENT SHALL BE INAPPLICABLE TO CUSTOMER.

1. Definitions

The capitalized terms, below, shall have the following meanings for the purposes of the Agreement:

"Customer"	means the contracting end user organisation/enterprise.
"Volume Email"	means a group of more than five thousand (5000) Email messages with substantially similar content sent or received in a single operation or a series of related operations;
"Email"	means any SMTP message sent or received via the Service;
"Non-Severable Service Bundle"	means a bundle of Services as stipulated in Section B "Service and Charges" of the Agreement and Clause 7 below, which are subject to the provisions of Clause 3.6 of the Agreement;
"Member"	means the Customer and organizations with whom the Customer creates an encrypted network by utilising the Boundary Encryption Service;
"Normal Working Hours"	means between 8:30am and 5:30pm UK time, Monday to Friday excluding public holidays as recognized in the UK;
"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;
"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";
"Spam"	means unsolicited commercial Email;
"Tower"	means a cluster of load balanced Email servers;
"User"	means a person, mailbox or machine that uses the Service; and
"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.

2. Introduction

2.1 Interoute is a non exclusive reseller of Symante MessageLabs Services.

2.2 Symantec is a managed services provider specialising in Internet-level Email, Instant Messaging and Web security.

2.3 The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis from Symantec's Global Operations Centre. The Service is monitored for hardware availability, service capacity and network resource utilisation.

2.4. If Symantec is unable to deliver Email to a Customer's mail server, Symantec will store the Customer's inbound Email for up to seven (7) days pending delivery.

2.5. The Service is available to Customers who are permanently connected to the Internet with a fixed IP address. It cannot be provided to Customers whose systems are connected to the Internet via dial-up or ISDN lines or whose IP address is dynamically allocated.

2.6. For all incoming Email the IP reputation of the sender is ascertained. Email originating from a disreputable source (such as a spammer) will be slowed down to minimize network capacity impact.

2.7 The Customer should configure its email servers to limit the number of recipients per outbound SMTP connection to less than 500. A recipient is an individual email address. An email group may contain one or many recipients. If an inbound or outbound Email includes more than 500 recipients in an SMTP connection, Symantec will process the first 500 recipients and send an SMTP reply code to the sending email server requiring the sending server to resend the Email to the remaining recipients.

3. Planned Maintenance

3.1. For the purposes of this Clause 3, "Planned Maintenance" means periods of maintenance of which the Customer has been given seven (7) days prior notification by Symantec and which may cause disruption of Service due to non availability of Tower(s). Planned Maintenance shall not accumulate to more than eight (8) hours per calendar month and in any case shall not take place between 8am and 6pm (in the time zone in which a Tower is located).

3.2. Wherever possible, Planned Maintenance will be carried out without affecting the Service. This will generally be achieved by carrying out Planned Maintenance during periods of anticipated low traffic and by carrying out Planned Maintenance on part, not all, of the network at any one time. During Planned Maintenance periods the traffic may be diverted round sections of the network not undergoing maintenance in order to minimize disruption to the Service.

3.3. Where emergency maintenance is necessary and is likely to affect the Service, Symantec will endeavour to inform the affected parties and will post an alert message on ClientNet as soon as possible and in any case within one (1) hour of the start of the emergency maintenance.

4. ClientNet

4.1. An integral part of the Service is Symantec's internet-based configuration, management and reporting tool called ClientNet. ClientNet is made available to the Customer via a secure password protected login which should not be disclosed to a third party. ClientNet provides the facility for the Customer to view data and statistics on their use of the Service and offers a number of configuration and management facilities.

5. Technical Support

5.1. Interoute will provide first line service support to the customer for the services contracted. Interoute will liaise with Symantec to resolution of service issues.

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

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

6. Customer Service

6.1. Interoute working with Symantec will provide customer service during Normal Working 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 queries.

6.2. Unless stated otherwise in the relevant Service Description, on receipt of a fully completed and actionable order or Service Change Request, Interoute working with the Symantec Global Provisioning Team will aim to provision the Service within twenty-seven (27) Normal Working Hours, provided that all the phases of technical due diligence have been completed.

7. Non-Severable Service Bundles

7.1 Non-Severable Service Bundles (if selected in Section B "Service and Charges" of the Agreement) comprise the following constituent Services:

Current Non-Severable Service Bundle Name	Constituent Services (Legacy Constituent Service)	Legacy Non-Severable Service Bundle Name
Symantec MessageLabs Email Protect.cloud	Email AV, Email AS	MessageLabs Email Protect
Symantec MessageLabs Email Control.cloud	Email IC, Email CC	MessageLabs Email Control
Symantec MessageLabs Email Safeguard.cloud	Email AV, Email IC, Email AS, Email CC	MessageLabs Email Safeguard (or MessageLabs Email Protect & Control)
Symantec MessageLabs Web v2 Protect & Control.cloud	Web v2 Protect, Web v2 URL	MessageLabs Web Protect & Control
Not Offered	(Email AV, Email AS, Web AVASv2)	MessageLabs Email Protect & Web Protect
Not Offered	(Email AV, Email IC, Email AS, Email CC, Web AVASv2)	MessageLabs Email Protect & Control & Web Protect
Not Offered	(Email AV, Email AS, Web AVASv2, Web URLv2)	MessageLabs Email Protect & Web Protect & Control
Symantec MessageLabs Email & Web Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Web v2 Protect, Web v2 URL (Email AV, Email IC, Email AS, Email CC, Web AVASv2, Web URLv2)	MessageLabs Email & Web Safeguard (or MessageLabs Email & Web Protect & Control)
Symantec MessageLabs 2 Email Services Bundle	2 Email Services from Email AV, Email IC, Email AS, or Email CC	MessageLabs 2 Email Services Bundle
Symantec MessageLabs 3 Email Services Bundle	3 Email Services from Email AV, Email IC, Email AS, or Email CC	MessageLabs 3 Email Services Bundle
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving (P))	MessageLabs Email Protect & Control & Archiving (P)
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving Lite (P))	MessageLabs Email Protect & Control & Archiving Lite (P)
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving Premium(P))	MessageLabs Email Protect & Control & Archiving Premium(P)
Symantec MessageLabs Security Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Web AVASv2, Web URLv2, IMSS	MessageLabs Security Safeguard
Symantec MessageLabs Complete Email Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud	MessageLabs Complete Email Safeguard
Symantec MessageLabs Complete Email & Web Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud, Web v2 Protect, Web v2 URL	MessageLabs Complete Email & Web Safeguard
Symantec MessageLabs Ultimate Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud, Web v2 Protect, Web v2 URL , IMSS	MessageLabs Ultimate Safeguard
Symantec Enterprise Vault.cloud	Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud	MessageLabs Email Archiving L or Email Archiving.cloud (L)
Symantec Enterprise Vault Enhanced.cloud	Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec EnterpriseVault Mailbox Continuity.cloud	Messagelabs Email Enhanced Archive L or Email Enhanced Archiving.cloud (L)

8. Legacy Service Names

8.1 For Customers who purchased Services prior to June 1, 2011, the Service Names in this document are referenced using different nomenclature than the original names for the legacy Services. The chart below shows the corresponding legacy terms for the revised nomenclature so Customers can determine which sections of the document apply to the Services purchased under the previous nomenclature.

Legacy Service Name	Current Service Name
MessageLabs Email Anti-Virus	Symantec MessageLabs Email Anti-Virus.cloud
MessageLabs Email Image Control	Symantec MessageLabs Email Image Control.cloud
MessageLabs Email Anti-Spam	Symantec MessageLabs Email Anti-Spam.cloud
MessageLabs Email Content Control	Symantec MessageLabs Email Content Control.cloud
MessageLabs Boundary Encryption	Symantec MessageLabs Email Boundary Encryption.cloud
MessageLabs Web Anti-Spyware and Anti-Virus Service v2	Symantec MessageLabs Web v2 Protect.cloud
MessageLabs Web URL Service v2	Symantec MessageLabs Web v2 URL.cloud
MessageLabs Email Archiving P	Symantec MessageLabs Email Archiving.cloud (P)
MessageLabs Enterprise Instant Messenger (EIM)	Symantec MessageLabs EIM.cloud
MessageLabs EIM Connect	Symantec MessageLabs EIM Connect.cloud
MessageLabs EIM Communicate	Symantec MessageLabs EIM Communicate.cloud

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

MessageLabs Policy Based Encryption	Symantec MessageLabs Policy Based Encryption.cloud
MessageLabs Email Continuity (EC), or Symantec MessageLabs Email Continuity.cloud (D)	Symantec Email Continuity.cloud (EC)
Schemus Tool	Schemus Tool
MessageLabs Instant Messaging Security Service (IMSS)	Symantec MessageLabs Instant Messaging Security.cloud
MessageLabs Email Archiving D, or Symantec MessageLabs Email Archiving.cloud (D)	Symantec Email Continuity Archive.cloud
MessageLabs Email Archiving Lite D, or Symantec MessageLabs Email Archiving.cloud Lite (D)	Symantec Email Continuity Archive Lite.cloud
MessageLabs Volume Mail	Symantec MessageLabs Volume Mail
Hosted Endpoint Protection	Symantec Endpoint Protection.cloud
MessageLabs Personal Archive L or Symantec MessageLabs Email Personal Archiving.cloud (L)	Symantec Enterprise Vault Personal.cloud
MessageLabs Email Discovery Archive L, or Symantec MessageLabs Email Discovery Archiving.cloud (L)	Symantec Enterprise Vault Discovery.cloud
MessageLabs Personal Archive L for BlackBerry®, or Symantec MessageLabs Personal Archive for BlackBerry®.cloud (L)	Symantec Enterprise Vault.cloud Blackberry Option
MessageLabs Email Archiving Premiium L , or Symantec MessageLabs Email Premium Archiving.cloud (L)	AdvisorMail on Symantec.cloud™
MessageLabs Email Archiving IM Premium L, or Symantec MessageLabs Email Premium Archiving.cloud for IM (L)	AdvisorMail IM Option on Symantec.cloud™
MessageLabs Email Archiving Bloomberg Message Premium L, or Symantec MessageLabs Premium Archiving.cloud for Bloomberg	AdvisorMail Bloomberg Option on Symantec.cloud™
MessageLabs Email Archive Import Service L, or Symantec MessageLabs Email Archiving.cloud (L) Import	Symantec Enterprise Vault.cloud Data Import Option
MessageLabs Email Continuity L, or Symantec MessageLabs Email Continuity.cloud (L)	Symantec Enterprise Vault Mailbox Continuity.cloud
MessageLabs User Roaming Agent Service (“Smart Connect”)	Symantec MessageLabs Web v2 Smart Connect.cloud

Schedule 2
Service Descriptions

Appendix 1 – Symantec MessageLabs Email Anti-Virus.cloud Service

1. Overview

1.1. The Symantec MessageLabs Email Anti-Virus.cloud Service ("Email AV") is Symantec's Internet-level Email Virus scanning Service. The Customer's inbound and outbound Email including all attachments, macros or executables are directed through Email AV using DNS and MX record settings.

1.2. The Email and attachments are scanned by multiple industry leading anti-virus products including Symantec's own heuristic scanner, Skeptic™.

2. Alert Messages

2.1. If a Customer's inbound Email or attachments are found to contain a Virus, an automatic alert may, if selected by the Customer, be despatched to the sender and intended recipient by way of notification. With a Customer's outbound Email the Service may notify the sender only and not the intended recipient. User notifications may also be sent to an Email administrator in both cases. The infected Email is forwarded to a secure server pending automatic destruction after seven (7) days, provided that it is not transported as a mass mailer virus, in which case it will be deleted immediately.

2.2. In the case of a major breakout of a new Virus, an alert message will be posted on ClientNet.

3. Configuration

3.1. ClientNet can be used for customising banner texts, releasing Virus-infected Email and setting maximum Email sizes.

4. Releasing a Virus-Infected Email

4.1. Where a Virus-infected Email is shown to be releasable, it can be released from the secure server using ClientNet. The Email will be released either to the first address of the original recipient list or to a specified address previously notified to Symantec and logged by Symantec in ClientNet (Note: these addresses may be group Email names or aliases in which case the Email will be released to all addressees in the group or alias). Optionally the Virus-infected Email may be released to an alternative address by Symantec on receipt of the appropriate Release Authorization Form. Symantec will only act on requests authorized by Customers to forward Virus-infected Email. Symantec will not return Virus-infected Email to the sender. Symantec will not forward Virus-infected Email to third parties. Certain Virus-infected Emails sent to the customer are not releasable due to them containing a Virus which is particularly infectious or damaging. These are shown on ClientNet as being not releasable.

5. Email AV Terms and Conditions

5.1. If requested to release a Virus-infected Email, Symantec will release it within eight (8) Normal Working Hours of receipt of a duly authorized release request.

Appendix 2 – Symantec MessageLabs Email Image Control.cloud Service

1. Overview

1.1. The Symantec MessageLabs Email Image Control.cloud service ("Email IC") is Symantec's Internet-level Email image control service which is designed to detect pornographic images contained in image files.

2. Service Description

2.1. The Customer's inbound and outbound Email can be scanned using Image Composition Analysis (ICA) for pornographic images contained in image files attached to Email.

2.2. If a Customer's inbound or outbound Email is suspected to contain a pornographic image, one of a number of actions will be taken depending on the configuration options selected by the Customer.

3. Configuration

3.1. On receipt of a fully completed and accepted order, Symantec will make Email IC available to the Customer. Initially Email IC will be enabled for each of the Customer's domains. The Customer is responsible for setting the configuration options for Email IC for each domain according to the Customer's needs. The Customer configures Email IC using ClientNet.

3.2. Options are available for specifying the level of detection sensitivity to which the ICA filter operates. Sensitivity can be set to High, Medium or Low. These settings are particularly subjective, however, as a guide more images will be suspected to be pornographic at High sensitivity and fewer images will be suspected to be pornographic at Low sensitivity.

3.3. Options are available for defining the actions to be taken on detecting a suspected pornographic image. These options may be set independently for inbound and outbound Email and should be set in line with the Customer's existing acceptable computer use policy (or its equivalent). These options are:

3.3.1. log suspected Email (provides statistics viewable via ClientNet);

3.3.2. tag suspected Email within the header (for inbound Email only);

3.3.3. copy suspected Email to a pre-defined Email address;

3.3.4. redirect suspected Email to a pre-defined Email address;

3.3.5. delete suspected Email;

3.3.6. tag suspected Email in the subject line.

3.4. Where the Customer has identified trusted Email senders or recipients for the administration of Email IC, the Email of such senders and recipients will not be scanned by Email IC.

4. Reporting

4.1. If the chosen options in Clause 3.3 of this Appendix are to redirect or delete Email containing a suspected pornographic image, then an automatic alert can be despatched to the sender. If the Email is inbound to the Customer an automatic alert can also be sent to the intended recipient. Such automatic alerts may be activated and deactivated by the Customer through ClientNet.

4.2. Reporting on the effectiveness of Email IC is provided through ClientNet where statistics are available on the numbers of inbound and outbound Emails suspected of containing pornographic images. ClientNet may be configured to generate reports which are sent by Email to the Customer on a weekly or monthly basis.

5. Email IC Terms and Conditions

5.1. NO PORNOGRAPHIC IMAGE DETECTION SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE INTEROUTE NOR SYMANTEC CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO DETECT A PORNOGRAPHIC IMAGE OR FOR WRONGLY IDENTIFYING AN IMAGE AS SUSPECTED TO BE PORNOGRAPHIC WHICH PROVES SUBSEQUENTLY NOT TO BE SO.

5.2. 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).

5.3. Email IC able to scan for pornographic images embedded in certain versions of Word, Excel, PowerPoint and pdf documents, but not other documents.

5.4. Interoute and Symantec emphasizes that the configuration of Email IC is entirely in the control of the Customer. Email IC is intended to be used solely to enable the Customer to enforce an existing, effectively implemented acceptable computer use policy (or its equivalent). In certain countries it may be necessary to obtain the consent of individual personnel. Interoute and Symantec advise the Customer to always check local legislation prior to deploying Email IC. Interoute or Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of Email IC. The Customer recognizes that the definition of what does and what does not constitute a pornographic image is subjective. The Customer should take this into consideration when configuring the Service.

5.5. If the Customer releases or requests the release of a Virus-infected Email, the released Email will not be scanned by Email IC prior to release.

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Appendix 3 – Symantec MessageLabs Email Anti-Spam.cloud Service

1. Overview

1.1. The Symantec MessageLabs Email Anti-Spam.cloud service ("Email AS") is Symantec's Internet-level Email Anti-Spam service which is designed to protect the Customer from unsolicited or unwanted Email.

2. Service Description

2.1. The Customer's inbound Email may be scanned using a number of different detection methods to determine whether or not it is Spam. If an inbound Email is suspected as being Spam, one of a number of actions will be taken depending on the configuration options selected by the Customer in Clause 3.2 below.

2.2. A private approved senders list may be compiled by the Customer, and by an individual User if the Customer has enabled User level settings. If this detection method is selected and an incoming Email is received from an approved senders listed domain, it will automatically bypass any other selected Spam detection methods.

2.3. A private blocked senders list may be compiled by the Customer, and by an individual User if the Customer has enabled User level settings. If this detection method is selected and an incoming Email is received from a blocked senders listed domain an action will be taken as defined by the configuration options in Clause 3.2 below.

2.4. A number of public blocked senders lists may be used. If any of these detection methods are selected and an incoming Email is received from a domain listed on one of the selected public blocklists an action will be taken as defined by the configuration option in Clause 3.2 below.

2.5. If the Email has not been deleted as a result of being blocked as above and the signaturing system is selected and the action that would be taken as a result of detecting the Email as Spam as is more severe than that already selected as a result of blocked senders list detection, the Customer's inbound Email is scanned using the signaturing system. If an Email is detected by this method as being Spam then action will be taken as defined by the configuration options in Clause 3.2 below. This action will supersede any less severe action previously allocated by any of the blocked senders list methods.

2.6. If the Email has not been deleted as a result of the preceding processes and heuristics detection is selected and the action that would be taken as a result of detecting the Email as Spam as configured by the Customer is more severe than that already selected as a result of detection by the preceding processes, the Customer's inbound Email is scanned using heuristics scanning. If an incoming Email is heuristically detected as being Spam action will be taken as defined by the configuration options in Clause 3.2 below. This action will supersede any less severe action previously allocated by any of the preceding methods.

2.7. Blocked senders/approved senders lists provided by Symantec are given as examples only.

3. Configuration

3.1. On receipt of a fully completed and accepted order via Interoute, Symantec will enable Email AS for the Customer. Initially Email AS will be enabled for each of the Customer's domains. THE CUSTOMER ACKNOWLEDGES THAT EMAIL AS WILL BE PROVISIONED WITH SYMANTEC'S DEFAULT SETTINGS APPLIED FROM THE OUTSET AND THAT IT IS THE CUSTOMER'S SOLE RESPONSIBILITY TO CONFIGURE EMAIL AS THROUGH CLIENTNET TO ITS OWN REQUIREMENTS. The default settings applied for Email AS include the following actions:

3.1.1. Block and delete Email; or
3.1.2. Quarantine Email; and
3.1.3. Use of an approved senders list for IP addresses, domains and email addresses; and
3.1.4. Use of predictive Spam detection (Skeptic).

3.2. Options are available for specifying the actions to be taken should an Email be suspected as being Spam. These options, listed below, are selectable for each of the available detection methods:

3.2.1. tag suspected Email within the header;

3.2.2. tag suspected Email within the subject line;

3.2.3. redirect suspected Email to a pre-defined Email address (which must be on a domain being scanned by the Service);

3.2.4. delete suspected Email;

3.2.5. Spam Quarantine.

4. Spam Quarantine Service Description

4.1. If the Customer configures Spam Quarantine for a domain, each User's Spam Quarantine account will be set up automatically upon the first time that suspected Spam is identified by Email AS and the User will automatically receive an Email notification.

4.2. Spam Quarantine is accessed by the User via the Spam Manager interface.

4.3. Suspected Spam can be stored for a maximum of fourteen (14) days after which it will be automatically deleted. The Customer may purchase extended storage ("Symantec MessageLabs Extended Spam Quarantine") beyond such fourteen (14) day period upon payment of an additional charge calculated on a per User per day basis.

4.4. If Spam Quarantine is not able to accept Email the suspected Spam will be tagged and sent to the recipient.

5. Spam Quarantine Configuration

5.1. The Customer configures Spam Quarantine via ClientNet.

5.2. Default User notifications are set to 5.2.1 below. The User may at any time select one of the following notification options:

5.2.1. Notifications to be received daily;

5.2.2. Notifications to be received at various frequencies;

5.2.3. Notifications not to be received.

5.3. The following release options are available through Spam Manager: (i) Delete Email; (ii) Release Email to original recipient address; (iii) Review text of Email.

5.4. In order to utilize Spam Quarantine the Customer must have registered a Validation List with MessageLabs. The Validation List comprises all valid Email addresses utilized by the Customer. Any recipient address not on the Validation List is deemed invalid and Email will not be delivered to that address.

5.5. Through ClientNet a Customer may control other aspects of Spam Manager: (a) automated or manual notification policy; (b) setup of summary notifications; (c) default language settings; (d) User level settings; (e) preset alias Emails and (f) specialized Users (e.g. Quarantine Administrators).

5.6. The Customer may establish groups of email addresses for Spam Quarantine in order to 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 the Customer's account group or aliasing links in the event that this maximum is exceeded.

6. Reporting

6.1. Reporting on the effectiveness of Email AS is provided through ClientNet. ClientNet may be configured to generate reports which are sent by Email to the Customer on a weekly or monthly basis.

7. Email AS Terms and Conditions

7.1. NO ANTI-SPAM SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE INTEROUTE NOR SYMANTEC CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO DETECT SPAM OR FOR WRONGLY IDENTIFYING AN EMAIL SUSPECTED AS BEING SPAM WHICH PROVES SUBSEQUENTLY NOT TO BE SO.

7.2. Interoute and Symantec emphasize that the configuration of Email AS is entirely in the control of the Customer. Interoute and Symantec recommend that the Customer has an acceptable computer use policy (or its equivalent) in place. In certain countries it may be necessary to obtain the consent of individual personnel. Interoute and Symantec advise the Customer to always check local legislation prior to deploying Email AS. Neither Interoute or Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of Email AS.

Appendix 4 – Symantec MessageLabs Email Content Control.cloud Service

1. Overview

1.1. Symantec MessageLabs Email Content Control.cloud ("Email CC") is Symantec's content control service designed to enable the Customer to configure its own rule based filtering strategy in line with its acceptable computer use policy (or its equivalent) in relation to Email.

2. Service Description

2.1. Email CC allows a Customer to build a collection of rules upon which incoming and outgoing Email is filtered in accordance with this Appendix 4. A rule is an instruction set up by the Customer which is used to identify a particular format of message/attachment or content which has prescribed to it a particular course of action to be taken in relation to the Email.

3. Configuration

3.1. On receipt of a fully completed and accepted order via Interoute, Symantec will enable Email CC for each of the Customer's applicable domains. The Customer is responsible for implementing the configuration options for Email CC for each domain according to the Customer's needs. The Customer configures Email CC via ClientNet.

3.2. The Customer may configure rules on a 'per domain', 'per group' or 'individual' basis.

3.3. Changes made by the Customer to the rules will become effective within 24 hours of such change being made.

3.4. Options are available for defining the action to be taken upon detecting a suspected Email. These options may be set independently for inbound and outbound Email and should be set in line with the Customer's existing acceptable computer use policy (or its equivalent). These options are:

3.4.1. Block and delete suspected Email;

3.4.2. Tag (if inbound) and redirect suspected Email to a specified administrator;

3.4.3. Tag (if inbound) and copy suspected Email to a specified administrator;

3.4.4. Tag (if inbound) header of suspected Email;

3.4.5. Compress Email attachments;

3.4.6. Log only to ClientNet statistics;

3.4.7. Tag in the subject line.

4. Reporting

4.1. Through ClientNet a Customer will be able to review the results of their rules in the form of daily, weekly, monthly and annual summaries organized by both rule and by User.

4.2. Reports containing service activity logs can be generated on a weekly or monthly basis and emailed to the Customer upon request.

4.3. Through ClientNet the Customer is able to activate and deactivate notifications configured by the Customer on a per rule basis.

5. Content Control Support

5.1. Support includes a walkthrough of the Email CC interface including a Service description and Q&A session.

6. Wildcarding

6.1. Email CC works on an exact match of the Customer configured rules. As a specific exception to this, however, wildcarding allows the Customer to configure Email CC through ClientNet to identify certain alphanumeric formulae that follow a specific pattern (e.g. Social Security numbers, National Insurance numbers and credit card information).

7. Content Control Terms and Conditions

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

7.2. Customer accepts and agrees that Symantec may compile and publish default word lists using words obtained from the Customers' custom word lists.

7.3. The Customer recognizes that if Email CC is used in conjunction with the quarantine action of the Email Anti-Spam Service, this may result in suspected Spam being quarantined before it has been filtered by Email CC.

7.4. Email CC is able to scan for content embedded in certain versions of Word, Excel PowerPoint and pdf documents, but not other documents.

7.5. Interoute and Symantec emphasizes that the configuration of Email CC is entirely under the control of the Customer and that the accuracy of such configuration will determine the accuracy of the Email CC Service, therefore neither Interoute or Symantec can accept no liability for any damage or loss resulting directly or indirectly from any failure of the Service to detect or wrongly identify an Email containing suspected content which proves subsequently not to be so.

7.6. Interoute and Symantec recommend that the Customer has an acceptable computer use policy (or its equivalent) in place governing its Users' use of Email and that any template rules supplied by Symantec support such policy. In certain countries it may be necessary to obtain the consent of individual personnel. Interoute and Symantec advise the Customer to always check local legislation prior to deploying Email CC. Interoute nor Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of Email CC.

Appendix 5 – Symantec MessageLabs Email Boundary Encryption.cloud Service

1. Overview

1.1. The Symantec MessageLabs Email Boundary Encryption.cloud Service ("BE") provides encrypted communication channels which enable the Customer to form a secure private Email network (SPEN) with nominated partner organisations ("SPEN Partners"). This configuration is known as "Enforced" encryption.

1.2. Additionally, the Customer can also receive encrypted Emails sent opportunistically from organisations that have TLS-capable mail servers for which there is no Enforced encryption with the Customer if such organisations have TLS-capable mail servers. This configuration is known as "Opportunistic" encryption.

1.3. If the Customer has subscribed to BE but has not explicitly identified any SPEN Partners, the Customer can receive Email sent opportunistically inbound over TLS, and send Emails encrypted opportunistically outbound to non-SPEN Partner organisations.

1.4. The Customer may also configure its email servers for the "Secure Connection" model of BE, in which case:

1.4.1 Email exchanges between Symantec and Customer's Secure Connection 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.

1.4.2 **CUSTOMER ACKNOWLEDGES AND ACCEPTS THAT IF THE SECURE CONNECTION MODEL IS NOT APPLIED TO A PARTICULAR MAIL SERVER, CUSTOMER'S INBOUND AND OUTBOUND EMAILS ORIGINATING FROM OR RECEIVED BY THAT MAIL SERVER SHALL NOT BE SECURED BY TLS ENCRYPTION. ACCORDINGLY, THE CUSTOMER ACKNOWLEDGES AND ACCEPTS THAT IT SHOULD NOT SEND OR RECEIVE SENSITIVE DATA VIA SUCH MAIL SERVERS AND DOES SO ENTIRELY AT ITS OWN RISK**.

1.5 If the Customer is using BE in conjunction with the PBE Service, Symantec's recommended best practice is for the Customer to implement the Secure Connection model of BE on all its mail servers.

1.6 **BE ONLY OPERATES WHEN USED IN CONJUNCTION WITH ONE OF THE FOLLOWING SERVICES AND CANNOT OPERATE AS A STANDALONE SERVICE: EMAIL AV, EMAIL AS, EMAIL IC AND/OR EMAIL CC.**

2. Provisioning and Invoicing

2.1. Interoute and Symantec shall commence charging for BE from the date that Symantec confirms that the Customer's network is technically capable of supporting BE (the "Technical Approval Date").

2.2 Clause 6.2 of Schedule 1 shall not apply to BE. Symantec will aim to provision BE orders and BE change requests within 4 weeks of the Technical Approval Date, provided that all required due diligence has been completed by the Customer.

2.3 In the event that Symantec is required to allocate additional technical resources to the provision of BE due to the Customer failing to perform the required due diligence, Symantec reserves the right to charge additional professional services fees at the rate of £1500/€1500 (depending on the currency in which the Customer is invoiced) per person per day.

3. Configuration

3.1. Customer will define SPEN Partners with whom it wishes to communicate securely by domain. SPEN Partners may be customers or non-customers of BE, however Symantec will not support SPEN Partners directly. Non-SPEN Partner organisations may receive Emails over Opportunistic Outbound TLS as described in Clause 1 above should their mail servers support the receipt of encrypted mail.

3.2. BE is based on the standard 'SMTP over TLS' (Simple Mail Transfer Protocol over Transport Layer Security) ("STARTTLS").

3.3. Both Customer's and the SPEN Partner's mail server must support STARTTLS to enable use of BE.

3.4. BE is supported by selected Towers through which all STARTTLS Email will be routed. Accordingly, Customer nominates which of their domains are to utilize BE.

3.5. When utilising BE in conjunction with the signaturing system functionality of Email AS, Symantec recommends that the Customer includes in its Email AS approved senders list all its SPEN Partner domains. If this recommended best practice is not followed the Customer recognizes and accepts that in certain circumstances involving unavailability of the local signaturing system, Email may be redirected to a remote signaturing system via a public network.

4. Certificates and Authentication

4.1. Where the Customer originates a STARTTLS connection the accepting mail server must provide its certificate for authentication. If the accepting mail server wishes to authenticate the Service then Symantec will supply its client certificate for authentication. If the accepting mail server cannot authenticate the Email will be returned to the Customer.

4.2. Where an external mail server originates a STARTTLS connection, the Service will supply its server certificate for authentication, but will not insist on the external mail server supplying its client certificate for authentication.

4.3. 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 STARTTLS 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 aborted and the Email will be returned to the sender.

5. Encryption Terms and Conditions

5.1. Interoute and Symantec can take no responsibility for the failure of Customer or any third party (including without limitation any SPEN Partner) to fulfil their obligations with regard to registering certificates or for the timeliness or accuracy of such information.

5.2. BE is intended to be used solely to enable Customer to enforce an existing, effectively implemented acceptable computer use policy (or its equivalent). Use of encrypted services in some countries may be subject to legislation. Customer is advised to always check relevant legislation prior to deploying the BE Service. Symantec can accept no liability for any civil or criminal liability that may be incurred by Customer as a result of the operation of BE.

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Appendix 6 – Symantec MessageLabs Web v2 Protect.cloud

1. Overview

1.1. Once the relevant configuration changes are made requests for Web pages and attachments are electronically routed via the Symantec MessageLabs Web v2 Protect.cloud Service ("Web v2 Protect") and digitally examined for viruses.

1. Service Description

2.1. The Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through Web v2 Protect.

2. Configuration

3.1. The configuration settings required to direct this external traffic via Web v2 Protect are made and maintained by the Customer and are dependent on the Customer's technical infrastructure. The Customer should ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed via Web v2 Protect. Where the Customer has Internet services that mandate a direct connection rather than via a proxy, it is the responsibility of the Customer to make the necessary changes to its own infrastructure to facilitate this.

3.2. Access to Web v2 Protect is restricted via Scanning IP i.e. the IP address(es) from which the Customer's web traffic originates. The Scanning IPs are also used to identify the customer and dynamically select customer-specific settings.

3.3. Web v2 Protect will scan appropriate elements of the Web page and its attachments that may contain viruses, malicious code, spyware or adware. It may not be possible to scan certain Web pages, content or attachments (for example, 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 Web v2 Protect unscanned.

3.4. Roaming User Support is an optional feature which extends the Web v2 Protect Service to Users who are not within the corporate network (for example to a User who works from home). The 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 started up. To access the web portal, the User must enter a password and user name. A PAC file template can be downloaded from ClientNet and modified by the Customer.

3. Alerts

4.1. If a Customer's Web page or attachments are found to contain an item identified as a Virus, Spyware or Adware, then access to that Web page or attachment is denied and the Internet user will be displayed an automatic alert Web page. In rare cases, and where one or more elements of the requested content is blocked, it may not be possible to display the alert Web page and the alert page may replace the content of the requested item, but access to the infected page or attachment will still be denied.

4.2. There is a section within the automatic alert Web pages that customers can customize via ClientNet.

4. Reporting

5.1 Reporting on the effectiveness of Web v2 Protect is provided through ClientNet.

5.2 To enable per User or group reporting, the Customer will be required to install the relevant software application (the "Client Site Proxy") in accordance with the installation guidelines. Use of the Client Site Proxy is subject to the End User License Agreement provided with the Client Site Proxy.

5.3 The Customer recognizes that ClientNet detailed reporting data is only stored for a maximum period of forty (40) days and will be not be available to the Customer upon the expiry of this period. ClientNet summary data is available for a maximum period of twelve (12) months.

5.4 The Customer may request an extended reporting period for the ClientNet detailed report of up to a maximum of six (6) months by subscribing to WSS Enhanced Data Retention.

6. General Terms and Conditions

6.1. NO WEB SCANNING SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE INTEROUTE NOR SYMANTEC CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF Web v2 Protect TO DETECT VIRUSES, MALICIOUS CODE, SPYWARE OR ADWARE.

6.2. Interoute and Symantec emphasizes that the configuration of Web v2 Protect is entirely in the control of the Customer. Web v2 Protect is intended to be used solely to enable the Customer to enforce an existing, effectively implemented acceptable computer use policy (or its equivalent). In certain countries it may be necessary to obtain the consent of individual personnel. Interoute and Symantec advise the Customer to always check local legislation prior to deploying Web v2 Protect. Interoute and Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of Web v2 Protect.

6.3 The Customer's web traffic when using Web v2 Protect shall not exceed thirty megabytes (30MB) per User per day (calculated as an average per User across the Customer's total Registered Usage for Web v2 Protect). In the event such daily limit is exceeded, Interoute and Symantec reserve the right to:

6.3.1 withhold provision of or suspend all or part of Web v2 Protect immediately and until such excess use is remedied; or

6.3.2 require the Customer to purchase additional Users to reflect the Customers actual web traffic usage and raise additional invoices and/or make adjustments to subsequent invoices to cover charges for the increase in Registered Usage on a pro-rata basis for the remaining part of the current invoicing period.

Appendix 7 – Symantec MessageLabs Web v2 URL.cloud

1. Overview

1.1. Once the relevant configuration changes are made requests for Web pages and attachments are electronically routed via the Symantec MessageLabs Web v2 URL.cloud Service ("Web v2 URL") and digitally examined.

2. Service Description

2.1. The Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through Web v2 URL.

3. Configuration

3.1. The configuration settings required to direct this external traffic via Web v2 URL are made and maintained by the Customer and are dependent on the Customer's technical infrastructure. The Customer should ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed via Web v2 URL. Where the Customer has Internet services that mandate a direct connection rather than via a proxy, it is the responsibility of the Customer to make the necessary changes to its own infrastructure to facilitate this.

3.2. Access to Web v2 URL is restricted via Scanning IP i.e. the IP address(es) from which the Customer's web traffic originates. The Scanning IPs are also used to identify the Customer and dynamically select Customer-specific settings.

3.3. The Customer is able to configure Web v2 URL to create access restriction policy rules via ClientNet (based both on categories and types of content) and deploy these at specific times to specific Users or groups by using the Client Site Proxy described in Clause 5.1.

3.4. THE CUSTOMER ACKNOWLEDGES THAT WEB URLv2 WILL BE PROVISIONED WITH SYMANTEC'S DEFAULT SETTINGS APPLIED FROM THE OUTSET AND THAT IT IS THE CUSTOMER'S SOLE RESPONSIBILITY TO CONFIGURE WEB URLv2 THROUGH CLIENTNET TO ITS OWN REQUIREMENTS. The default settings comprise of a "Block and Log" function for the following URL Categories:

3.4.1 Adult / Sexually Explicit; and
3.4.2 Spyware; and
3.4.3 Spam URLs; and
3.4.4 Criminal Activity.

3.5 Roaming User Support is an optional feature which extends the Web v2 URLService to Users who are not within the corporate network (for example to a User who works from home). The 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 started up. To access the web portal, the User must enter a password and user name. A PAC file template can be downloaded from ClientNet and modified by the Customer.

4. Alerts

4.1. If a User requests a Web page or attachment where an access restriction policy applies, then access to that Web page or attachment is denied and the User will be displayed an automatic alert Web page. In rare cases, and where one or more elements of the requested content is blocked, it may not be possible to display the alert Web page and the alert page may replace the content of the requested item, but access to the relevant page will still be denied.

4.2. There is a section within the automatic alert Web pages that customers can customize via ClientNet.

5. Reporting

5.1. Reporting on the results of a Customer's access restriction policy rules created under Clause 3.3 above is provided through Client Net.

5.2 To enable per User or group administration and reporting, the Customer will be required to install the relevant software application (the "Client Site Proxy") in accordance with the installation guidelines. Use of the Client Site Proxy is subject to the End User License Agreement provided with the Client Site Proxy.

5.3 The Customer recognizes that ClientNet detailed reporting data is only stored by Symantec for a maximum period of forty (40) days and will be not be available to the Customer upon the expiry of that period. ClientNet summary data is available for a maximum period of twelve (12) months.

5.4 The Customer may request an extended reporting period for the ClientNet detailed report of up to a maximum of six (6) months by subscribing to WSS Enhanced Data Retention.

6. General Terms and Conditions

6.1. NO WEB FILTERING SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE INTEROUTE NOR SYMANTEC CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF Web v2 URL TO DETECT BLOCKED URLs OR CONTENT.

6.2. Interoute and Symantec emphasize that the configuration of Web v2 URL is entirely in the control of the Customer. Web v2 URL is intended to be used solely to enable the Customer to enforce an existing, effectively implemented acceptable computer use policy (or its equivalent). In certain countries it may be necessary to obtain the consent of individual personnel. Interoute and Symantec advise the Customer to always check local legislation prior to deploying Web v2 URL. Interoute nor Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of Web v2 URL.

6.3 The Customer's web traffic when using Web v2 URL shall not exceed thirty megabytes (30MB) per User per day (calculated as an average per User across the Customer's total Registered Usage for Web v2 URL). In the event such daily limit is exceeded, Interoute and Symantec reserve the right to:

6.3.1 withhold provision of or suspend all or part of Web v2 URL immediately and until such excess use is remedied; or
6.3.2 require the Customer to purchase additional Users to reflect the Customers actual web traffic usage and raise additional invoices and/or make adjustments to subsequent invoices to cover charges for the increase in Registered Usage on a pro-rata basis for the remaining part of the current invoicing period.

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Appendix 8 – Symantec MessageLabs Email Archiving.cloud (P) Service

1. Service Overview

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

1.2 For Customers with *500 Users or fewer*, the *Symantec MessageLabs Email Archiving.cloud Lite (P) Service* includes the following:

(i) Standard features as described in Clause 3 below;
(ii) 3 year retention period;
(iii) Maximum storage of 3GB per User (calculated as an average per User based on the total number of Users).

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

(i) Standard features as described in Clause 3 below;
(ii) 1 year retention period;
(iii) Maximum storage of 1.5GB per User (calculated as an average per User based on the total number of Users).

1.3 For Customers with *500 Users or fewer*, the *Symantec MessageLabs Email Archiving.cloud (P) Service* includes the following:

(i) Standard features as described in Clause 3 below;
(ii) 10 year retention period;
(iii) Maximum storage of 10GB per User (calculated as an average per User based on the total number of Users).

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

(i) Standard features as described in Clause 3 below;
(ii) Unlimited retention period;
(iii) Maximum storage of 6GB per User (calculated as an average per User based on the total number of Users).

1.4 For Customers with *500 Users or fewer*, the *Symantec MessageLabs Email Archiving.cloud Premium (P) Service* includes the following:

(i) Standard features as described in Clause 3 below;
(ii) Premium features as described in Clause 4 below;
(iii) 10 year retention period;
(iv) Maximum storage of 10GB per User (calculated as an average per User based on the total number of Users).

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

(i) Standard features as described in Clause 3 below;
(ii) Premium features as described in Clause 4 below;
(iii) Unlimited retention period;
(iv) Maximum storage of 6GB per User (calculated as an average per User based on the total number of Users).

1.5 The Customer is required to 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 the 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.

1.6 Symantec shall monitor the Customer's actual usage of the Archiving.cloud (P) Service and if the actual storage exceeds the amount of storage purchased, then the Customer will be required to purchase an additional block of storage at Symantec's then current rates. Symantec will advise Interoute to raise additional invoices and/or make adjustments to subsequent invoices to cover charges for the increase in storage on a pro-rata basis for the remaining part of the current invoicing period.

1.7 The Customer acknowledges and agrees that once an Email has been archived, it cannot be deleted until the assigned retention period expires. This means that it is not possible to delete individual Emails selectively.

1.8 The Customer acknowledges and agrees that Symantec is unable to act as a third party downloader. If the event that the Customer is required to nominate a third party downloader for compliance purposes, Symantec shall use reasonable endeavours to facilitate a direct and independent agreement between the Customer and Symantec's third party service provider for this purpose. The Customer acknowledges that the third party service provider may impose charges for this service.

2. Service Activation

2.1 The Customer must complete Symantec's provisioning form accurately.

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

2.3 Symantec will contact the Customer to schedule an initial client call.

2.4 Actions outlined in Symantec's Client Setup Document must be completed by the Customer before the initial client call and include but are not limited to:

2.4.1 Set up new active directory user account;
2.4.2 Set up additional active directory groups;
2.4.3 Add users to Exchange groups;
2.4.4 Firewall configuration (if required);
2.4.5 Enable Microsoft Exchange Journaling (no earlier than 48 hours before installing the Email Archiving Appliance);
2.4.6 Install Email Archiving Appliance (in rack and booted up);
2.4.7 Ensure all mailboxes required for archiving are "mail enabled";
2.4.8 Configure remote access for MessageLabs.

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

2.5 The initial client call shall be carried out via WebEx. In this call the parties shall:

2.5.1 Verify all actions in the Client Setup Document have been completed;
2.5.2 Install the archiving and other software using Symantec's Archiving Installation Procedures Document;
2.5.3 Review Active directory setup;
2.5.4 Activate the service;
2.5.5 Verify user interface accessibility;
2.5.6 Verify archiving (site-to-site);
2.5.7 Generate copies of encryption keys in accordance with Symantec's Key Backup Procedures Document.

2.6 A training session is available on or after the initial client call and comprizes sessions focused on: (i) IT, (ii) Policy, (iii) Supervision, (iv) End user.

2.7 A post-review call is approximately one (1) week following activation. Following satisfactory completion of the post-review call, the Customer may follow the standard support procedures if additional assistance is required.

3. Standard Features

3.1 *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.

3.2 *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.

3.3 *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 the Customer only. The Customer has sole possession of all passwords, encryption keys and configuration settings and accordingly the Customer should ensure that they are maintained safely, and are kept in escrow or another suitable location. Symantec cannot accept liability for the loss of any passwords, encryption keys or configuration settings. The Customer understands that loss of passwords and encryption keys will result in the archive being inaccessible.

3.4 *Retention Policies*. The 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.

3.5 *InfoTags (metadata)*. The 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.

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

3.7 *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. This information can be used to create policies and legal holds that reference Users that have been deleted from Active Directory, as well as providing other Users with access to former employees' email.

3.8 *Attachment Stubbing*. The Customer may enable functionality that replaces attachment content within the Customer's mail system ("Mailbox Data") with a pointer to the appropriate copy within the archive. The 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, the Customer may install the Attachment Stubbing custom form to its Organization Forms Library (a special public folder on the Exchange server). Outlook will then automatically install the custom form from the server. To facilitate access to retrieve attachments outside of the Customer's network, the 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. The Customer can enable an option that stores a copy of attachments not previously archived to facilitate stubbing of the attachments contained in the mailbox. The 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.

3.9 *End-User Access*. The Customer may opt to provide individual Users with access to search the archive, either within the web user interface or directly within Outlook.

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

3.11 *Ad-Hoc Legal Holds*. The Customer can use the policy user interface to define and update ad-hoc legal holds. The legal 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 legal holds. The message is associated with each legal hold that it matches. To capture existing archived data into an ad-hoc legal hold, the Customer can perform a search with similar criteria, copy the results to a folder, then copy the contents of the folder to the legal hold. Each ad-hoc legal hold has an indefinite retention period – all messages in a given ad-hoc legal hold are retained until that hold is released.

3.12 *People-based Legal Holds*. The Customer can use the policy user interface to define and update people-based legal holds. Each people-based legal 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 legal 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.

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

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

3.15 *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.

3.16 *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 a set of privileges associated with them. 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 sign in using their standard Active Directory username and password and disabled accounts will lose 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.

3.17 *Retention and Disposition Management*. Based upon the retention policies defined by the Customer within the user interface, 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, the 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, the Customer's authorized User(s) can formally approve disposition for all messages that were archived during a given month. Customer acknowledges and agrees that when data is designated for disposal, it cannot be restored in human readable form from any and all storage mediums (including without limitation backups).

4. Premium Features

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

4.1 *Supervision.*

4.1.1 *Automatic Selection for Supervisory Review.* The Customer can define and update policies via the user interface 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.

4.1.2 Supervisory Review. The 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.
4.2 *Bloomberg Archiving*
4.2.1 The Symantec MessageLabs 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.
4.2.2 If the 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.
4.2.3 The FIRM format is supported, but not the ACCOUNT format or historical extract format of Bloomberg logs.
4.2.4 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, the 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.
4.2.5 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.
4.2.6 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.

5. Legacy Data Import
5.1 The Customer may import legacy data into the Archiving.cloud (P) Service subject to payment of a 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.
5.2 In the event that the Customer elects to use independent third party software in order to facilitate the import of data to the archive, the Customer acknowledges and agrees that Symantec is not responsible for such third party software and that the Customer does so at its own risk and expense.

6. Service Termination
6.1 Upon termination of the Archiving.cloud (P) Service, Symantec shall delete the Customer's data from the archive. Prior to termination, the Customer is able to extract its data from the archive, or the Customer can request that Symantec's nominated third party transfers the archived data back to the Customer in PST file format in accordance with Clause 6.2 below.
6.2 If the Customer requests Symantec's nominated third party to transfer the archived data upon termination:
6.2.1 The Customer must enter into a direct agreement with the nominated third party. Symantec shall not be a party to such agreement.
6.2.2 As the data is stored in an encrypted format, the Customer will need to provide the third party with an encryption key in order to decode the email into a free format.
6.2.3 The Customer will be responsible for the costs of transfer. Costs will be agreed upon in the agreement with the third party. Costs are dependent 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.
6.2.4 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.

7. Service Terms and Conditions
7.1 Symantec may, at its sole discretion, terminate the Archiving.cloud (P) Service immediately without notice and take such defensive action as it deems necessary:
7.1.1 If so directed by a court or competent authority;
7.1.2 In the event of an attack on the Archiving.cloud (P) Service or network;
7.1.3 In the event that the Customer or any of its Users is in breach of the Acceptable Use Policy in Clause 7.3 below.
7.2 The Customer shall be responsible for ensuring that it and all of its Users are aware of and comply with the Acceptable Use Policy in Clause 7.3 below.
7.3 *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:
7.3.1 Any attempt to crash a service host or network;
7.3.2 "Denial of service" attacks or "flooding" attacks against a service host or network;
7.3.3 Any attempt to circumvent the user authentication or security of a service host or network;
7.3.4 Any profligate use of the Archiving.cloud (P) Service;
7.3.5 The creation, transmission, storage, or publication of any kind of Virus or corrupting program or corrupted data;
7.3.6 Any other action that may adversely affect the Archiving.cloud (P) Service or its operation.
7.5 NO EMAIL ARCHIVE SERVICE CAN GUARANTEE 100% ACCURACY AND THEREFORE INTEROUTE NOR SYMANTEC CAN ACCEPT NO LIABILITY 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.
7.6 The Customer acknowledges that emails may contain personally identifiable information and that the archiving of emails may therefore constitute the processing of personal data. Furthermore, the Customer acknowledges that the Archiving.cloud (P) Service is a configurable service and that the Customer is solely responsible for configuring the Archiving.cloud (P) Service in accordance with the Customer's acceptable computer use policy (or equivalent) and all applicable laws or regulations. Any templates supplied by Symantec are for use solely as a guide to enable the Customer to create its own customized policies and other templates. Accordingly, Interoute and Symantec advise the Customer to always check local legislation prior to deploying the Archiving.cloud (P) Service, and to ensure that it, and all its employees, are aware of and comply with any responsibilities they have in respect of data protection and privacy laws and/or regulations in connection with the Customer's use of the Archiving.cloud (P) Service. In certain countries it may be necessary to obtain the consent of individual personnel prior to use of the Archiving.cloud (P) Service. Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the Customer's operation of the Archiving.cloud (P) Service. The Customer should take this into consideration when configuring the Archiving.cloud (P) Service. 7.6 The 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. IF AN ARCHIVING DATA CENTRE IN THE UNITED STATES OF AMERICA IS SELECTED, 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 UNITED STATES OF AMERICA; AND (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.

7.7 The Customer acknowledges and agrees that (i) the Symantec scanning services (Email AV, Email AS, Email IC and Email CC) do not scan all emails that originally enter the archive and (ii) the Symantec scanning services (Email AV, Email AS, Email IC and Email CC) do not scan emails that are released from the archive for reinstatement to a User's mailbox. Accordingly, Interoute nor 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.

8. Software License

8.1 The following terms and conditions apply to the software installed on the Email Archiving Appliance (the "Software"):

8.1.1 The Customer acknowledges and agrees that at all times as between the Customer and MessageLabs, Symantec and/or its suppliers is the owner of the Software. This Agreement grants the Customer a non-exclusive limited license to use the Software in connection with the Archiving.cloud (P) Service described in this Appendix and is not for the sale of the Software or any other intellectual property. All rights not expressly granted under this Agreement are reserved by Symantec and its suppliers.

8.1.2 The Customer may use one copy of the Software with one Email Archiving Appliance. For the purposes of this Agreement "use" means to execute, run, display, and store the Software for the duration of the provision of the Archiving.cloud (P) Service.

8.1.3 The Software is protected by Canadian and United States copyright laws and international treaties. The Customer may not rent or lease the Software or copy the documentation accompanying the Software. The Customer may not copy, reverse engineer, disassemble, decompile, or decode or attempt to create the source code from the Software.

8.1.4 The Customer agrees that a breach of these provisions will result in irreparable harm to Symantec and its suppliers and hereby agrees that Symantec and/or its suppliers directly may enforce this section including (without limitation) through specific performance or injunctive relief in addition to whatever remedies such party may otherwise be entitled to at law or in equity.

8.1.5 All technology, software, documentation and processes used by Symantec to provide the Archiving.cloud (P) Service are the exclusive property of Symantec or its suppliers.

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Appendix 9 – Symantec MessageLabs EIM.cloud Service

1. Service Description

1.1 The Symantec MessageLabs EIM.cloud Service ("EIM") is a managed service that allows for administrative control, centralized storage and domain management of instant messages.

1.2 With the exception of MSI and Java versions, the EIM client (the "POD") is installed on each User's work station. All instances allow the User to securely connect to the EIM platform and use EIM. 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).

1.3 The EIM administration tool, a web-based console, allows defined administrators to manage their domain structure and user base.

2. EIM Service Features

Service Features - Symantec MessageLabs EIM Communicate.cloud ("COMMUNICATE")

(i) Integrated file sharing (100mb capacity per User);
(ii) Desktop back-up solution;
(iii) Ability to share information with EIM Users that are online or offline;
(iv) Access control lists;
(v) Secure, 168-bit 3DES SSL encrypted POD-to-POD communications;
(vi) Web-based administration console;
(vii) Comprehensive user options interface;
(viii) Advanced presence detection and tracking;
(ix) Support for a wide variety of proxy servers;
(x) HTTP tunnelling capabilities;
(xi) Alert notifications for new files;
(xii) Object oriented file system with extensive search capabilities.

Service Features – Symantec MessageLabs EIM Connect.cloud ("CONNECT")

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

(i) Interoperable Instant Messenger (AOL, MSN, Yahoo!);
(ii) SMS messaging (2 messages per User, or "User Quota");
(iii) Instant Messaging Log Capabilities.

Service Features – COLLABORATE

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

(i) Integration with WebEx;
(ii) Integration with Salesforce.com.

3. Responsibility for Account Number/Password.

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

4. Responsibility for Content of Communications on Customer's Account.

4.1 Interoute and Symantec makes no express or implied warranty relating to the provision of the EIM Service except as provided in this Agreement. Interoute and Symantec does not guarantee a 100% Virus or Spam detection rate and therefore Interoute orSymantec will not accept liability for any damage or loss resulting directly or indirectly from any failure of EIM to detect Viruses or Spam or for wrongfully identifying a message suspected as being a Virus or Spam which proves subsequently not to be so.

4.2 Symantec makes no express or implied warranty relating to the availability of EIM, or the ability of EIM to retain all data.

4.3 Interoute and Symantec emphasize that the configuration of EIM is entirely within the control of the Customer. In certain countries it may be necessary to obtain the consent of individual personnel. Interoute and Symantec advise the Customer to always check local legislation prior to deploying EIM. Interoute nor Symantec will not accept liability for any civil or criminal liability which may be incurred by the Customer as a result of the operation of EIM.

5. Obligations

5.1 The Customer agrees that it will not:

5.1.1 transmit or store via the POD or EIM any data, text, video, audio, software, or other content that is illegal;

5.1.2 transmit or store via the POD or EIM any content that infringes any patent, trademark, copyright, rights of publicity, or other intellectual property right;

5.1.3 transmit or store any content that violates any applicable local, state, national, or international law that could give rise to civil or criminal liability;

5.1.4 transmit or store any unsolicited promotional content, advertising materials, Spam, "spim," chain-letters, or other such solicitation;

5.1.5 use the POD or EIM to publicly broadcast, transmit, or display content other than for the purposes of company communications;

5.1.6 use the POD or EIM 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, EIM or any other Internet host; or

5.1.7 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.

6. Interoperability

6.1 Customer will receive interoperability functionality as per Clause 2 above (see CONNECT package above). Symantec makes no warranties or guarantees around the ability of EIM to interoperate with any IM provider including but not limited to AOL, MSN and Yahoo!

7. US Only Data Storage

7.1 THE CUSTOMER'S ATTENTION IS DRAWN TO THE FACT THAT ALL MESSAGES WILL BE STORED IN THE UNITED STATES AND SYMANTEC CANNOT ACCEPT ANY RESPONSIBILITY FOR ANY BREACH OF APPLICABLE LEGISLATION OR REGULATIONS. THE CUSTOMER ACCEPTS THAT CONFIGURATION AND USE OF EIM IS ENTIRELY AT ITS CONTROL AND DISCRETION. Interoute nor Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of EIM. The Customer should take this into consideration when configuring EIM.

8. Logging and Compliance

8.1 The Customer may choose to log instant messages that pass through the EIM Service, subject to payment of the corresponding fees for the logging functionality.

8.2 Symantec sends log files to the Customer on a daily basis so that the Customer may store such logs in a compatible archive if desired.

8.3 Symantec retains logs for a period of three (3) years, after which time the logs are permanently deleted. The Customer's authorized representative may upon written request require (i) a copy of such logs or (ii) the deletion of such logs, at any time prior to the expiry of such three (3) year retention period.

8.4 The Customer is advised that the administration console permits the 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 EIM Service.

8.5 Symantec may provide six (6) months' prior written notice of its intention to cease the provision and support of the EIM Service. Upon expiry of such notice period, the EIM Service shall terminate.

8.6 Upon termination of the EIM Service, the Customer may request the return or deletion of its logs. If the Customer does not determine its preference within ninety (90) days of termination, Symantec shall permanently delete the logs.
8.7 The Customer acknowledges and agrees that Symantec cannot act as a third party downloader in any event for the purposes of SEC regulations.

9. Software Licence
9.1 Grant of Licence
Subject to the terms and conditions of this Agreement, Symantec grants Customer the non-exclusive, non-transferable right to install and use the Software for the EIM Service solely for the Customer's own internal business operations ("Software" means each Symantec software program for the EIM Service in object code format licenced by Symantec and governed by the terms of the Agreement, including without limitation new releases or updates as provided hereunder). All intellectual property rights in the Software are and shall remain the property of Symantec (and/or its suppliers). The Software is licenced by MessageLabs, not sold. Customer acknowledges that the 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 End User's compliance with or breach of the terms of this Agreement. Customer shall immediately notify Symantec of any unauthorized use or violation of terms of this licence.
9.2. Copy and Use Restrictions
Customer may download and install the Software subject to the following conditions:
9.2.1. Customer may not download or install the Software to more than the number of End User licences licenced by Customer ("End User" shall mean the physical computer where the software is installed).
9.2.2. Customer may copy the Software as reasonably necessary for backup, archival or disaster recovery purposes. Printed Documentation may be reproduced by the Customer for internal use only ("Documentation" means the Symantec's user guides and/or manuals for operation of the Software that are included with the downloaded Software.).
9.2.3 Customer may not, nor allow any third party to: (i) decompile, disassemble, or reverse engineer the 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 Software for timesharing or service bureau purposes; (iv) modify translate, adapt or create derivative works of the Software, or (v) otherwise use or copy the Software except as expressly provided herein.
9.3. Transfer of Rights
Customer may not transfer, assign or delegate the software licence under this Agreement without the prior written consent of MessageLabs. Any such transfer, assignment or delegation in violation of the foregoing shall be void.
9.4. Limited Warranty and Disclaimer
9.4.1 Symantec warrants that, upon download the Software will conform in all material respects to Symantec's current Documentation.
9.4.2 The preceding warranty will not apply if: (i) the Software is not used in accordance with this Agreement or the Documentation; (ii) the Software or any part thereof has been modified by any entity other than MessageLabs; or (iii) a malfunction in the Software has been caused by any of the Customer's equipment or third party software.
9.4.3 SYMANTEC DOES NOT WARRANT THAT THE OPERATION OF THE 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 EIM Service or the Agreement, all of Customer's right to use the Software granted herein shall immediately cease and Customer shall promptly return to Symantec or destroy all copies of the Software and Documentation.

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Appendix 10 – Symantec MessageLabs Policy Based Encryption.cloud Service

1. Service Description

1.1 The Symantec MessageLabs Policy Based Encryption.cloud Service ("PBE") provides the ability to send and receive encrypted Emails based on the Customer's email security policy.

1.2 In order to receive PBE, the Customer must also subscribe to the following Services:

- **Symantec MessageLabs Email Boundary Encryption.cloud Service ("BE**") as detailed in Schedule 2 Appendix 5; and
- **Symantec MessageLabs Email Content Control.cloud Service ("Email CC")** as detailed in Schedule 2 Appendix 4.

1.3 PBE provides the following functionality:

- Ability to use Email CC to define outbound encryption policies for Emails;
- Encrypted Email delivery through to the external recipient's inbox;
- Recipient gains access to the encrypted Email via a secure web portal;
- Recipient can access the secure web portal to respond to the Email in an encrypted format.

2. PBE Features

2.1 PBE allows the Customer to send an encrypted Email directly into a recipient's inbox without the need for the recipient to download software.

2.2 The Customer can configure the encryption method to be either Push or Pull. For Symantec MessageLabs Policy Based Encryption.cloud (Z) ("PBE Z"), the Email CC rule decides between Push or Pull. For For Symantec MessageLabs Policy Based Encryption.cloud (E) ("PBE E"), the default encryption method is Pull but can be changed to Push by the recipient by downloading the Secure Reader functionality within the recipient's secure web portal.

2.2.1 The "PBE Push" variant of the PBE Service sends the recipient an email notification with the original Email saved within it as an encrypted attachment. Following initial registration online, the recipient is able to view the decrypted Email offline using a Java application on their desktop.

2.2.2 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.

2.3 PBE also enables a recipient to enter a secure web portal and respond to an encrypted Email in an encrypted format.

2.4 The Customer may brand the portal that recipients use to read their encrypted Emails (for example to include the Customer's logo and support numbers).

2.5 The recipient of an encrypted Email may also send a brand new Email to any of the Customer's PBE Users.

2.6 If the Customer subscribes to PBE E, a third party Outlook Plug-In is available which adds an "encypt" icon to the recipient's Outlook toolbar. The Customer acknowledges and agrees that Symantec is not responsible for such third party software.

2.7 If the Customer subscribes to PBE E the following additional features are available:

a) a recipient can choose the language of the recipient's secure web portal and notification emails from a list of supported languages;

b) recipients can log into their accounts without opening a specific message, even if they have no active messages;

c) recipients can view all of their previous messages (that have not been permanently deleted) in their inbox, including messages they have sent;

d) if using the Pull method, a message composed in the web portal may have multiple recipients provided that such recipients share a domain from which the User has previously received a secure email;

e) if using the Push method, recipients can reply to any email address under the same domain;

f) initial notifications to new Users are available in more than one language;

g) It is possible to use a third party certificate/key to encrypt an outbound Email using the recipient's public key and decrypt an inbound Email using the recipient's private key, rather than the default certificates/keys generated by the PBE Service.

3. Provisioning, Invoicing and Change Requests

3.1. Interoute and Symantec shall commence charging for PBE from the date that Symantec confirms that the Customer's network is technically capable of supporting PBE (the "Technical Approval Date").

3.2 Clause 6.2 of Schedule 1 shall not apply to PBE. Interoute working with Symantec will aim to provision PBE orders and PBE change requests within 4 weeks of the Technical Approval Date, provided that all required due diligence has been completed by the Customer.

3.3 Customer agrees to provide all necessary resources, information, and authorizations, as required, and to activate or correct its DNS mail services for connectivity to PBE.

3.4 The Customer may change the branding of the portal a maximum of twice per annum.

4. Configuration

4.1 The Customer is responsible for implementing the configuration of PBE according to the Customer's needs. The Customer configures PBE via ClientNet by selecting the options available under the Email CC Service.

4.2 Interoute and Symantec emphasize that the configuration of PBE is entirely under the control of the Customer and that the accuracy of such configuration will determine the accuracy of PBE. Interoute and Symantec can therefore accept no liability for any damage or loss resulting directly or indirectly from any failure of PBE to fulfil the Customer's encryption obligations.

5. Service Parameters

5.1 The following limitations apply to PBE:

5.1.1 The number of secure Emails the Customer may send in any month using PBE Z may not exceed three hundred (300) times the Registered Usage for PBE. The number of secure Emails the Customer may send in any month using PBE E may not exceed four hundred and eighty (480) times the Registered Usage for PBE. When sending to multiple recipients, each unique address will be counted as a secure Email. In the event that the Customer exceeds the number of permitted secure Emails in any month, Symantec shall advise Interoute to increase the Registered Usage accordingly. Where Symantec advises increases in the Registered Usage, Symantec shall at its sole option raise additional invoices and/or make adjustments to subsequent invoices to cover charges for the increase in Registered Usage on a pro-rata basis for the remaining part of the current invoicing period which will be passed through Interoute to the customer.

5.1.2 Emails routed through PBE Z are limited to a maximum size of fifty megabytes (50 MB) per Email when compressed. Emails routed through PBE E are limited to a maximum size of fifty megabytes (50 MB) per Email post-encryption.

5.1.3 The Email Latency service level in the Service Level Agreement shall not apply to PBE.

5.1.4 The minimum number of Users of PBE Z is 50 Users. Initial and subsequent orders of PBE Z may be placed for minimum blocks of 50 Users or increments of 10 Users for orders exceeding 50 Users.

5.1.4 **PBE ONLY OPERATES WHEN USED IN CONJUNCTION WITH THE BE AND EMAIL CC SERVICES AND CANNOT OPERATE AS A STANDALONE SERVICE. EACH INDIVIDUAL PBE USER MUST BE AN EMAIL CC USER.**

6. Terms and Conditions

6.1 THE CUSTOMER ACKNOWLEDGES AND ACCEPTS THAT USE OF PBE IS ENTIRELY AT ITS CONTROL AND DISCRETION. PBE is intended to be used solely to enable Customer to enforce an existing, effectively implemented

acceptable computer use policy (or its equivalent). Use of encrypted services in some countries may be subject to legislation. Customer is advised to always check relevant legislation prior to deploying PBE. Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of PBE.

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Appendix 11- Symantec Email Continuity.cloud Service ("EC")

1. EC Overview

1.1 The Symantec Email Continuity.cloud Service ("EC") is a standby messaging system for Microsoft Exchange and Lotus Notes environments. EC will synchronize key system and User information including, but not limited to, the Email directory and individual Users' personal contacts. The Customer can also configure EC to support BlackBerry® devices through wireless forwarding using the BlackBerry® Web Client or BlackBerry® Internet Service, and an integrated Outlook experience for Users on Outlook 2003 Cached Mode or Outlook 2007 Cached Mode through an installed Outlook Extension.

1.2. *Supported Versions*: Microsoft Exchange 5.5, Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007, Lotus Notes Version 6, Lotus Notes Version 7.

1.3 *Supported Versions for Outlook Extension*: Microsoft Outlook 2003 in Cached Mode; Microsoft Outlook 2007 in Cached Mode.

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

2. EC Service Description

2.1. *Activation.* The Customer can request activation of EC via telephone to the Interoute Symantec support team or via the Email Management Services ("EMS") portal. Upon activation of EC, the Customer shall receive alerts via SMS to nominated mobile phones and personal email addresses. At that time, EC will begin to receive and sort incoming Emails, filter them (subject to Clause 4.4 below) in accordance with any other Symantec Email Services to which the Customer has subscribed (e.g. the Email AV Service), and route them to the appropriate User mailboxes. EC will provide storage and retention of Email traffic sent and received during activation for up to thirty (30) days after de-activation in order to enable the Customer to merge such Emails into its primary mail system if so desired.

2.2 *Retention.* The Customer is responsible for designating which Users' Emails are to be retained and the specified retention period for each such User. The retained Emails will be deleted upon the earlier of (a) expiry of the designated retention period for such User or (b) termination of EC. The Customer is required to purchase sufficient storage to meet its retention requirements in accordance with Clause 5.1 below.

2.3 *Authentication Manager.* The Customer may extend Customer's security policies for Microsoft Active Directory authentication to EC by enabling Users to log into their EC mailboxes using their Windows password, thereby removing the need for a separate EC password. Windows authentication requires the availability of a Windows domain controller accessible by Authentication Manager at the time of EC activation which is able to authenticate Users attempting to log on to EC mailboxes. Supported Versions: Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007

2.4 The minimum number of Users of EC that may be purchased by the Customer is the greater of (a) a number of Users equal to the number of mailboxes in the Customer's Microsoft Exchange organisation or (b) ten (10) Users.

3. Reserved.

4. Configuration

4.1 *Partial Activation*: For certain email systems/versions (Microsoft Exchange 2000, 2003 and 2007 environments), EC is capable of being activated for subsets of the Customer's environment (one or more individuals, servers and/or locations), "Partial Activation", in order to deal with more localized email outages.

4.2 *Activation*: The EC subscription entitles the Customer to twenty four (24) activations per annum, each lasting for a period of up to twelve (12) consecutive hours ("Included Activations"). (For illustration purposes, a single activation lasting for six (6) hours would count as one (1) activation, and a single activation lasting for nineteen (19) hours would count as two (2) activations.) In the event that the Customer has used its quota of Included Activations, the Customer may purchase additional activations (each lasting for a period of up to twelve (12) consecutive hours) at Symantec's then current rates.

4.3 System Testing: System Testing shall include (a) one (1) quarterly test of EC for all Users, with such test lasting up to four (4) hours, and (b) for Microsoft Exchange 2000, Microsoft Exchange 2003 or Microsoft Exchange 2007 environments, unlimited partial testing of up to ten percent (10%) of Users. The Customer must schedule these tests with Symantec no less than seven (7) business days prior to the Customer's desired test date.

4.4 **THE CUSTOMER ACKNOWLEDGES AND ACCEPTS THAT WHERE THE CUSTOMER IS IN AN ACTIVATED STATE, AND THE CUSTOMER THEN SENDS EMAILS TO, OR RECEIVES EMAILS FROM ANOTHER ORGANISATION THAT IS ALSO IN AN ACTIVATED STATE, EMAILS WILL BYPASS THE SYMANTEC INBOUND AND OUTBOUND SCANNING SERVICES TO WHICH CUSTOMER SUBSCRIBES**.

4.5 If the Customer uses the Email AV, Email AS, Email CC and/or Email IC Services, Symantec is able to configure the failover routing for the Customer's emails to the EC environment within ClientNet. This failover routing will be used when the EC service is activated.

4.6 **IF THE CUSTOMER DOES NOT USE EMAIL AV, EMAIL AS, EMAIL CC OR EMAIL IC, IT IS THE CUSTOMER'S RESPONSIBILITY TO CONFIGURE AND TEST THE FAILOVER ROUTING FOR THE CUSTOMER EMAILS TO THE EC ENVIRONMENT. THESE FAILOVERS MUST BE SET UP ACCORDING TO SYMANTEC'S INSTRUCTIONS DURING THE PROVISIONING PROCESS AND MAINTAINED THEREAFTER. IN THE EVENT THAT THE CUSTOMER FAILS TO SET UP OR MAINTAIN SUCH FAILOVERS, THE CUSTOMER ACKNOWLEDGES AND ACCEPTS THAT EMAILS CANNOT BE ROUTED TO EC**.

5. Options

5.1 *Symantec Email Continuity.cloud Storage Option*.

5.1.1 The Customer is required to purchase sufficient storage for retention purposes.

5.1.2 If the Customer subscribes to the Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email & Web Safeguard.cloud or Symantec MessageLabs 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 the Customer exceeds its storage allowance, Symantec shall charge for such additional storage at its then current rates.

5.1.3 If the Customer does not subscribe to one of the bundles listed in Clause 5.1.2, no storage is included in the per User price and the Customer is required to purchase sufficient storage for the Service at Symantec's then current rates.

5.1.4 Where the Customer is required to purchase additional storage, Symantec shall raise additional invoices and/or make adjustments to subsequent invoices to cover charges for the increase in storage on a pro-rata basis for the remaining part of the current invoicing period.

5.2 *Symantec Email Continuity.cloud Wireless Option.*

5.2.1 If the 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 EC 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.

5.2.2. 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).

6. EC Terms and Conditions

6.1 NO EMAIL CONTINUITY SERVICE CAN GUARANTEE A 100% SYNCRONIZATION AND THEREFORE INTEROUTE

NOR SYMANTEC CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF EC TO SYNCRONIZE EMAIL SYSTEMS.

6.2 Interoute and Symantec emphasize that the configuration of EC is entirely in the control of the Customer. Interoute and Symantec recommend that the Customer has an acceptable computer use policy (or its equivalent) in place. In certain countries it may be necessary to obtain the consent of individual personnel. Interoute and Symantec advise the Customer to always check its local legislation prior to deploying EC. Interoute nor means the contracting end user organisation/enterprise.

Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of EC.

7. Software License for EC

7.1 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 Software for EC as applicable solely for the Customer's own internal business operations. ("Software" means each Symantec software program for EC in object code format licensed by Symantec and governed by the terms of the Agreement, including without limitation new releases or updates as provided hereunder). All intellectual property rights in the Software are and shall remain the property of Symantec (and/or its suppliers). The Software is licensed by MessageLabs, not sold. Customer acknowledges that the 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 immediately notify Symantec of any unauthorized use or violation of terms of this license.

7.2. Copy and Use Restrictions

Customer may download and install the Software subject to the following conditions:

7.2.1. Customer may not download or install the Software to more than the number of End User licenses licensed by Customer. ("End User" shall mean the physical computer where the software is installed).

7.2.2. Customer may copy the Software as reasonably necessary for backup, archival or disaster recovery purposes. Printed Documentation may be reproduced by the Customer for internal use only. ("Documentation" means the Symantec's user guides and/or manuals for operation of the Software that are included with the downloaded Software).

7.2.3 Customer may not, nor allow any third party to: (i) decompile, disassemble, or reverse engineer the 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 Software for timesharing or service bureau purposes; (iv) modify translate, adapt or create derivative works of the Software; or (v) otherwise use or copy the Software except as expressly provided herein.

7.3. Transfer of Rights

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

7.4. Limited Warranty and Disclaimer

7.4.1 Symantec warrants that, upon download, the Software will conform in all material respects to Symantec's current Documentation.

7.4.2 The preceding warranty will not apply if: (i) the Software is not used in accordance with this Agreement or the Documentation; (ii) the Software or any part thereof has been modified by any entity other than MessageLabs; or (iii) a malfunction in the Software has been caused by any of the Customer's equipment or third party software.

7.4.3 SYMANTEC DOES NOT WARRANT THAT THE OPERATION OF THE 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.

7.5. Termination

Upon termination of EC, all of Customer's rights to use the Software granted herein shall immediately cease and Customer shall promptly return to Symantec or destroy all copies of the Software and Documentation.

Appendix 12 - Schemus Tool

1.1 The Schemus Tool is software that synchronizes data between the Customer's directory server and the Symantec services to which the Customer subscribes.
1.2 The Schemus Tool is licensed to the Customer by Schemus Limited via a separate end user license agreement ("Third Party EULA").
1.3 The Customer acknowledges and agrees that access to and use of the Schemus Tool is subject to the Customer accepting and complying with the terms and conditions of the Third Party EULA (a copy of which is available from Symantec upon request).
1.4 The Schemus Tool is controlled technology which is subject to applicable import and export laws and regulations as more specifically set forth in the export controls provision of the "General" section of the Agreement. **THE CUSTOMER ACKNOWLEDGES AND AGREES THAT IT SHALL BE REQUIRED TO SIGN A DECLARATION OF COMPLIANCE (A COPY OF WHICH IS AVAILABLE FROM SYMANTEC UPON REQUEST) (I) PRIOR TO SOFTWARE DOWNLOAD, (II) PRIOR TO LICENCE KEY ISSUANCE AND (III) ANNUALLY THEREAFTER IF REQUESTED BY MESSAGELABS.**
1.5 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 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.
1.6 Symantec's maximum liability to the Customer in relation to the Schemus Tool shall be limited to a sum equal to the actual amount paid by the Customer to Symantec for the Schemus Tool or £250 (or €350 if the Customer pays in Euros), whichever is the greater.

Appendix 13 – Symantec MessageLabs Instant Messaging Security.cloud Service (IMSS)

1 Overview

1.1 The Customer is required to synchronize its user directory with Symantec in order to create a list of Active Directory usernames and corresponding instant message (IM) usernames within ClientNet. An "Internal User" is a user known to the Customer's directory and uploaded into the IMSS administrative interface. An "External User" is a user unknown to the Customer's directory and/or not uploaded into the IMSS administrative interface.

1.2 The Customer is also required to make basic firewall changes to direct its IM conversations via MessageLabs.

1.3 Once IMSS has been configured in accordance with Clauses 1.1 and 1.2 above, IMs passing from Internal Users to External Users and vice versa are directed through IMSS for scanning by leading products including Symantec's own heuristic scanner, Skeptic™.

1.4 IMSS is only able to scan certain versions of public IM clients. Symantec shall publish a list of supported versions of public IM clients on ClientNet. The Customer acknowledges and accepts that Symantec may update and change this list on a regular basis without notice.

1.5 If an **incoming** IM:
1.5.1 is deemed to contain a Virus or other malicious code, it shall be blocked;
1.5.2 contains a URL for a webpage where a Virus or other malicious code has been detected, access to such webpage shall be denied.

1.6 IMSS also provides basic anti-Phishing functionality which will block **incoming** IMs deemed to be Phishing attacks.

1.7 IMSS is able to scan certain versions of Word, Excel and PowerPoint documents, but not other attachments.

1.8 IMSS is unable to scan encrypted IMs.

2. Reserved.

3. IMSS Content Control

3.1 IMSS allows the Customer to configure its own rule based content filtering strategy for incoming and outgoing IMs.

3.2 The Customer is responsible for implementing the configuration options in line with the Customer's acceptable computer use policy (or equivalent) via ClientNet. Rules may be configured on a group or individual basis. Changes made to the rules by the Customer shall become effective within four (4) hours.

3.3 Options are available for defining the action to be taken upon detecting controlled content within an IM. These options are detailed on ClientNet and in the current version of the Administrator's Guide.

3.4 The Customer can review the results of its rules via ClientNet in the form of daily, weekly, monthly and annual summaries organized both by rule and by User.

4 Logs and Storage

4.1 If the Customer has enabled the logging functionality, Symantec shall compile daily logs of IMs scanned. Each log shall include date and time stamps, content, and names of files transferred. Any logs that are unable to pass to the Customer shall be stored for a period of thirty-one (31) days and then destroyed.

4.2 The Customer may also configure IMSS to send a copy of each IM to the Customer's compatible archive or storage solution.

5 Notifications

5.1 The Customer may configure IMSS to send an automatic notification:
5.1.1 to the sender and intended recipient in the event that an IM is blocked because it is deemed to contain a Virus, Phishing attack or controlled content; or
5.1.2 to the recipient if access to a webpage is denied because it is deemed to contain a Virus or malicious content.

5.2 The Customer can activate, customize and deactivate notifications using ClientNet.

6 Support

6.1 Support includes:

6.1.1 Walk through of the IMSS interface including a service description and Q&A session. (This does not include assistance with the set up of rules or analysis of the effectiveness of rules);
6.1.2 Administrator's Guide;
6.1.3 User Guide.

7 IMSS Terms and Conditions

7.1 Suggested content control word lists and template rules supplied by Symantec contain words which may be considered offensive. Customer accepts and agrees that Symantec may compile and publish default word lists using words obtained from the Customers' custom word lists.

7.2 The Customer acknowledges that IMs may contain personally identifiable information and that the logging and interception of IMs may therefore constitute the processing of personal data. Furthermore, the Customer acknowledges that IMSS is a configurable service and that the Customer is solely responsible for configuring IMSS in accordance with the Customer's acceptable computer use policy (or equivalent) and all applicable laws or regulations. Accordingly, Symantec advises the Customer to always check local legislation prior to deploying IMSS, and to ensure that it, and all its employees, are aware of and comply with any responsibilities they have in respect of data protection and privacy laws and/or regulations in connection with the Customer's use of IMSS. In certain countries it may be necessary to obtain the consent of individual personnel prior to the interception and logging of IMs. At a minimum, the Customer shall implement, with reasonable and minimal customisation, Symantec's default notification for IMSS to those who use any communications system covered by IMSS that (i) indicates that communications transmitted through such system will be logged and may be intercepted, (ii) indicates the purposes of such logging and interception, and (iii) obtains prior user consent to any such logging and interception. The Customer may translate but shall not otherwise modify any language relating to items (i), (ii) and (iii) in the preceding sentence as part of any customisation to the default notification for IMSS. Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the Customer's operation of IMSS. The Customer shall hold Symantec harmless from any claims from its employees, any third party and/or governmental agencies relating to the interception or logging of IMs by Symantec or the Customer's failure to comply with laws and/or regulations.

7.3 **THE CUSTOMER'S ATTENTION IS DRAWN TO THE FACT THAT IMS PASSING THROUGH IMSS MAY BE SCANNED AND STORED ON HARDWARE LOCATED IN THE UNITED STATES OF AMERICA. CONSEQUENTLY 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 IMSS OF THE FACT THAT ANY INFORMATION, INCLUDING POSSIBLY PERSONALLY IDENTIFIABLE INFORMATION OF INDIVIDUALS, PASSING THROUGH IMSS MAY BE PROCESSED IN THE UNITED STATES OF AMERICA; AND (II) OBTAIN SUCH EMPLOYEES, AGENTS, CONTRACTORS AND THIRD PARTIES' CONSENT TO SUCH PROCESSING PRIOR TO OR CONTEMPORANEOUSLY WITH THE OPERATION OF IMSS BY CUSTOMER. FURTHERMORE, ANY PERSONAL DATA THAT THE CUSTOMER PROVIDES TO SYMANTEC MAY BE TRANSFERRED TO AFFILIATES OF SYMANTEC AND/OR SUBCONTRACTORS ACTING ON BEHALF OF MESSAGELABS. SUCH AFFILIATES OR SUBCONTRACTORS MAY BE SITUATED IN THE UNITED STATES OR OTHER COUNTRIES THAT MAY HAVE LESS**

PROTECTIVE DATA PROTECTION LAWS THAN THE REGION IN WHICH THE CUSTOMER IS SITUATED, IN WHICH CASE SYMANTEC WILL HAVE TAKEN STEPS SO THAT THE COLLECTED DATA, IF TRANSFERRED, RECEIVES AN ADEQUATE LEVEL OF PROTECTION. CUSTOMER AGREES TO TAKE ALL NECESSARY STEPS TO (I) INFORM ANY AND ALL OF ITS EMPLOYEES, AGENTS AND CONTRACTORS AS WELL AS THIRD PARTIES WHOSE PERSONAL DATA CUSTOMER PROVIDES TO SYMANTEC OF THE FACT THAT THEIR DATA MAY BE PROCESSED IN THOSE COUNTRIES; AND (II) OBTAIN SUCH EMPLOYEES, AGENTS, CONTRACTORS AND THIRD PARTIES' CONSENT TO SUCH PROCESSING. SYMANTEC CANNOT ACCEPT ANY RESPONSIBILITY FOR ANY CORRESPONDING BREACH OF APPLICABLE LEGISLATION OR REGULATIONS.

7.4 **NO SOFTWARE OR SERVICE CAN GUARANTEE A 100% IM DETECTION RATE AND THEREFORE INTEROUTE AND SYMANTEC CAN ACCEPT NO LIABILITY FOR ANY LOSS OR DAMAGE RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF IMSS TO DETECT SPIM, VIRUSES, PHISHING ATTACKS, MALICIOUS CODE, BLOCKED URLs OR CONTROLLED CONTENT, OR FOR IMSS WRONGLY IDENTIFYING IM AS CONTAINING SPIM, VIRUSES, PHISHING ATTACKS, MALICIOUS CODE, BLOCKED URLs OR CONTROLLED CONTENT.** Furthermore, the configuration of IMSS content control rules is entirely under the control of the Customer and the accuracy of such configuration will affect the accuracy of IMSS.

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Appendix 14 – Symantec Email Continuity Archive.cloud and Symantec Email Continuity Archive Lite.cloud

1. Overview

1.1The 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.

2. Customer Obligations

2.1 The Customer is responsible for the following actions in relation to the Service:
2.1.1 Providing and maintaining the necessary hardware and software (as identified in the provisioning form);
2.1.2 Ensuring that a dedicated technical resource with administrative rights is available for provisioning of the Service;
2.1.3 Designating which Users are entitled to receive the Service and the specified retention period for each such User;
2.1.4 Designating and protecting access privileges to the archive via the customer interface;
2.1.5 Setting and managing archiving retention policies;
2.1.6 Executing searches for retrieval of archived data.
2.2 In the event that the Customer has failed to perform the actions required in order to provision the Service within thirty (30) days from the date of the Customer's order, Symantec may commence charging for the Service.

3. Features

3.1 The *Symantec Email Continuity Archive.cloud Service* includes the following service features:
3.1.1 *Email Capture and Storage* – email is captured as it is delivered to the 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.
3.1.2 *Recovery* – provides the capability to restore email from the email archive back to the Customer's Exchange message stores.
3.1.3 *E-Discovery* – provides the capability for the 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.
3.1.4 *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.
3.1.5 *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. The Customer's email administrators can also specify whether or not Users can forward emails from their personal archive.
3.1.6 *Storage Management* – the Customer's system administrator can define a storage management policy which will move attachments from the Customer's Exchange message stores to the Service with the purpose of reducing storage requirements.
3.2 The *Symantec Email Continuity Archive Lite.cloud Service* includes the following service features (as each is further described above):
3.2.1 *Email Capture and Storage*
3.2.2 *Recovery*
3.2.3 *E-Discovery*
3.2.4 *Windows Authentication*
The Symantec Email Continuity Archive Lite.cloud Service does not include the End User Archive or Storage Management features. The Customer may upgrade to include the End User Archive service feature by subscribing to the *Symantec Email Continuity Archive Lite.cloud End User Pack*.
3.3 *Data Import Option* - the 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 standard rates.

4. Symantec Email Continuity.cloud Storage Option

4.1 Customer's storage shall be measured by the raw amount of email transferred to the Service and currently under storage.
4.2 If the Customer subscribes to the Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email & Web Safeguard.cloud or Symantec MessageLabs Ultimate Safeguard.cloud bundles:
4.2.1 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 the Customer exceeds its storage allowance, Symantec shall charge for such additional storage at its then current rates.
4.2.2 The bundle does not include storage for any legacy data imported under Clause 3.3 above and the Customer is required to purchase sufficient additional storage to meet such requirements at Symantec's then current rates.
4.3 If the Customer does not subscribe to one of the bundles listed in Clause 4.2, no storage is included in the per User price and the Customer is required to purchase sufficient storage for the Service at Symantec's then current rates.
4.4 Where the Customer is required to purchase additional storage, Symantec shall raise additional invoices and/or make adjustments to subsequent invoices to cover charges for the increase in storage on a pro-rata basis for the remaining part of the current invoicing period.

5. Terms and Conditions

5.1 NO EMAIL ARCHIVE SERVICE CAN GUARANTEE 100% ACCURACY AND THEREFORE INTEROUTE AND SYMANTEC CAN ACCEPT NO LIABILITY 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.
5.2 Interoute and Symantec shall not be responsible for any inability to provide the Service as set out herein which is caused by (a) Symantec's inability to apply its standard practices in deploying and managing the Service to Customer, (b) failure of the Customer to follow the Symantec guidelines set forth in the user manual or the provisioning form, or (c) failure of the Customer to activate or use the Service.
5.3 Interoute and Symantec emphasize that the configuration and use of the Service is entirely in the control of the Customer. Interoute and Symantec recommend that the Customer has an acceptable computer use policy (or its equivalent) in place. In certain countries it may be necessary to obtain the consent of individual personnel. Interoute and Symantec advise the Customer to always check its local legislation prior to deploying the Service. Interoute and Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of the Service.
5.4 THE CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA AND THAT THE CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL CONSENTS AND APPROVALS REQUIRED TO EFFECT THE TRANSFER OF DATA. THE CUSTOMER FURTHER ACKOWLEDGES AND AGREES THAT SYMANTEC CANNOT ACCEPT ANY RESPONSIBILITY FOR ANY CORRESPONDING BREACH OF APPLICABLE LEGISLATION OR REGULATIONS.

5.5 The Customer acknowledges and agrees that (i) the Symantec scanning services (Email AV, Email AS, Email IC and Email CC) do not scan all emails that originally enter the archive and (ii) the Symantec scanning services (Email AV, Email AS, Email IC and Email CC) do not scan emails that are released from the archive for reinstatement to a User's mailbox. Accordingly, Interoute and 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.
5.6 The Customer acknowledges and agrees that Symantec cannot act as a third party downloader in any event for the purposes of SEC regulations.

6. Software License

6.1 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 Software for the Symantec Email Continuity Archive.cloud or Symantec Email Continuity Archive Lite.cloud Service as applicable solely for the Customer's own internal business operations. ("Software" means each Symantec software program for the Symantec Email Continuity Archive.cloud or Symantec Email Continuity Archive Lite.cloud Service in object code format licensed by Symantec and governed by the terms of the Agreement, including without limitation new releases or updates as provided hereunder). All intellectual property rights in the Software are and shall remain the property of Symantec (and/or its suppliers). The Software is licensed by MessageLabs, not sold. Customer acknowledges that the 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 immediately notify Symantec of any unauthorized use or violation of terms of this license.

6.2. Copy and Use Restrictions

Customer may download and install the Software subject to the following conditions:

6.2.1. Customer may not download or install the Software to more than the number of End User licenses licensed by Customer. ("End User" shall mean the physical computer where the software is installed).

6.2.2. Customer may copy the Software as reasonably necessary for backup, archival or disaster recovery purposes. Printed Documentation may be reproduced by the Customer for internal use only. ("Documentation" means the Symantec's user guides and/or manuals for operation of the Software that are included with the downloaded Software).

6.2.3 Customer may not, nor allow any third party to: (i) decompile, disassemble, or reverse engineer the 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 Software for timesharing or service bureau purposes; (iv) modify translate, adapt or create derivative works of the Software, or (v) otherwise use or copy the Software except as expressly provided herein.

6.3. Transfer of Rights

Customer may not transfer, assign or delegate the software 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.

6.4. Limited Warranty and Disclaimer

6.4.1 Symantec warrants that, upon download, the Software will conform in all material respects to Symantec's current Documentation.

6.4.2 The preceding warranty will not apply if: (i) the Software is not used in accordance with this Agreement or the Documentation; (ii) the Software or any part thereof has been modified by any entity other than Symantec; or (iii) a malfunction in the Software has been caused by any of the Customer's equipment or third party software.

6.4.3 SYMANTEC DOES NOT WARRANT THAT THE OPERATION OF THE 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.

6.5. Termination

Upon termination of the Symantec Email Continuity Archive.cloud or Symantec Email Continuity Archive Lite.cloud Service, all of Customer's rights to use the Software granted herein shall immediately cease and Customer shall promptly return to Symantec or destroy all copies of the Software and Documentation

7. Service Termination & Data Extraction

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

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

Appendix 15 – Symantec MessageLabs Volume Mail Service

1. If the Customer subscribes to the Symantec MessageLabs Volume Mail Service ("Volume Mail Service"), the Customer may send and receive Volume Mail subject to the following conditions:

1.1 The Volume Mail must be made up of confirmed, opt-in solicited recipients only. The Customer shall, upon Symantec's request and subject to applicable legislation, provide evidence of such confirmations.

1.2 The size of each Volume Mail including attachments must not exceed 500 kilobytes.

1.3 The 'Recipients' box on each single Volume Mail must not contain over five hundred (500) Email addresses.

1.4 The Customer must operate an effective list management system including the prompt removal of invalid and subscription cancellation email addresses.

1.5 The Customer must receive the Symantec MessageLabs Email Anti-Virus.cloud Service for its standard Email.

1.6 The Customer's Volume Mail must originate from or be directed towards a separate domain to their standard Email enabling the Volume Mail to be pointed towards a specially provisioned Control Tower.

1.7 The default outbound banner shall notify the recipient that the Volume Mail has been virus scanned but it will not contain the Symantec logo.

1.8 If the Customer subscribes to Bands F or G of the Volume Mail Service in Section B "Service and Charges", the Customer must send or receive Volume Mail in batches of no more than 250,000 recipients per day.

1.9 The Customer recognises 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 Levels set out in the Service Level Agreement shall not apply to Volume Mail.

1.10 If at any time (i) the Customer's Email systems are blacklisted, or (ii) the Customer causes the Symantec systems to become blacklisted due to the sending of Spam, or (iii) the Customer fails to meet any of the obligations set out in this Appendix, Symantec shall inform the Customer and reserves the right at its sole discretion to withhold provision of, suspend or terminate all or part of the Services immediately.

1.11 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.

1.12 The Customer shall notify Symantec if at any time its actual Volume Mail usage exceeds the number of Recipients per Month permitted for the Customer's current Band and Symantec shall increase the charge to the appropriate Band in accordance with Symantec's then current price list. Additionally, Symantec will monitor the Customer's actual Volume Mail usage and if the number of Recipients per Month exceeds the number permitted for the Customer's current Band, Symantec will increase the charge in accordance with Symantec's then current price list. Symantec will at its sole option raise additional invoices and/or make adjustments to subsequent quarterly invoices to cover for any such increases.

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Appendix 16 – Symantec Enterprise Vault.cloud

1. Overview

1.1 Symantec EV.cloud is the collective name for a number of archiving Services (as each is described in Clauses 1.1 to 1.10 inclusive below) to which the Customer may subscribe. All Services within the Symantec EV.cloud range are compatible with approved versions of on-premise mail servers and hosted mail services.

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

1.2.1 The maximum email size that can be ingested by the Symantec Enterprise Vault Personal.cloud and Symantec Enterprise Vault Discovery.cloud Service is 50MB.

1.2.2 For both the Symantec Enterprise Vault Personal.cloud and Symantec Enterprise Vault Discovery.cloud Services the following applies:

1.2.3 Customers can directly reply to or forward messages located in the archive created by either service, which enables Customer to create backup files regularly in the event of Customer's email failure.

1.2.4 Neither service replaces the Customer's need to backup Customer's mail server locally. In the event that Customer needs to rebuild its mail server, it should rebuild the mail server from locally managed data rather than from the archive.

1.1. Symantec Enterprise Vault Personal.cloud

The Symantec Enterprise Vault Personal.cloud Service is Symantec's Internet-based email archiving service which is designed to give the Customer's individual Users access to their own personal email archives directly from Microsoft Outlook or Outlook Web Access (where supported) in order to find and restore lost or deleted emails.

1.1.1 Customer's inbound and outbound emails, including attachments, are captured in an online searchable repository (the "Personal Archive"), which Users can search to find lost or deleted emails.

1.1.2 Users can also access the Personal Archive from Microsoft Outlook, Outlook Web Access (where supported), IBM Lotus Notes, BlackBerry® devices and through a browser-based, secure website.

1.1.3 Users can search the Personal Archive for specific emails and attachments in two ways: Quick Search and Advanced Search. The Advanced Search option gives Users the ability to customize their searches based on a variety of criteria, such as message keywords, to, from, subject, date(s), and attachment type.

1.1.4 If enabled, Users can compose, reply to and forward messages directly from Symantec Enterprise Vault Personal.cloud, as they would in Outlook or Notes.

1.1.5 Users can create custom searches, based on a variety of criteria (e.g. date range, email sender, attachment type, etc.) and then save them so Users can re-run them as needed.

1.1.6 Moving Customer's legacy email into the Personal Archive and removing local archives helps reclaim space on Customer's shared drives and email servers.

1.1.7 Customer's Personal Archive can be used to recover historical email if a computer or laptops are lost or stolen.

1.1.8 Customers can ingest PST files into Symantec Enterprise Vault Personal.cloud where the folder structure is optionally maintained upon initial ingestion.

1.2. Symantec Enterprise Vault Discovery.cloud

The Symantec Enterprise Vault Discovery.cloud Service is Symantec's Internet-based email archiving service designed to expedite legal discovery (e-discovery) requests, enforce email use policies and aid in mitigating data loss. Discovery Archive aids Customers in email preservation related to lawsuits/legal holds, and aids in protecting attorney-client privileged communications.

1.2.1 Symantec Enterprise Vault Discovery.cloud stores and indexes emails, attachments, and BlackBerry® messages (SMS text, PIN-to-PIN, call log) in a centralized, online repository.

1.2.2 Customers can place legal holds on specific communications (based upon search criteria) to aid in safeguarding the Customer's staff or automated deletion policies from inadvertently deleting case-relevant emails. Administrators and reviewers can flag attorney-client privileged communications, which can be excluded from e-discovery requests.

1.2.3 Symantec Enterprise Vault Discovery.cloud search log captures the activities of reviewers, so administrators can conduct appropriate reviews.

1.2.4 Administrators have the ability to group Users based on custom criteria. Reviewers can then search across these groups.

1.2.5 Customers can search the contents of archived emails and attachments using a variety of search criteria, including to, from, date, subject, message body, message attachments and other message properties.

1.2.6 Customer's reviewers can efficiently navigate through search results, identify highlighted search terms and tag potentially harmful emails, so they are easily retrievable for further review.

1.2.7 Customers can tag emails related to a specific case or legal matter and then export emails into a third-party case management solution or other application for further review and analysis.

1.2.8 Customer's reviewers can create and save customized email searches based on Customer's email policies, and re-run them as necessary.

1.2.9 Customer's reviewers can set up policy alerts to notify them when an email meets "Saved Search" criteria (e.g., contains specific words or phrases).

1.3. Symantec Enterprise Vault.cloud Blackberry® Option

The Symantec Enterprise Vault.cloud Blackberry® Option is Symantec's Internet-based service designed to allow the Customer's individual Users to access and search archived emails, attachments, SMS, PIN-to-PIN messages and call log files via their BlackBerry® devices. Users can find and restore lost or deleted emails and continue to use their BlackBerry® device to compose, reply to and send messages in real time even when the Customer's primary email server experiences an outage. The Symantec Enterprise Vault.cloud Blackberry® Option is an optional add-on service to the Symantec Enterprise Vault Personal.cloud Service.

1.3.1 The Symantec 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.

1.3.2 Users can log into the Symantec Enterprise Vault.cloud Blackberry® Option by clicking on the icon displayed on the device's home screen.

1.3.3 When the User clicks on the application, a splash screen is displayed for three seconds and then the User is prompted for their user credentials.

1.3.4 After successful login, the User is directed to the Home Screen (i.e. List View screen) of Personal Archive.

1.3.5 From the List View (Mailbox) Screen, Users can perform a number of functions, including: composing new messages, reply to or forward emails, and conduct simple or advanced searches.

1.3.6 Users can find old, lost or deleted emails using simple or advanced searches of all messages and call log files stored in their Personal Archive and then restore these messages back to their inbox.

1.3.7 The User can enter text into the search box and press the search icon to start the search. Search results can be filtered based on "Date", "From" and "To."

1.3.8 The User can use their Personal Archive to compose, reply to and send messages even if the Customer's primary email platform (e.g., Microsoft Exchange) is unavailable.

1.4 AdvisorMail on Symantec.cloud™

AdvisorMail on Symantec.cloud™ ("AdvisorMail") is Symantec's Internet-based email archiving service which endeavors to expedite the email review process required by some regulatory

requirements. AdvisorMail archives emails into a single repository. Messages are auto-scanned and flagged based on the Customer's specific policies. Messages or attachments containing specified keywords or phrases can then reviewed by compliance professionals for policy enforcement.
1.4.1 AdvisorMail automatically captures sent and received messages without Customer intervention and securely transmits them to multiple data centers for retention, using TLS or VPN encryption.
1.4.2 AdvisorMail's administration and reporting tools include pre- or post-review modes, random sampling, customizable rules for specific domains or email addresses and summary reports.
1.4.3 AdvisorMail offers two distinct permission levels for email review: Administrator (full access) and Auditors (supervisory rights for selected mailboxes).
1.4.4 AdvisorMail offers a number of tools to streamline the supervisory process, including automatic flagging of suspicious emails for auditor review.
1.4.5 Customers can preselect their starting folder (e.g., post review), date range and message view (e.g., List or Snippet View).
1.4.6 Customers can use the Next Click feature to jump to the next violation in email messages and attachments with a single mouse click while right-click actions let the Customer choose commands by simply right clicking the mouse (e.g., adding keywords to the lexicon).
1.4.7 AdvisorMail's tiered supervision feature allows Customers to push out a corporate lexicon (list of violating keywords and phrases) to remote offices with a single command.
1.4.8 AdvisorMail's whitelist editor lets Customers whitelist keywords and phrases frequently found in disclaimers (i.e., legal disclaimers that appear in the footers of emails) to reduce the number of false-positive compliance violations.
1.4.9 AdvisorMail allows Customers to add email addresses, move users to other offices, modify rules and review multiple emails.
1.4.10 AdvisorMail's search log captures the auditing activities of Company's reviewers, aiding administrators in meeting compliance requirements.
1.4.11 Auditors can add notes to messages as needed.

1.5 AdvisorMail IM Option on Symantec.cloud™

AdvisorMail IM Option on Symantec.cloud™ is Symantec's Internet-based archiving service for supported instant message platforms. Instant messages are captured, stored and indexed in Advisor Mail and then monitored based on the Customer's specific compliance policies. Instant messages containing specified keywords or phrases can then be reviewed by compliance professionals for policy enforcement. AdvisorMail IM Option on Symantec.cloud™ is an optional add-on service to AdvisorMail on Symantec.cloud™.
1.5.1 AdvisorMail IM Option on Symantec.cloud™ interoperates with supported IM networks and clients which currently include public IM networks such as AOL, MSN, Yahoo, and Google Talk, private networks (Reuters), and enterprise IM clients (Microsoft Office Communicator, Lotus Sametime and Jabber).
1.5.2 Instant messages are indexed and copied in their original form to media where they can be readily searched.
1.5.3 The Customer can search and retrieve specific IM conversations based on a variety of search criteria, including date range, keyword or phrase, and sender/receiver.
1.5.4 There is a logging history for audit purposes.

1.6 AdvisorMail Bloomberg Option on Symantec.cloud™

AdvisorMail Bloomberg Option on Symantec.cloud™ is Symantec's Internet-based archiving service for Instant Bloomberg (instant messages) and Bloomberg email. Bloomberg messages are captured, stored and indexed in Advisor Mail and then monitored based on the Company's specific policies. Bloomberg messages containing specified keywords or phrases can then reviewed by compliance professionals. AdvisorMail Bloomberg Option on Symantec.cloud™ is an optional add-on service to AdvisorMail on Symantec.cloud™.
1.6.1 AdvisorMail Bloomberg Option on Symantec.cloud™ captures Instant Bloomberg and Bloomberg email into Advisor Mail in their proprietary format.
1.6.2 Bloomberg messages are indexed and copied in their original form to storage media where they can be readily searched.
1.6.3 The Customer can search and retrieve specific Bloomberg messages based on a variety of search criteria, including date range, keyword or phrase, and sender/receiver.
1.6.4 There is a logging history for audit purposes.

1.7 Reserved.

1.8 Symantec Enterprise Vault.cloud Data Import option

1.8.1 The Symantec Enterprise Vault.cloud Data Import Option is Symantec's Internet-based service designed to migrate and ingest existing legacy email data into the Customer's archive repository. The import service allows the Customer to then search their email archive (e.g., Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, and Advisor Mail) including both ingested legacy email and new email streams.
1.8.1 The Symantec Enterprise Vault.cloud Data Import Option requires a customer to ship via S-FTP or secure courier email data in PST, MSG or EML file format.
1.8.2 The Customer can manually extract the data and provide it in PST, MSG or EML format or use Symantec's professional services for automated extraction from supported repositories.
1.8.3 With the Customer's guidance, the Symantec Enterprise Vault.cloud Data Import Option assigns ownership to each message that has been located. Messages that cannot be directly assigned to a specific individual are archived into a "catchall" mailbox within the email archive.
1.8.4 All migration activity can be logged and audited to provide integrity of the Customer's Email records and maintain "chain of custody."
1.8.5 The Symantec Enterprise Vault.cloud Data Import Option involves active participation by the Customer to plan, analyze and execute an ingestion plan with minimal business disruption.
1.8.6 The maximum size for an email to be ingested is 40MB.

1.9 Symantec Enterprise Vault Mailbox Continuity.cloud

IF SYMANTEC IS UNABLE TO ESTABLISH AN SMTP CONNECTION TO THE CUSTOMER, THE CUSTOMER'S EMAILS WILL BE ROUTED TO THE SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD SERVICE ON BEHALF OF CUSTOMER ("CONTINUITY EVENT"). FOR THE AVOIDANCE OF DOUBT: (I) IF THE CUSTOMER'S FIREWALL ACTS AS A PROXY AND RESPONDS ON BEHALF OF THE MAIL SERVER, OR (II) IF THE 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.

1.9.1 During a Continuity Event, the Customer's individual Users can access their email via a dedicated folder in Microsoft Outlook® or a web-based User interface. The User can: (i) view up to ninety (90) days of historical email, including new emails sent and received during the Continuity Event; (ii) create, reply to and forward emails; and (iii) use common email tools such as spell checking, inserting attachments and rich formatting.
1.9.2 If Customer is Symantec Enterprise Vault Mailbox Continuity.cloud subscriber only, Continuity Emails will be stored within such service for a period of ninety (90) days. If Customer has purchased an additional archiving service under this Appendix 17, Continuity Emails will be retained based on the retention period selected by Customer in such service.
1.9.3 Continuity Emails will be delivered to Customer's primary email server at the point such server again begins to accept emails, with the exception that any emails which have been queuing for more than seven (7) days will not be delivered, and the Customer must instead retrieve the emails from the continuity archive described in Clause 1.9.2 above.

1.9.4 Symantec Enterprise Vault Mailbox Continuity.cloud utilizes an opportunistic, rather than an enforced, transport layer security ("TLS") connection when attempting e-mail delivery. TLS is an enhanced security protocol designed to protect/encrypt e-mail during transport over the Internet. **ALL BOUNDARY ENCRYPTION AND POLICY BASED ENCRYPTION CUSTOMERS ALSO SELECTING THE SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD SERVICE ACKNOWLEDGE AND AGREE THAT A TLS CONNECTION WILL BE ATTEMPTED BUT MAY NOT BE ACHIEVED AND THUS SUCH EMAILS MAY NOT BE ENCRYPTED. ACCORDINGLY, CUSTOMER ACKNOWLEDGES THAT IT SHOULD NOT SEND OR RECEIVE SENSITIVE DATA VIA THE SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD SERVICE OR CUSTOMER DOES SO ENTIRELY AT ITS OWN RISK.**

1.9.5 Symantec Enterprise Vault Mailbox Continuity.cloud Obligations

Symantec Enterprise Vault Mailbox Continuity.cloud only delivers email to a single nominated server per specified domain and "per User routing" Customers hereby accept this aspect of the service. Customer agrees to configure Symantec Enterprise Vault Mailbox Continuity.cloud as a failover delivery route with the ClientNet interface 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 the Symantec Enterprise Vault Mailbox Continuity.cloud 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 will adversely impact the functionality of the Symantec Enterprise Vault Mailbox Continuity.cloud Service.

1.10 Symantec Enterprise Vault.cloud Folder Sync Option

1.10.1 The Symantec Enterprise Vault.cloud Folder Sync Option is an add-on service to the Enterprise Vault Personal.cloud Service only described in Section 1.1 of this Appendix. The Symantec Enterprise Vault.cloud Folder Sync Option enables a Customer to view emails in the Enterprise Vault Personal.cloud Service in a manner similar to the e-mail organization in the Customer's Outlook folders. The Symantec Enterprise Vault.cloud Folder Sync Option allows administrators to synchronize the Customer's Outlook folder structures inside of the Personal Archive. As Customers move email messages between Outlook folders and create and move the location of Outlook folders, the synchronization service subsequently replicates the folder structure inside the Personal Archive.

1.10.2 The Symantec Enterprise Vault.cloud Folder Sync Option is deployed by administrators for Customer via a local service that tracks folder and per-item movements.

1.10.3 After initial synchronization, the Symantec Enterprise Vault.cloud Folder Sync Option provides incremental synchronization between Outlook folders and the Personal Archive.

1.10.4 Incremental synchcronizations may be scheduled on an hourly, daily or weekly basis as determined by Customer.

1.10.5 A Customer can filter the results of an archive search by switching on the 'filter' feature and selecting a folder from the list returned in the Search Filters.

1.10.6 The service is only supported on Microsoft Exchange Server 2003, 2007 or 2010 platforms.

2. Additional Terms.

2.1 Symantec emphasizes that the configuration and use of the Service is entirely in the control of the Customer. Symantec recommends that the Customer has an acceptable computer use policy (or its equivalent) in place. In certain countries it may be necessary to obtain the consent of individual personnel. Symantec advises the Customer to always check its local legislation prior to deploying the Service. Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of the Service.

2.2 **THE CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA AND THAT THE CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL CONSENTS AND APPROVALS REQUIRED TO EFFECT THE TRANSFER OF DATA. THE CUSTOMER FURTHER ACKOWLEDGES AND AGREES THAT SYMANTEC CANNOT ACCEPT ANY RESPONSIBILITY FOR ANY CORRESPONDING BREACH OF APPLICABLE LEGISLATION OR REGULATIONS.**

2.3 The Customer acknowledges and agrees that (i) the Symantec scanning services (Email AV, Email AS, Email IC and Email CC) do not scan all emails that originally enter the archive and (ii) the Symantec scanning services (Email AV, Email AS, Email IC and Email CC) 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.

2.4 Subject to the terms and conditions of this Agreement, Symantec grants Customer the non-exclusive, non-transferable right to install and use any software appurtenant to the aforementioned Services as applicable solely for the Customer's own internal business operations. All intellectual property rights in this software are and shall remain the property of Symantec (and/or its suppliers). Such software is licensed by Symantec, not sold. Customer acknowledges that the 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 immediately notify Symantec of any unauthorized use or violation of terms of this license.

2.5 Customer acknowledges and agrees that Symantec cannot act as a third party downloader in any event for the purposes of SEC regulations.

2.6 All Customer data stored or archived hereunder 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 the Customer Data.

2.7 Customer Data shall be stored or archived during the Term of the Service, and for a period of one hundred twenty (120) days after the Term of the Service, or one hundred twenty (120) days after the termination date if the Service is terminated before the Term expires (collectively, the "Post-Termination Retention Period"). During or before the Post-Termination Retention Period, Customer shall make a written election for Symantec to: (i) delete Customer's 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 s then current rates and at the rate of no more than two (2) terabytes delivered per month until all Customer Data is returned to Customer. In the event Customer fails to provide written instruction to Symantec as provided in the preceding sentence, Symantec shall delete the Customer Data (unless prohibited by law or court order) at the expiration of the Post-Termination Retention Period.

Appendix 17 – Symantec Endpoint Protection.cloud

1. Overview

1.1 In order to receive the Symantec Endpoint Protection.cloud Service, Customer is required to install an agent on applicable end–user computers and assign appropriate policy to utilize the Service. The Symantec Endpoint Protection.cloud management portal is an administrator portal used for managing computers, policies, alerts and reports ("Management Portal").

1.2 Customer may have to make some basic firewall changes to allow the agent to communicate and operate with the Symantec Endpoint Protection.cloud infrastructure.

1.3 Once the service has been configured in accordance with clauses 1.1 and 1.2 the Management Portal is used to manage the agent(s).

1.4 Symantec shall publish a list of supported computer operating systems for the agent and supported browser for the Management Portal. The Customer acknowledges and accepts that Symantec may update and change this list on a regular basis without notice.

1.5 The agent on the computer:

1.5.1 Shall protect the computer from detected malwares based on known methods as per the service

1.5.2 Shall block known malicious attacks from the network on the computer

1.5.3 Shall endeavour to provide anti-Phishing functionality on the supported browsers which will block deemed Phishing attacks.

2. Management Portal

2.1 The Management Portal allows the Customer to configure its own policy based security for the agents.

2.2 The Customer is responsible for implementing the configuration options in line with the Customer's acceptable computer use policy (or equivalent) via the Management Portal. Policies are configured on the computer group.

2.3 Changes made to the policy are visible immediately on the Management Portal, and are batched to push down to the agents. Effective policy setting on individual agent can be viewed on the Management Portal or on the agent running on the end-user computer.

3. Logs and Reports

3.1 All logs and reports reported by the agent are stored on, viewable and downloadable from the Management Portal, for twelve(12) months after which the logs are deleted.

4. Notifications

4.1 The Customer may configure the Symantec Endpoint Protection.cloud Service to send an automatic notification to configured email recipients based on the alerts rule, configurable in the Management Portal.

4.2 The Customer can create, delete and customize notifications using the Management Portal.

5. Support

5.1 Support includes:

5.1.1 Walk through of the Management Portal 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);

5.1.2 Administrator's Guide;

5.1.3. User Guide.

6. Symantec Endpoint Protection.cloud Data Privacy

6.1 The Customer acknowledges that logs may contain personally identifiable information and that the logging and interception of logs may therefore constitute the processing of personal data. Furthermore, the Customer acknowledges that Symantec Endpoint Protection.cloud is a configurable service and that the Customer is solely responsible for configuring Symantec Endpoint Protection.cloud in accordance with the Customer's acceptable computer use policy (or equivalent) and all applicable laws or regulations. Accordingly, Symantec advises the Customer to always check local legislation prior to deploying Symantec Endpoint Protection.cloud, and to ensure that it, and all its employees, are aware of and comply with any responsibilities they have in respect of data protection and privacy laws and/or regulations in connection with the Customer's use of Symantec Endpoint Protection.cloud. In certain countries it may be necessary to obtain the consent of individual personnel prior to the interception and logging. At a minimum, the Customer shall install any Symantec Endpoint Protection.cloud agent, with reasonable and minimal customization, Symantec's default notification for Symantec Endpoint Protection.cloud to those who use any computer covered by Symantec Endpoint Protection.cloud that (i) indicates that logs transmitted through such computer will be logged and may be intercepted, (ii) indicates the purposes of such logging and interception, and (iii) obtains prior user consent to any such logging and interception. Symantec can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the Customer's operation of Symantec Endpoint Protection.cloud.

6.2 THE CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA AND THAT THE CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL CONSENTS AND APPROVALS REQUIRED TO EFFECT THE TRANSFER OF DATA. THE CUSTOMER FURTHER ACKOWLEDGES AND AGREES THAT SYMANTEC CANNOT ACCEPT ANY RESPONSIBILITY FOR ANY CORRESPONDING BREACH OF APPLICABLE LEGISLATION OR REGULATIONS.

7. Configuration

7.1 If Customer has purchased the Service via a Symantec reseller, Customer expressly authorizes such Symantec reseller to (i) make configuration changes to the Service with the aim of achieving optimal functionality of the Service, and (ii) lodge Support tickets on behalf of Customer.

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Appendix 18 – Symantec MessageLabs Webv2 Smart Connect.cloud ("Smart Connect.cloud")

1. **Overview**

1.1. Once the roaming user agent is installed and relevant configuration changes are made, requests for Web pages and attachments are electronically routed via the user agent to the Symantec URL Filtering Service ("Web v2 URL") and Web Anti Spyware and Anti-Virus Service ("Web v2 Protect") and digitally examined.

2. **Service Description**

2.1. When the user connects to the Internet in designated 'in service' countries, the Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through the Web v2 URL and Web v2 Protect service offerings.

3. **Configuration**

3.1. The configuration settings required to direct this external web traffic to the roaming user agent software, as well as forward traffic outbound to the Web v2 URL and Web v2 Protect services, are made and maintained by the Customer and are dependent on the Customer's technical infrastructure. The Customer must install a PAC file onto the User's PC so that the browser is pointed to Symantec's roaming agent when the browser is started up. A PAC file template can be downloaded from ClientNet and modified by the Customer. The Customer should ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed to the roaming agent software.

3.2. Access to the Web v2 URL and Web v2 Protect is restricted to authorized systems that contain a valid version of the customer roaming agent software, as well as authorized users who are activated for these services in ClientNet. The roaming software agent and authorized user information is used to identify the Customer and dynamically select customer-specific settings.

3.3. Policy rules for the Web v2 URL service and content scanning for the Web v2 Protect service will be the same when a user is using the roaming agent service as when connected via a configured network location, i.e. corporate LAN.

3.4. The Customer acknowledges that the roaming agent will be provisioned with Symantec's default settings applied from the outset which includes using reasonable endeavours to route the user's web traffic to an 'optimal' service infrastructure access point. This routing is based on an understanding of the roaming user's location based on IP address and use of a third party geo-location database to identify the likely country that the user is currently connecting from. Symantec will route users with the appropriate country designation to what is believed to be the optimal service access point for the specified country. This will be done independently of any assessment of the likely performance for the individual end user's connection and only for those countries which Symantec has deemed capable of providing an acceptable level of service.

For any other country outside of the acceptable service countries, the customer acknowledges that Symantec will not be able to provide the Web v2 URL or Web v2 Protect service capabilities. In these situations upon determining that the end user is located in a 'non-service' country, the roaming agent will 'fail open' such that the end user will be able to connect to the internet without the benefits of the Symantec's service offerings that are available in acceptable service countries.

THE CUSTOMER ACKNOWLEDGES AND AGREES THAT THE USER'S WEB TRAFFIC MAY BE DIRECTED TO INFRASTRUCTURE LOCATED IN A GEOGRAPHIC LOCATION OUTSIDE THE EU FOR PROCESSING IN ACCORDANCE WITH THIS CLAUSE 3.4. THE CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL CONSENTS AND APPROVALS REQUIRED FOR THE TRANSFER OF SUCH WEB TRAFFIC. THE CUSTOMER FURTHER ACKOWLEDGES AND AGREES THAT SYMANTEC CANNOT ACCEPT ANY RESPONSIBILITY FOR ANY CORRESPONDING BREACH OF APPLICABLE LEGISLATION OR REGULATIONS.

4. **Additional Export Terms for Smart Connect.cloud**

4.1 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.

4.2 Customer or Partner shall not transfer the Web Roaming Agent to any other company, or to any individual that is not an employee of the Customer or Partner except that: (i) Customer or Partner may transfer to or enable the download of the Web Roaming Agent by its third party subcontractors for use on the Customer or Partner's behalf; and/or (ii) the Customer or Partner may transfer to or enable the download of the Web Roaming Agent by its third party end customers to whom it resells the Symantec Service, provided that the Customer or Partner makes such third parties aware of the obligations in this Clause.

Interoute Symantec.cloud (formerly MessageLabs) Services Schedule

Schedule 3
Service Level Agreement

1. Definitions

1.1. The following words shall have the following meanings for the purposes of this Service Level Agreement:

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

"**Designated Tower Cluster**" means two (2) or more Towers, distributed over a minimum of two (2) locations, designated to provide Service to the Customer;

"Email Virus False Positive" means a legitimate Email incorrectly marked/captured as containing a Virus;

"**Email Services**" means the Email AV, Email AS, Email IC, Email CC, Policy Based Encryption and Boundary Encryption 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 third party commercial scanners 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 two Wild List participants.

"Symantec Tracker" means a Symantec tool by which Service Availability and Latency are measured;

"**Monthly Charge**" means the monthly charge for the affected Services as detailed in the Agreement;

"**Service Level**" means each of the Service parameters defined in this Service Level Agreement;

"Spam False Negative" means a Spam Email that is not identified as Spam;

"Spam False Positive" means a legitimate Email incorrectly marked/captured as Spam;

"Spam Recommended Settings" means Symantec's best practice configuration guidelines for the Email AS Service; and

"Tower" means a number of load balanced servers;

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

3. General

NOTE: These Service Level Agreement Terms, except where indicated, are flow down terms from Symantec/MessageLabs. Any claims made against these terms are dependent on Symantec/MessageLabs agreement and acceptance of loss of service. Interoute as a reseller of this service is not empowered to make payments on this Service Level Agreement without Symantec/MessageLabs agreement that payment is liable and without Symantec/MessageLabs releasing the funds to allow payment.

2.1. In the event that the Customer believes it is entitled to a remedy in accordance with this Service Level Agreement, the Customer must submit a Credit Request within ten (10) working days of the end of the calendar month in question. The Customer recognizes that logs are only kept for a limited number of days and therefore any Credit Request submitted outside of the provided timeframe will be deemed invalid.

2.2. All Credit Requests will be subject to verification by Symantec in accordance with the applicable provisions of this Service Level Agreement.

2.3. 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 the Customer or a third party; (ii) during any period of suspension of service by Symantec in accordance with the terms of the Agreement; (iii) where the Customer is in breach of the Agreement (including without limitation if the Customer has any overdue invoices); (iv) in respect of any Emails that have not passed through the Service (including without limitation if the Customer has not locked down its router to point all Email traffic to MessageLabs); or (v) in respect of any inbound or outbound Emails that were initially sent to Symantec containing more than 500 recipients per SMTP session.

2.4. The remedies set out in this Service Level Agreement shall be the Customer's sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise in respect of levels of Service.

2.5. 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 the Customer for the affected Service(s).

2.6 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 constituent Services comprising such bundle; and

b) if the 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 constituent Services comprising such bundle, and multiplied by the number of remaining constituent Services comprising such bundle.

2.7 The Service Levels for the Email Services do not apply to the Customer's EC Service and therefore the Service Levels for the Email Services in Clauses 3 to 5 inclusive below shall be suspended during any period in which the EC Service is in an activated state.

3. 100% Service Availability

3.1 This Service Availability Service Level will only operate if the Customer utilizes one or more of the Email Services or Web Services.

3.2 In relation to the Email 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:

3.2.1 receive the Customer's inbound Email on behalf of the Customer's domain on a 24x7 basis; and

3.2.2 accept the Customer's outbound Email from a correctly configured Customer SMTP host on behalf of the 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 the Customer's outbound web requests and shall only apply if the 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%), the Customer may be entitled to 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, the Customer shall be entitled to terminate the affected Service forthwith 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 the Customer utilizes one or more of the Email Services.

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

4.2.1 the Email must have been received by the Customer's Designated Tower Cluster; and
4.2.2 the Email must not contain a Virus, Spam or other content which has caused it to be blocked by the Email Services.
4.3 Subject to Clauses 4.1 and 4.2 above, in the event Symantec fails to deliver an Email to or from the Customer and the Customer is not in breach of the terms of the Agreement, the Customer is entitled to terminate the Email Services upon thirty (30) 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 the Customer utilizes one or more Email 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 Services Tower within the Customer's Designated Tower Cluster exceeds the delays stated in the table below, the Customer may submit a Credit Request 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:
5.4.1. If the Customer has not supplied Symantec with a list of specific Email addresses to receive the Service (the "Validation List") and the Customer suffers a Denial of Service attack;
5.4.2. During periods of delay caused by a mail loop from/to the Customer's systems;
5.4.3 If the 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 the Customer utilizes one or more Web Services.
6.2. 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, the Customer may submit a Credit Request:

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

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

7. Spam – False Positives 0.0003%

7.1. This Spam False Positive Service Level will only operate if the Customer utilizes the Email Anti Spam Service and implements the Symantec Spam Recommended Settings.
7.2. Where the average Spam False Positive capture rate rises above 0.0003% of all Customer's Email traffic in any calendar month the Customer may be entitled to a 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:
7.3.1. Emails which do not constitute legitimate business Email;
7.3.2. Emails containing more than 20 recipients;
7.3.3. Where the sender of the Email is on the Customer's blocked senders list, including without limitation those defined by the individual User if the Customer has enabled User-level settings;
7.3.4. Emails which are sent from a compromised machine;
7.3.5. Emails which are sent from a machine which is on a third party block-list;
7.3.6. Emails which have been sent to more than 20 recipients (in a single operation or a series of operations) and have at least 80% the same in content.

8. 99% Spam Capture Rate

8.1. This Spam Capture Service Level will only operate if the Customer utilizes the Email Anti Spam Service and implements the Spam Recommended Settings. The provisions of this Clause 8 correspond to the number of Spam False Negatives measured in a month.
8.2. The Customer may be entitled to a 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 Asian character sets. In the event that such Spam Capture rate falls below 95% the Customer shall be entitled to a 25% percent credit of the Monthly Charge. In the event that the Spam Capture rate falls below 90% the Customer shall be entitled to a 100% percent credit of the Monthly Charge.

9. Spam Service Credit Requests

9.1. In order to be eligible for credit under Clauses 7 and 8 the Customer must send suspected False Positive or False Negative Emails to support@messagelabs.com within 5 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 if the Customer believes the number of confirmed Spam False Positives or Spam False Negatives entitles it to a credit in accordance with the table above, the Customer must send a Credit Request to Symantec in accordance with Clause 2.1 of this Schedule.

10. Email Virus Protection – 100%

10.1. This Email Virus Protection Service Level will only operate if the Customer utilizes the Email Anti Virus Service.
10.2. Should the Customer's systems be infected by one or more Viruses in any calendar month as notified to Symantec in a logged and validated support call confirming that a Virus has been passed to the Customer through the Email AV Service, the Customer may invoice Symantec for liquidated damages equal to 100% of the Monthly Charge subsisting at that time or £5,000/€10,000 (depending on the currency in which the Customer is invoiced), whichever is the lower. The remedy set out in this Clause 10.2 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 the Customer or a third party through the Service. For the avoidance of doubt, the remedy set out in this Clause 10.2 shall not apply in cases of deliberate self-infection.
10.3. The Customer's systems are deemed to be infected if a Virus contained in an Email received through the Email AV Service has been activated within the 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 the Customer, providing sufficient information to enable the Customer to identify and delete the Virus-infected Email. If such notification results in a prevention of infection the remedy set out in Clause 10.2 above shall not apply. Failure of the Customer to promptly act on such information will invalidate the Service Level contained in Clause 10.2 above.
10.5. The Email AV 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 in Clause 10.2 above.
10.6. This Email Virus Protection Service Level shall not operate in relation to Viruses that have been intentionally released by the Customer.

11. Email Virus False Positives 0.0001%

11.1 This Email Virus False Positive Service Level will only operate if the Customer utilizes the Email Anti Virus Service.
11.2. Where the Email Virus False Positive capture rate rises above 0.0001% of all Customer's Email traffic in any calendar month the Customer may be entitled to a 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 operate if the Customer utilizes the Web v2 Protect Service.
12.2. Should the Customer's systems be infected by one or more Known Viruses in any calendar month as notified to Symantec in a logged and validated support call including details of the URL from which the item was downloaded, confirming that a Known Virus has been passed to the Customer through the Web v2 Protect Service, the Customer may invoice Symantec for liquidated damages equal to 100% of the Monthly Charge subsisting at that time or £5,000/€10,000 (depending on the currency in which the Customer is invoiced), whichever is the lower. The remedy set out in this Clause 12.2 shall be the sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise in respect of any infection by a Known Virus passed to the Customer or a third party through the Web v2 Protect Service. For the avoidance of doubt, the remedy set out in this Clause 12.2 shall not apply in cases of deliberate self-infection or deliberate download of known malicious code by the Customer.
12.3 The Customer's systems are deemed to be infected if a Known Virus contained in a web transaction received through the Web v2 Protect Service has been activated within the 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 web transaction through the Symantec Web v2 Protect Service, Symantec will promptly notify the Customer, providing sufficient information to enable the Customer to identify and delete the item. If such notification results in a prevention of infection the remedy set out in Clause 12.2 above shall not apply. Failure of the Customer to promptly act on such information will invalidate the Service Level contained in Clause 12.2 above.
12.5. The Web v2 Protect Service will scan as much of the web item downloaded as possible. It may not be possible to scan items that are encapsulated or tunnelled 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 in Clause 12.2.

13. 24x7 Technical Support and Fault Response

13.1 Interoute and Symantec will on a twenty-four (24) hours/day by seven (7) days/week basis:
a) provide technical support to the Customer for problems with the Service; and
b) liaise with the Customer to resolve such problems.
13.2 Whenever a Customer raises a problem, fault or request, for service information via telephone or email with Interoute and consequently MessageLabs, its priority level is determined and it is responded to as defined in the table below:

Priority Level	Definition	Response Target
Critical	Loss of Service	95% of calls responded to within 2 hours
Major	Partial loss of Service or Service impairment	85% of calls responded to within 4 hours
Minor	Potentially Service affecting or non-Service affecting information request	75% of calls responded to within 8 hours

13.3 Faults originating from the Customer's actions or requiring the actions of other service providers are beyond the control of Interoute and Symantec and as such are specifically excluded from the fault response times in Clause 13.2 above.
13.4 Subject to Clause 13.3, if the 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 credit. Credit Requests must state the time, date and the Interoute log number of the incident. If eligible the Customer will be credited in accordance with the table below:

Priority	Failure to meet target	Percentage Credit of Monthly Charge
Critical	More than once in a calendar month	15
Major	More than twice a calendar month	10
Minor	More than three times in a calendar month	5

14. Archiving.cloud (P) Service

14.1 The provisions of this Clause 14 shall apply to the Archiving.cloud (P) Service only.

14.1 Archiving.cloud (P) Service Availability

14.1.1 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: a) the measurement will be performed by Symantec's monitoring systems (such measurement may be provided to the Customer upon written request), b) monitoring will occur in 5 minute intervals with two successive failures required to be an outage, c) 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.
14.1.2 For each one (1) percent or part thereof of non-availability beyond the availability target of 99.9% under this Clause 14.1 in the calendar month in question, the Customer will be entitled to a credit equivalent to ten per cent (10%) of the monthly charges due to Symantec in relation to the Archiving.cloud (P) Service, subject to a maximum of 100% of the monthly charges due in relation to the Archiving.cloud (P) Service in any calendar month. The 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.

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

14.2.1 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 the Customer during Normal Working Hours and within eight (8) hours of receiving notification of the problem outside of Normal Working Hours. Within twenty (20) Normal Working Hours of receiving notification of the problem, Symantec will either:
14.2.1.1 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
14.2.1.2 repair the Email Archiving Appliance by means of hardware and/or software; or

14.2.1.3 notify Customer that a replacement Email Archiving Appliance is required; or
14.2.1.4 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.
14.2.2 Should Symantec be obligated under Clause 14.2.1.3 above to provide a replacement Email Archiving Appliance, Symantec shall deliver such replacement Email Archiving Appliance to the Customer's site within forty eight (48) Normal Working Hours from the time Symantec notifies the Customer that a new Email Archiving Appliance is warranted.
14.2.3 Should Symantec be obligated under Clauses 14.2.1.2 and 14.2.1.3 above to repair or replace the Email Archiving Appliance or Software and fail to do so within the time-frames set out in Clauses 14.2.1 and 14.2.2, Symantec will refund Customer five percent (5%) of the monthly charges for the Archiving.cloud (P) Service for every day in delay past such time frame.
14.2.4 The foregoing terms in this Clause 14.2 shall be the Customer's sole and exclusive remedy with respect to any defect or breach of warranty with respect to the Email Archiving Appliance.

15. EC Service

15.1 The provisions of this Clause 15 shall apply to the EC Service only.
15.1.1 EC 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: a) the measurement will be performed by Symantec's monitoring systems (such measurement may be provided to the Customer upon written request), b) 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 MessageLabs.
15.1.2 For each one (1) percent or part thereof of non-availability beyond the availability target of 99.9% under this Clause 15.1 in the calendar month in question, the Customer will be entitled to a credit equivalent to ten per cent (10%) of the monthly charges due to Symantec in relation to the EC Service, subject to a maximum of 100% of the monthly charges due in relation to the EC Service in any calendar month. The Customer may terminate the EC Service at its sole option if at any time this availability falls below ninety percent (90%) in any calendar month.

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

16.1 The provisions of this Clause 16 shall apply to the Symantec Email Continuity Archive.cloud Service and Symantec Email Continuity Archive Lite.cloud Service only.
16.1.1 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.
16.1.2 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, the Customer shall be entitled to a 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 day of the Symantec Email Continuity Archive.cloud Service or Symantec Email Continuity Archive Lite.cloud Service.

17. Symantec EV.cloud Service

17.1 Symantec shall provide 99.99% server availability for Symantec EV.cloud . If server availability for a full calendar month falls below 99.99%, Symantec will issue a credit to Customer as provided below:

Server 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

17.2 Credit Requests must include the dates and times of server unavailability. Symantec will compare the server unavailability information provided by Customer with server availability monitoring data maintained by MessageLabs. A credit shall be issued if the server unavailability triggers a credit pursuant to the table in Clause 17.1 above. The credit described in this Clause 17.2 shall be Customer's sole and exclusive remedy in connection with any server unavailability. Server unavailability for maintenance purposes is excluded from server availability calculations.

18. Symantec Endpoint Protection.cloud

18.1 The provisions of this Clause 18 shall apply to the Symantec Endpoint Protection.cloud Service only.
18.1.1 Symantec Endpoint Protection.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 the Customer upon written request), b) 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 MessageLabs.
18.1.2 For each one (1) percent or part thereof of non-availability beyond the availability target of 99.9% under this Clause 18.1 in the calendar month in question, the Customer will be entitled to a credit equivalent to ten per cent (10%) of the monthly charges due to Symantec in relation to the Symantec Endpoint Protection.cloud Service, subject to a maximum of 100% of the monthly charges due in relation to the Symantec Endpoint Protection.cloud Service in any calendar month. The Customer may terminate the Symantec Endpoint Protection.cloud Service at its sole option if at any time this availability falls below ninety percent (90%) in any calendar month.
The credit described in this Clause 18.1.2 shall be Customer's sole and exclusive remedy in connection with any server unavailability for the Symantec Endpoint Protection.cloud Service. The Service Levels in Sections 3.1, 3.4, and 11.1 of this Service Level Agreement shall not apply to the Symantec Endpoint Protection.cloud Service.