IBM United Kingdom Limited
Registered in England: 741598
Registered Office: PO Box 41,
North Harbour, Portsmouth,
PO6 3AU (hereinafter "IBM")

Services Description

IBM Managed Security Services (Cloud Computing) - hosted e-mail and Web security - express managed e-mail security

IN ADDITION TO THE TERMS AND CONDITIONS SPECIFIED BELOW, THIS SERVICES DESCRIPTION INCLUDES THE "IBM MANAGED SECURITY SERVICES GENERAL PROVISIONS" ("GENERAL PROVISIONS") LOCATED AT http://www-935.ibm.com/services/uk/gts/html/contracts_landing.html AND INCORPORATED HEREIN BY REFERENCE.

1. Scope of Services

IBM Managed Security Services (Cloud Computing) - hosted e-mail and Web security - express managed e-mail security (called "E-mail Security" or "Services") may include:

a. E-mail Antivirus services to help detect viruses and certain other images in the Services Recipient's Internet e-mail;

b. E-mail Image Control services to help detect pornographic images contained in image files in the Services Recipient's inbound and outbound Internet e-mail and attachments;

c. E-mail Antispam services to help safeguard the Services Recipient's Internet e-mail from Spam; and/or

d. E-mail Content Control services to help the Services Recipient detect content in line with its acceptable computer use policy (or its equivalent) in the Services Recipient's Internet e-mail.

The Services features described herein are dependent upon the availability and supportability of products and product features being utilised. Even in the case of supported products, not all product features may be supported. Information on supported features is available from IBM upon request. This includes both IBM-provided and non-IBM-provided hardware, software, and firmware.

2. Definitions

Bulk E-mail – a group of more than 5,000 e-mails, with substantially similar content, sent or received in a single operation or a series of related operations.

Designated Tower Cluster – a cluster of load balanced e-mail servers (minimum of two), designated to provide E-mail Security to the Services Recipient.

E-mail Services Availability – the ability to establish a Simple Mail Transfer Protocol ("SMTP") session on port 25 of the Designated Tower Cluster as measured by IBM availability tracking systems.

Latency – the average roundtrip time for e-mail sent every five minutes to and from every Tower, as measured by IBM availability tracking systems.

Open Relay – an e-mail server, configured to receive e-mail from an unknown or unauthorised third party and forward the e-mail to one or more recipients who are not users of the e-mail system to which that e-mail server is connected. Open Relay may also be referred to as "Spam Relay" or "Public Relay".

Planned Maintenance – maintenance periods which cause disruption of the services due to non-availability of the Designated Tower Cluster. Notice will be provided to the Services Recipient a minimum of five calendar days prior to such maintenance. Planned Maintenance shall not exceed more than eight hours per calendar month and will not take place during local business hours.

Quarantine – isolation of e-mail suspected of carrying unwanted content, per Services Recipient's configuration settings, prior to action by the User or automatic deletion.

Services Recipient – any entity or individual receiving or using the Services, or the results or products of the Services.

Spam – unsolicited commercial e-mail.

User - a person or mailbox on behalf of which e-mail is being scanned by the Services.

Virus – program code that plants itself in a file or memory, infects other files and memory areas, and runs without authorisation.

3. Services

3.1 General Services

THE SERVICES DESCRIBED HEREIN ARE PROVIDED "AS IS" AND WITHOUT WARRANTY OR INDEMNITY OF ANY KIND BY IBM, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF PROPRIETARY AND INTELLECTUAL PROPERTY RIGHTS.

3.1.1 IBM General Services Responsibilities

IBM will:

a. provide you with password access to a proprietary Internet-based reporting and management tool to allow you to view data and statistics on your use of the Services. This tool will also offer a number of configuration and management facilities;

b. provide the Services on a 24 hours/day by 7 days/week basis; and

c. provide technical support for the Services on a 24 hours/day by 7 days/week basis.

3.1.2 Your General Services Responsibilities

You agree to:

a. monitor the number of Users, and notify IBM if the actual number of Users exceeds the number ordered or falls below the required minimum of ten Users. IBM will work with you to upgrade the Schedule to include the additional Users.

b. ensure:

(1) all e-mail systems to be supported have a static IP address;

(2) supported e-mail systems do not send Bulk E-mail, act as an Open Relay, or send Spam; and

(3) you or any member of your Enterprise does not use the Services (or any part or portion thereof) to in any way develop or promote commercial services similar to said Services;

SHOULD YOU FAIL TO MEET THESE OBLIGATIONS AND DISRUPTION OCCURS TO THE SERVICES, IBM WILL INFORM YOU OF SUCH FAILURES AND RESERVES THE RIGHT TO WITHHOLD PROVISION OF OR SUSPEND ALL OR PART OF THE SERVICES IMMEDIATELY AND UNTIL SUCH USE IS TERMINATED.

c. provide all technical data and other information IBM may reasonably request from time to time to allow IBM to supply the Services to you;

d. maintain the security of the password provided to you for access to the proprietary Internet-based configuration, management and reporting tool, including not disclosing to any third party;

e. provide IBM with the name, telephone number and e-mail address of your e-mail administrator, if you have selected this option in your profile; and

f. ensure the appropriate release authorisation form, to redirect e-mail to an alternate e-mail address is submitted to IBM in a timely manner.

3.2 General Service Level Agreements

IBM Service Level Agreements ("SLAs") establish response time objectives and countermeasures for specific events resulting from the Services. The SLAs become effective when the deployment process has been completed, and support and management have been successfully transitioned to you. The SLA remedies are available provided you meet your obligations as defined in this Services Description and all associated contract documents.

SLAs are not applicable:

a. until 30 days after activation of E-mail Security;

b. if your system configurations do not comply with the provided configuration guidelines;

c. during periods of Planned Maintenance;

d. during periods of non-availability due to force majeure or acts or omissions by you, IBM, or a third party; or

e. during any period of suspension of E-mail Security in accordance with this Services Description and all associated contract documents.

3.2.1 General SLA Availability

The SLA defaults described below comprise the measured metrics for delivery of the Services. Unless explicitly stated below, no warranties of any kind shall apply to Services delivered under this

Services Description. The sole remedies for failure to meet the SLA defaults are specified in the section of this Services Description entitled "General SLA Remedies".

a. E-mail delivery - In order for IBM to perform the Services, your e-mail will be routed through IBM. IBM will transmit 100% of all e-mail sent or received for this purpose. This SLA does not apply to e-mail containing a Virus, or e-mail stopped by E-mail Antispam.

b. E-mail Services Availability – IBM will maintain E-mail Services Availability for 100% of the calendar month

   E-mail Services Availability is only applicable if the Designated Tower Cluster is able to:

   (1) receive your inbound e-mail on behalf of your domain on a 24x7 basis; and

   (2) accept your outbound e-mail from your correctly configured SMTP host on behalf of your domain(s) on a 24x7 basis.

c. E-mail Latency – In any calendar month, the average roundtrip time of your Designated Tower Cluster will be a maximum of one minute. This roundtrip time will not include delays caused by a mail loop to/from your systems.

   E-mail Latency is not applicable during:

   (1) any Virus outbreak where the Virus to e-mail ratio is greater than 1:50; or

   (2) a Denial of Service attack.

3.2.2 General SLA Remedies

The general SLA remedies are available provided you meet your obligations as defined in this Services Description and all associated contract documents.

As described in the following tables, a credit will be issued as the sole remedy for failure to meet any of the SLAs described in the section above entitled "General SLA Availability", during any given calendar month. You may obtain no more than 100% of the monthly charge for the Services in a given calendar month.

All credit requests must be submitted to IBM within five days after the end of the month in which the eligibility occurred. Credit eligibility is subject to verification by IBM.

a. E-mail delivery remedy - In the event IBM fails to transmit an e-mail message, and you are not in breach of the terms of this Services Description, you will be entitled to terminate Hosted E-mail Security upon 30 days written notice.

b. E-mail Services Availability remedy - If the E-mail Services Availability is below 100% in any calendar month during the contract period, a credit will be issued as follows:

% E-mail Services Availability per Calendar Month	Credit of Monthly Charge
Less than 100% but greater than 99.0%	25%
Less than 99.0% but greater than 98.0%	50%
Less than 98%	100% Termination of the Services, at your discretion. Should the Services be terminated, such termination shall be the sole and exclusive remedy with respect to availability of the Services of less than 98% in a given calendar month.

c. E-mail Latency remedy – If the E-mail Latency is greater than one minute on average in any calendar month during the contract period, a credit will be issued as follows:

Average Roundtrip Time	Credit of Monthly Charge
Greater than 1 minute but at most 1 minute and 30 seconds	25%
Greater than 1 minute and 30 seconds but at most 2 minutes	50%
Greater than 2 minutes but at most 2 minutes and 30 seconds	75%
Greater than 2 minutes and 30 seconds	100%

3.3 Boundary Encryption Services (Optional)

At your request, and for an additional charge specified in the Schedule, IBM will provide the optional Boundary Encryption Services, as described below.

The Boundary Encryption Services ("Boundary Encryption") provide encrypted communication channels designed to enable formation of a secure private e-mail network ("SPEN") with nominated partner organisations ("SPEN Partners"). Boundary Encryption is based on the Internet Engineering Task Force ("IETF") standard RFC 3207 Simple Mail Transfer Protocol ("SMTP") Services Extension for Secure SMTP over Transport Layer Security ("TLS") (called "STARTTLS").

3.3.1 IBM Boundary Encryption Responsibilities

IBM will:

a. transmit e-mail exchanged by Boundary Encryption, between your domains which utilise Boundary Encryption ("nominated domains") and SPEN Partners, only over TLS connections;

b. use unencrypted SMTP to pass e-mail sent from you to an organisation not configured as a SPEN Partner ("Non-SPEN Partner"), unless otherwise configured;

c. make commercially reasonable efforts to negotiate an opportunistic TLS connection with Non-SPEN Partners requesting a TLS connection to send e-mail to you. If the Non-SPEN Partner does not request a TLS connection, unencrypted SMTP will be used to pass the e-mail from Boundary Encryption to the recipient;

d. provide its server certificate for authentication when an external mail server originates a TLS connection. If so configured, Boundary Encryption will initiate, exchange, and verify a client certificate request. If a supplied certificate cannot be validated, the TLS connection will be aborted;

e. provide its client certificate for authentication when requested to do so by an accepting mail server. If a TLS connection cannot be established, the e-mail will be returned to the originating mail server via a TLS connection, with a suitable reason for the failure;

f. for each certificate submitted by a remote mail server as part of a TLS connection, validate that a recognised certificate authority has signed the certificate, the certificate has not expired, and the e-mail domain information matches that which is expected. If a certificate cannot be validated, the associated connection will be aborted; and

g. maintain a list of recognised certificate authorities for the purpose of certificate validation.

3.3.2 Your Boundary Encryption Responsibilities

You agree:

a. to provide IBM with a list of SPEN Partners;

b. to ensure your mail server, and the mail servers of your SPEN Partners, support STARTTLS;

c. to provide IBM with a list of nominated domains;

d. to ensure all certificates adhere to the X.509 v3 standard;

e. if IBM is required to allocate additional technical resources to the provision of PBE due to your failure to perform the required due diligence, to pay any associated charges; and

f. to be solely responsible for your failure, or the failure of any third party (including any SPEN Partners), to fulfil your obligations with regard to registering and maintaining valid certificates, or for the timeliness or accuracy of such information.

3.3.3 Additional Boundary Encryption Services

If you use Boundary Encryption in conjunction with Policy-Based Encryption (as detailed below), the "Secure Connection" model of Boundary Encryption must be implemented. In such event, the following rules regarding enforcement of encrypted e-mail exchange will apply:

- all e-mail exchanges between you and IBM must be secured by TLS encryption; and
- when e-mail is sent from a SPEN Partner organisation to you, IBM will be accept the connection and route the e-mail over TLS through to you.

If you use Boundary Encryption in conjunction with the signaturing system functionality of E-mail Antispam, it is recommended that you include all of your SPEN Partner domains in your E-mail Antispam-approved senders list.

If you subscribe to "Secure Connection" of Boundary Encryption:

- all e-mails addressed to your domain will be routed to you in an encrypted format; and
- all e-mails sent from your nominated domain(s) will be encrypted for receipt by IBM. The format of onward routing (i.e., unencrypted or encrypted) will be determined by TLS enforcements you specify, and capability of the destination server to receive e-mails over opportunistic TLS.

3.3.4 Disclaimer

Boundary Encryption is intended to be used solely to enable you to enforce an existing, effectively implemented, acceptable computer use policy (or its equivalent). Use of Boundary Encryption in some countries may be subject to legislation. You are responsible for checking relevant legislation prior to deploying Boundary Encryption. IBM is not responsible for any civil or criminal liability that may be incurred by you as a result of the operation of Boundary Encryption.

3.4 Policy Based Encryption Services

The Policy-Based Encryption Services ("PBE") is designed to allow you to send and receive encrypted e-mails based on your e-mail security policy. PBE is only available if you have a current subscription for the Boundary Encryption Services and E-mail Content Control.

3.4.1 IBM Policy Based Encryption Services Responsibilities

IBM will:

a. allow E-mail Content Control to define outbound encryption policies for e-mail;

b. provide encrypted e-mail delivery through to the external recipient's inbox;

c. allow the recipient to gain access to the encrypted e-mail via a secure Web portal;

d. allow the recipient to access the secure Web portal to respond to the e-mail in an encrypted format;

e. allow you to send an encrypted e-mail directly into a recipient's inbox without the need for the recipient to download software;

f. notwithstanding anything to the contrary in this Services Description or a related agreement, provision of PBE will begin within four calendar weeks after the Contract Period Start Date which is defined as the first business day following IBM's electronic notification to you of order acceptance. Such provision of PBE is dependent on your having completed all technical due diligence.

3.4.2 Your Policy Based Encryption Services Responsibilities

You agree:

a. to provide all necessary resources, information, and authorisations to activate or correct your DNS mail services for connectivity to PBE;

b. to contract for a minimum of 50 Users. Each individual PBE User will be an E-mail Content Control User;

c. to be responsible for initial setup charges and the recurring charges for PBE branding and PBE branding enterprise. At your request, subsequent changes to the branding of the Web portal will be available for an additional charge of $500 (U.S.) per change request;

d. to be solely responsible for the configuration of PBE in your environment and the accuracy of such configuration;

e. to be solely responsible for implementing the PBE configuration according to your needs. You will configure PBE via ClientNet by selecting available options under the E-mail Content Control services;

f. if IBM is required to allocate additional technical resources to the provision of PBE due to your failure to perform the required due diligence, you agree to pay the associated charges;

g. and acknowledge that the lead time for provisioning PBE orders and PBE change requests shall be four weeks from the date of IBM's acceptance of such order or change request, provided that all technical due diligence has been completed by you; and

h. and acknowledge that the configuration of PBE is entirely under your control and that the accuracy of such configuration will determine the accuracy of PBE.

3.4.3 Additional PBE Services

a. If you subscribe to "PBE Push Online" of PBE, the recipient is sent an e-mail notification with an encrypted attachment containing the original e-mail saved within it. The recipient is able to view the decrypted e-mail online (via a secure SSL session) in its browser by clicking on the encrypted attachment and entering its password.

b. If you subscribe to "PBE Push Offline" of the PBE, the recipient is sent an e-mail notification with an encrypted attachment containing the original e-mail saved within it. Following initial registration online, the recipient is able to view the decrypted e-mail offline using a Java application on its desktop.

c. If you subscribe to "PBE Pull" of PBE, the recipient is sent an e-mail notification. The recipient is able to view the decrypted e-mail online (via a secure SSL session) in its browser by logging into the secure Web portal and entering its password.

d. If you subscribe to "PBE Compose" of PBE, the recipient of an encrypted e-mail is able to send a brand new e-mail to any of your PBE Users.

e. If you subscribe to “PBE Branding Enterprise” of PBE, you will also receive both “PBE Branding” and “PBE Compose”.

f. If you subscribe to “PBE Combo” of PBE, E-mail Content Control will select the encryption method (i.e., “PBE Pull”, “PBE Push Online”, or “PBE Push Offline”) based on the E-mail Content Control rule determined by you.

3.4.4 Services Limitations

a. The number of secure e-mails, using PBE, you may send in any calendar month may not exceed 100 times the Registered Usage for PBE. When sending to multiple recipients, each unique address will be counted as a secure e-mail. In the event you exceed the number of permitted secure e-mails in a given calendar month, IBM will increase the Registered Usage and, at its sole discretion, adjust your subsequent invoices accordingly.

b. E-mails routed through PBE are limited to a maximum size of 15 MB per e-mail (when compressed).

c. The e-mail latency SLA does not apply to PBE.

3.4.5 Disclaimer

You acknowledge and agree that the encryption of e-mails using PBE will be performed in the United States and IBM cannot accept any responsibility for any breach of applicable legislation or regulations anywhere in the world. IBM is not liable for any damage or loss resulting directly or indirectly from any failure of PBE to fulfill your encryption obligations.

3.5 E-mail Antivirus

If selected by you in the Schedule, IBM will provide E-mail Antivirus to help you detect Viruses in your inbound and outbound Internet e-mail and attachments. E-mail Antivirus is limited to the number of Users specified in the Schedule.

3.5.1 IBM E-mail Antivirus Responsibilities

Activity 1 - Initialisation and Notification

IBM will:

a. provide automatic alerts of an inbound e-mail message or attachment found to contain a Virus, to the sender, intended recipient, and if requested by you in your profile to your e-mail administrator;

b. if you have selected to turn off notifications, forward Virus-infected e-mail to a secure server which is designed to automatically destroy it after 30 days;

c. at your request in exception circumstances, release e-mail which is shown to be releasable by the management tool, from the secure server to the originally intended recipient e-mail address (or addresses if a group e-mail name or alias), or redirect an infected e-mail to an alternate e-mail address upon receipt of the appropriate release authorisation form;

d. retain inbound Virus-infected e-mail, determined by IBM to be particularly infectious or damaging;

e. notify you of Virus-infected e-mail, detected but not intercepted by E-mail Antivirus, and provide you with sufficient information to enable you to delete such e-mail; and/or

f. configure the management tool to generate reports on a weekly or monthly basis, as selected by you in your profile.

Activity 2 - Technical and Ongoing Support

During the contract period, IBM will:

a. not intentionally transmit or release, and will instruct its subcontractors involved in E-mail Antivirus not to intentionally transmit or release, any known or suspected Virus-infected e-mail to third parties, other than to IBM, its subcontractors or any law enforcement personnel or entities involved in the detection of and protection against Viruses; and

b. should E-mail Antivirus be suspended or terminated for any reason whatsoever, reverse all relevant configuration changes made upon provisioning E-mail Antivirus and it shall be your responsibility to undertake all necessary configuration changes to your mail servers, and to inform your Internet Service Provider (“ISP”) of the need to reroute inbound e-mail.

3.5.2 Your E-mail Antivirus Responsibilities

You agree to:

a. assume primary responsibility for all configuration changes and e-mail Quarantine operations and administration. If you require assistance, you agree to:

   (1) promptly notify IBM if you require notifications to be turned off; or

   (2) promptly notify IBM if you require release of e-mail from the secure server (shown as releasable by the proprietary Internet-based configuration, management and reporting tool), to the originally intended recipient; and

b. take all necessary measures to ensure that you, and those sending e-mail from within the domains covered by E-mail Antivirus, are aware of any responsibilities you have with respect to data protection and privacy laws and/or regulations.

3.5.3 Service Level Agreements

In addition to the general SLAs described above, the following SLAs comprise the measured metrics for delivery of E-mail Antivirus. The sole remedies for failure to meet these SLAs are specified in the section entitled "SLA Remedies", below.

The SLA remedies are available provided you meet your obligations as defined in this Services Description.

SLAs

- Virus detection - E-mail Antivirus will detect 100% of the Viruses contained in scanned e-mail. Your systems will be deemed to be infected if a Virus, contained in an e-mail message received through E-mail Antivirus, has been activated within your systems.

  If a Virus-infected e-mail message is detected but not stopped, IBM may promptly notify you and provide sufficient information to enable you to identify and delete the Virus-infected mail. If infection is prevented, this SLA will not apply. If you fail to promptly act on notice of a Virus-infected mail, this SLA will not apply.

- Virus false positive capture rate - the Virus false positive capture rate will not exceed 0.0001% of your total e-mail traffic in a given calendar month.

SLA Remedies

A credit will be issued as the sole remedy for failure to meet any of the SLAs described in the section entitled "SLAs", during any given calendar month. You may obtain no more than one credit for each SLA per day, not to exceed a total for all SLAs of $10,000 (U.S.), or the equivalent in local currency, in a given calendar month.

- Virus detection remedy - If IBM fails to meet the Virus detection SLA, a credit will be issued for the applicable charges for one month of the E-mail Antivirus monitoring fee or $10,000 (U.S.), whichever is less.

  Such credit will only apply if you have provided notice to IBM, and IBM has confirmed and logged that a Virus has been passed to you through E-mail Antivirus. This remedy is the sole and exclusive remedy for any Virus infection passed to you through the E-mail Antivirus Services. This remedy shall not apply to any deliberate self-infection by you.

  IBM will scan as much of the e-mail 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 or encrypted attachments). Such e-mail and attachments are excluded from this SLA.

- Virus false positive capture rate remedy - if the Virus false positive capture rate exceeds 0.0001% of your total e-mail traffic in a given calendar month, a credit will be issued for the applicable charges for one month of the monitoring fee for E-mail Antivirus as specified below.

Percent Virus False Positive Capture Rate (during the Calendar Month)	Percent Credit of Monthly Charge
Greater than 0.0001% but at most 0.001%	25
Greater than 0.003% but at most 0.03%	50
Greater than 0.03% but at most 0.3%	75
Greater than 0.3%	100

3.6 E-mail Image Control

If selected by you in the Schedule, IBM will provide E-mail Image Control to help detect pornographic images contained in image files in your inbound and outbound e-mail and attachments. E-mail Image Control is limited to the number of Users specified in the Schedule.

IBM emphasises that the configuration of E-mail Image Control is entirely within your control. E-mail Image Control is intended to be used solely to enable you to enforce an existing, effectively implemented acceptable computer use policy (or its equivalent).

3.6.1 IBM E-mail Image Control Responsibilities

Activity 1 - Initialisation and Notification

IBM will:

a. scan your inbound and outbound Internet e-mail for potentially pornographic images contained in image files attached to an e-mail message;

b. make options available to you for determining the actions to be taken upon the detection of a suspected pornographic image, including:

   (1) log only;

   (2) identification of such e-mail within its header (for inbound e-mail only);

   (3) copying such e-mail to a predetermined e-mail address;

   (4) redirection of such e-mail to a predetermined e-mail address; and

   (5) deletion of such e-mail; and

c. provide automatic alerts to the sender and, if e-mail is inbound, provide alerts to recipient of an inbound e-mail or attachment found to contain a suspected pornographic image.

Activity 2 - Technical and Ongoing Support

During the contract period, IBM will:

a. not store any item suspected of containing a pornographic image, under any circumstances; and

b. should E-mail Image Control be suspended or terminated for any reason whatsoever, reverse all relevant configuration changes made upon provisioning E-mail Image Control and it shall be your responsibility to undertake all necessary configuration changes to your mail servers, and to inform your ISP of the need to reroute inbound e-mail.

3.6.2 Your E-mail Image Control Responsibilities

You agree to:

a. set the configuration options for E-mail Image Control for your domains according to your needs. Options are available for specifying the level of pornographic detection sensitivity. Sensitivity can be set to high, medium or low. More pornographic images will be detected at a high sensitivity level and fewer pornographic images will be detected at a low sensitivity level. However, the determination of what constitutes pornographic images is subjective. Therefore, the level of pornographic detection cannot be precisely measured; and

b. take all necessary measures to ensure that you, and those sending e-mail from within the domains that are covered by E-mail Image Control, are aware of any responsibilities you have with respect to data protection and privacy laws and/or regulations.

3.7 E-mail Antispam

If selected by you in the applicable Schedule, IBM will provide E-mail Antispam to help protect you from Spam by scanning your inbound Internet e-mail and attachments to detect Spam and handle it in accordance with predetermined guidelines. E-mail Antispam is limited to the number of Users specified in the Schedule.

3.7.1 IBM E-mail Antispam Responsibilities

Activity 1 - Initialisation and Notification

IBM will:

a. provide you with the capability to configure a blacklist. If this detection method is selected and an incoming e-mail is received from a blacklisted domain, an action will be taken as defined by the configuration options set by you in your profile;

b. provide you with the capability to configure a white list. If this detection method is selected and an incoming e-mail is received from a domain in the white list, it will automatically bypass any other Spam detection methods;

c. upon activation of E-mail Antispam, initialise the Spam action as “deletion of Spam”. You may request a different option prior to the initial activation of E-mail Antispam, or you may change

this option by accessing the Internet management tool. The following options for determining the action to be taken upon the detection of Spam are available:

(1) tagging of Spam within its header (the Spam continues to be sent to the designated recipient);

(2) redirection of Spam to a predetermined e-mail address;

(3) Quarantine of Spam; or

(4) deletion of Spam;

d. if the "Quarantine of Spam" option is selected, provide Spam Quarantine for each of the domains specified by you. The default option for notifying the User that Spam has been stored is set to "notifications to be received on a per day basis". You may alter the default setting, at any time, to one of the following options:

(1) notifications to be received on a per day basis;

(2) notifications to be received at various intervals; or

(3) notifications are not to be received.

Activity 2 - Technical and Ongoing Support

During the contract period, IBM will:

a. store suspected Spam for a maximum of 14 days after which it will be automatically deleted;

b. provide Spam Quarantine to a User after you configure each domain according to your needs;

c. configure the User's Spam Quarantine account so that it may be accessed by the User;

d. tag and send suspected Spam to the recipient, if for any reason the Spam Quarantine service is not able to accept e-mail; and

e. should E-mail Antispam be suspended or terminated for any reason whatsoever, reverse all relevant configuration changes made upon provisioning E-mail Antispam and it shall be your responsibility to undertake all necessary configuration changes to your mail servers, and to inform your ISP of the need to reroute inbound e-mail.

3.7.2 Your E-mail Antispam Responsibilities

You agree to:

a. be responsible for changing the default Spam option ("deletion of Spam"), via the Internet management tool, if another option is desired;

b. set the configuration options for E-mail Antispam for your domains according to your needs;

c. assume primary responsibility for all configuration changes and e-mail Quarantine operations and administration. If you require assistance, you agree to:

(1) promptly notify IBM if you require notifications to be turned off; or

(2) promptly notify IBM if you require release of e-mail from the secure server (shown as releasable by the proprietary Internet-based configuration, management and reporting tool), to the originally intended recipient; and

d. take all necessary measures to ensure that you, and those sending e-mail from within the domains that are covered by E-mail Antispam, are aware of any responsibilities you have with respect to data protection and privacy laws and/or regulations.

3.7.3 Service Level Agreements

In addition to the general SLAs described above, the following SLAs comprise the measured metrics for delivery of E-mail Antispam. The sole remedies for failure to meet these SLAs are specified in the section entitled "SLA Remedies", below.

The SLA remedies are available provided you meet your obligations as defined in this Services Description.

SLAs

- Spam capture rate - E-mail Antispam will detect 99% of the Spam contained in scanned e-mail.

  A lower Spam capture rate will apply to e-mail containing Asian character sets. In the event that such Spam capture rate falls below 99%, you may be entitled to a 25% credit of your monthly charge. In the event that the Spam capture rate falls below 96%, you may be entitled to a 100% credit of your monthly charge.

  The Spam capture rate SLA is not applicable if:

(1) you have not implemented the recommended settings for E-mail Antispam; or

(2) the e-mail message was not sent to a legitimate address.

- Spam false positive capture rate - the Spam false positive capture rate will not exceed 0.0003% of your total e-mail traffic in a given calendar month.

  The following e-mails are excluded from the Spam false positive capture rate guarantee:

  (1) e-mails which do not constitute legitimate business e-mail;

  (2) e-mails containing more than 20 recipients;

  (3) e-mails from senders who are on your blocked sender list, including those defined by individual Users if you have enabled User-level settings;

  (4) e-mail sent from a compromised machine;

  (5) e-mail sent from a machine which is on a third party block-list;

  (6) e-mail sent to more than 20 recipients and having at least 80% of the same content.

  Credit will be issued only for false positive e-mail you send to support@messagelabs.com within five days of receipt of the e-mail message.

SLA Remedies

A credit will be issued as the sole remedy for failure to meet any of the SLAs described in the section entitled "SLAs", during any given calendar month. You may obtain no more than one credit for each SLA per day, not to exceed a total for all SLAs of $10,000 (U.S.), or the equivalent in local currency, in a given calendar month.

- Spam capture rate remedy - If IBM fails to meet the Spam capture rate SLA, a credit will be issued for all or part of the monthly charge for E-mail Antispam, as indicated in the following table, or $10,000 (U.S.), whichever is less.

Spam Capture Rate during the Calendar Month	Monthly Charge to be Credited
Greater than 98% but less than 99%	25%
Greater than 97% but less than 98%	50%
Greater than 96% but less than 97%	75%
Less than 96%	100%

- Spam false positive capture rate remedy - if IBM fails to meet the Spam false positive capture rate SLA, a credit will be issued for all or part of the monthly charge for E-mail Antispam, as indicated in the following table.

Spam False Positive Capture Rate (during a Calendar Month)	Credit of Monthly Charge
Greater than 0.0003% but at most 0.003%	25%
Greater than 0.003% but at most 0.03%	50%
Greater than 0.03% but at most 0.3%	75%
Greater than 0.3%	100%

3.8 E-mail Content Control

If selected by you in the Schedule, IBM will provide E-mail Content Control for your e-mail that is in line with your acceptable computer use policy (or its equivalent). E-mail Content Control is limited to the number of Users specified in the Schedule.

E-mail Content Control will allow you to build a collection of rules (referred to herein as the "rules") upon which inbound and outbound Internet e-mail is filtered. IBM emphasises that the configuration of E-mail Content Control is entirely within your control. The accuracy of the rules and configuration will determine the accuracy of E-mail Content Control. E-mail Content Control is intended to be used solely to enable you to enforce an existing, effectively implemented acceptable computer use policy (or its equivalent).

If E-mail Content Control is used in conjunction with the Quarantine action of the E-mail Antispam services, it may result in suspected Spam being Quarantined before it has been filtered by E-mail Content Control.

3.8.1 IBM E-mail Content Control Responsibilities

Activity 1 - Initialisation and Notification

IBM will:

a. provide the capability to help you configure your own rule-based e-mail filtering strategy in accordance with your acceptable computer use policy (or its equivalent);

b. provide lists of suggested words (called "Word Lists") that you may use to create the rules;

c. scan as much of the e-mail and its attachments as feasible, based on the rules and your configuration. It may not be possible to scan attachments with content under the direct control of the sender; and

d. make options available to you for determining the actions to be taken upon the detection of e-mail suspected of meeting the rules, which should be in line with your existing acceptable computer use policy. The options include:

   (1) tagging e-mail within the e-mail headers;

   (2) redirecting e-mail to a predetermined e-mail address;

   (3) copying e-mail to a predetermined e-mail address;

   (4) compressing e-mail attachments;

   (5) logging only to the proprietary Internet-based reporting and management tool; and

   (6) deletion of e-mail.

Activity 2 - Technical and Ongoing Support

Should E-mail Content Control be suspended or terminated for any reason whatsoever during the contract period, IBM will reverse all relevant configuration changes made upon provisioning the E-mail Content Control and it shall be your responsibility to undertake all necessary configuration changes to your mail servers, and to inform your ISP of the need to reroute inbound e-mail.

3.8.2 Your E-mail Content Control Responsibilities

You agree to:

a. disclose the Word Lists only to those persons in your company involved in the matters hereunder and who have a specific need to know. You acknowledge that the Word Lists may be considered offensive and you agree to indemnify IBM and its subcontractors against any damages (including reasonable costs and attorneys' fees) that may be awarded to any third party (including any of your employees) with respect to any claim or action arising out of IBM or its subcontractors supplying you with the Word Lists;

b. allow IBM to compile and publish default word lists using the rules or words obtained from your custom word lists;

c. attend a training course on E-mail Content Control configuration;

d. assume primary responsibility for release of e-mail, shown as releasable from the secure server to the originally intended recipient, and in exceptional circumstances, to ensure your notice to IBM to release e-mail is processed in a timely manner;

e. set the configuration options for E-mail Content Control for each of your domains, according to your needs; and

f. take all necessary measures to ensure that you, and those sending e-mail from within the domains covered by E-mail Content Control, are aware of and comply with any responsibilities or obligations that you have with respect to data protection and privacy laws and/or regulations.