Service Description

IBM Managed Security Services for E-mail Security

1. Scope of Services

IBM Managed Security Services for E-mail Security (called "MSS for E-mail Security") may include:

a. E-mail Antivirus services to help detect viruses and certain other images in your Internet e-mails;

b. E-mail Image Control services to help detect pornographic images contained in image files in both your inbound and outbound e-mail and attachments;

c. E-mail Antispam services to help safeguard your Internet e-mails from Spam; and/or

d. E-mail Content Control services to help you detect content in line with your acceptable computer use policy (or its equivalent) in your Internet e-mails.

The details of your order (e.g., the services you require, contract period, and charges) will be specified in the Order.

Definitions of service-specific terminology can be found at www.ibm.com/services/iss/wwcontracts

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 Towers (minimum of two), designated to provide MSS for E-mail Security to you.

E-mail Services Availability – the ability to establish an SMTP session on port 25 of the Designated Tower Cluster and (i) receive your inbound e-mail on behalf of your domain on a 24 hours/day by 7 days/week basis; and (ii) accept your outbound e-mail from your correctly configured SMTP host on behalf of your domain(s) on a 24 hours/day by 7 days/week basis.

Latency – the average roundtrip time for e-mails sent every five minutes to and from every Tower. The time is measured and reported by a tracking tool on a monthly basis. If the average roundtrip of your Designated Tower Cluster exceeds the delays stated in the section of this document entitled "Other Terms and Conditions", subsection entitled "Service Level Agreements", subsection entitled "Latency", you may submit a credit request.

Open Relay – an e-mail server, configured to receive e-mail from an unknown or unauthorized 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 you 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 your configuration settings, prior to action by the user or automatic deletion.

Spam – unsolicited commercial e-mail.

Tower – a cluster of load balanced e-mail servers.

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

3. MSS for E-mail Security

3.1 MSS for E-mail Security Coordination

3.1.1 IBM Responsibilities

IBM will provide a deployment engineer who will be the IBM focal point during the deployment phase of MSS for E-mail Security. The deployment engineer will:

a. provide you with a customer profile, which you must complete prior to IBM providing MSS for E-mail Security;

b. review this Service Description, and any associated documents, with your Point of Contact;

c. coordinate and manage the technical activities of the IBM assigned personnel; and

d. establish and maintain communications through your Point of Contact during the deployment phase of MSS for E-mail Security.

3.1.2 Your Point of Contact Responsibilities

Prior to the start of MSS for E-mail Security, you will designate a person (called "your Point of Contact"), to whom all communications relative to the services will be addressed and who will have the authority to act on your behalf in all matters regarding these services. Your Point of Contact will:

a. complete and return the customer profile to IBM within ten business days of your receipt;

b. serve as the interface between the IBM MSS for E-mail Security team and all of your departments participating in MSS for E-mail Security, as well as any third-party vendors, including Internet service providers (“ISPs”) and content-hosting firms, used by you to implement your Internet presence;

c. obtain and provide applicable information, data, consents, decisions and approvals as required by IBM to perform MSS for E-mail Security, within two working days of an IBM request; and

d. help resolve MSS for E-mail Security issues, and escalate issues within your organization, as necessary.

3.1.3 Your General Responsibilities

The IBM performance of MSS for E-mail Security is dependent on your performance of these general responsibilities. You agree to:

a. provide all necessary equipment and software and pay communication charges to access the IBM Web portal or any other Web tool required for provision of MSS for E-mail Security;

b. make appropriate personnel available to assist IBM in the performance of the IBM responsibilities;

c. permit IBM to disclose this document and Order to its subcontractors, notwithstanding anything to the contrary in this document or a related agreement, in connection with the MSS for E-mail Security to be performed hereunder;

d. be responsible for the content of any database, the selection and implementation of controls on its access and use, backup and recovery and the security of the stored data. This security will also include any procedures necessary to safeguard the integrity and security of software and data used in MSS for E-mail Security from access by unauthorized personnel; and

e. be responsible for the identification and interpretation of any applicable laws, regulations, and statutes that affect your existing application systems or programs to which IBM will have access during delivery of MSS for E-mail Security. It is your responsibility to ensure that the systems and programs meet the requirements of those laws, regulations and statutes.

3.2 General Services

3.2.1 IBM 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 MSS for E-mail Security. This tool will also offer a number of configuration and management facilities;

b. provide MSS for E-mail Security on a 24 hours/day by 7 days/week basis;

c. provide technical support for MSS for E-mail Security on a 24 hours/day by 7 days/week basis; and

d. work with you to resolve problems with MSS for E-mail Security on a 24 hours/day by 7 days/week basis.

3.2.2 Your Responsibilities

You agree to:

a. monitor the number of users. Changes to the number of users will be processed in accordance with the “Changes” section of this document;

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 MSS for E-mail Security (or any part or portion thereof) to in any way develop or promote commercial services similar to said MSS for E-mail Security;

SHOULD YOU FAIL TO MEET THESE OBLIGATIONS AND DISRUPTION OCCURS TO MSS FOR E-MAIL SECURITY, IBM WILL INFORM YOU OF SUCH FAILURES AND RESERVES THE RIGHT TO WITHHOLD PROVISION OF OR SUSPEND ALL OR PART OF MSS FOR E-MAIL SECURITY 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 us to supply MSS for E-mail Security 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 the customer profile; and

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

3.3 E-mail Antivirus

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

3.3.1 IBM Responsibilities

Activity 1 - Initialization and Notification

IBM will:

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

b. notify the sender and, if requested by you in the customer profile, an e-mail administrator, of an outbound e-mail or attachment found to contain a Virus;

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

d. at your request in exception circumstances, to 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 authorization form from you;

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

f. 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

g. configure the management tool to generate reports on a weekly or monthly basis, as selected by you in the customer 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 ISP of the need to reroute inbound e-mail.

Activity 3 - Service Level Agreements

The following Service Level Agreements ("SLAs") apply only to E-mail Antivirus during the Contract Period:

a. The objective is for E-mail Antivirus to detect 100% of the Viruses contained in e-mails scanned by this service. Your systems will be deemed to be infected if a Virus, contained in an e-mail received through this service, has been activated within your systems.

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

c. If your systems are infected by one or more Viruses in a single calendar month during the Contract Period, IBM will credit you with the lesser of: (i) 100% of your monthly charge for the E-mail Antivirus service, or (ii) three thousand dollars ($3,000 U.S.) or the equivalent in local currency. 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 the service. This remedy is the sole and exclusive remedy for any Virus infection passed to you through the E-mail Antivirus service. This remedy shall not apply to any deliberate self-infection by you.

3.3.2 Your Responsibilities

You agree to:

a. assume primary responsibility for all configuration changes and e-mail Quarantine operations and administration. However, if you require assistance, you agree to promptly notify IBM if you require notifications to be turned off or if you require release of e-mails, shown as releasable by the proprietary Internet-based configuration, management and reporting tool, to the originally intended recipient from the secure server; 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.

3.4 E-mail Image Control

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

IBM emphasizes 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).

3.4.1 IBM Responsibilities

Activity 1 - Initialization and Notification

IBM will:

a. scan your inbound and outbound e-mail using Image Composition Analysis to attempt to detect potentially pornographic images contained in image files attached to an e-mail;

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.

3.4.2 Your 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.

3.5 E-mail Antispam

If selected by you in the applicable Order, IBM will provide E-mail Antispam to help protect you from Spam by scanning your inbound 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 Order.

3.5.1 IBM Responsibilities

Activity 1 - Initialization 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 the customer 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, initialize the Spam action as “deletion of Spam”. You may request a different option prior to the initial activation of the service, 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.

Activity 3 - Service Level Agreements

The following SLAs apply only to E-mail Antispam during the Contract Period:

False Positive E-mails

a. If the false positive capture rate exceeds 0.0004% of your total e-mail traffic in a calendar month, you may be entitled to the following credit:

Percentage False Positive Capture Rate During the Calendar Month	Percentage of Monthly Charge to be Credited
Greater than 0.0004 but less than 0.004	25%
Greater than 0.004 but less than 0.04	50%
Greater than 0.04 but less than 0.4	75%
Greater than 0.4	100%

b. Credit will be given only for false positive e-mails sent to support@messagelabs.com within five days of receipt.

c. The following e-mails are excluded from the false positive SLA:

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

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

(3) e-mails in which less than 80% of the e-mail content is in native English;

(4) sender of the e-mail is on your blacklist;

(5) e-mails sent from a compromised machine;

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

(7) e-mails sent to more than 20 recipients and have at least 80% the same in content.

d. IBM reserves the right to charge you $200.00 per hour for administrative costs of substantially burdensome investigations of false positive e-mails.

False Negative E-mails

a. If the false negative capture rate exceeds 5% of your total e-mail traffic in the number of consecutive days stated in the following table, you may be entitled to the specified credit:

Number of consecutive days during which the false negative capture rate rises above 5% in any calendar month	Percentage of Monthly Charge to be Credited
5	25%
10	50%
20	75%
21+	100%

b. the false negative SLA is not applicable if:

(1) you have not implemented the provided configuration guidelines; or

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

c. credit will be given only for false negative e-mails sent to support@messagelabs.com within five days of receipt of the e-mail.

d. IBM reserves the right to charge you $200.00 per hour for administrative costs of substantially burdensome investigations of false negative e-mails.

3.5.2 Your 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. However, if you require assistance, you agree to promptly notify IBM if you require notifications to be turned off or if you require release of e-mails shown as releasable by the proprietary Internet-based configuration, management and reporting tool to the originally intended recipient from the secure server, is processed in a timely manner; 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.

3.6 E-mail Content Control

If selected by you in the applicable Order, IBM will provide E-mail Content Control to help you configure a rule-based filtering strategy 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 Order.

E-mail Content Control will allow you to build a collection of rules (referred to herein as the "rules") upon which inbound and outbound e-mail is filtered. IBM emphasizes 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 service, it may result in suspected Spam being Quarantined before it has been filtered by E-mail Content Control.

3.6.1 IBM Responsibilities

Activity 1 - Initialization 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 its header;

   (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

During the Contract Period, IBM will:

a. should E-mail Content Control be suspended or terminated for any reason whatsoever, 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.

3.6.2 Your 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) in respect of 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-mails, 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-mails 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.

4. Changes

You may request a change to your MSS for E-mail Security by delivering one month's prior written notice to IBM. IBM will confirm the change in a revised Order with any applicable adjustment in charges. The Total Annual Charge will not be less than the Minimum Annual Charge set forth in the Order.

5. Other Terms and Conditions

IBM reserves the right to modify the terms of this Service Description, including the SLAs, with 30 days prior written notice.

5.1 Disclaimer/Warranty

You understand and agree that IBM does not make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information provided as part of MSS for E-mail Security.

5.2 Service Level Agreements

5.2.1 General

a. 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.

b. Service levels are not applicable:

(1) until 30 days after activation of MSS for E-mail Security;

(2) if your system configurations do not comply with the provided configuration guidelines;

(3) during periods of Planned Maintenance;

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

(5) during any period of suspension of MSS for E-mail Security in accordance with the Agreement.

c. All credits will be pro-rated to the number of users affected by the degradation in levels of service.

d. The IBM total maximum liability, in any calendar month, shall not exceed 100% of your monthly charge.

5.2.2 Availability

If the service availability is below 100% in any calendar month during the Contract Period, you may be entitled to the following credit:

Percentage Email Service Availability per calendar month	Percentage credit of Monthly Charge
Less than 100% but greater than 99.0%	20
Less than 99.0% but greater than 98.0%	40

Less than 98.0% but greater than 97.0%	60
Less than 97.0% but greater than 96.0%	80
Less than 96.0% but greater than 95.0%	100
Less than 95%	Termination of MSS for E-mail Security, at your discretion. Should the services be terminated, such termination shall be the sole and exclusive remedy for availability of MSS for E-mail Security of less than 95% in a given calendar month.

5.2.3 Latency

This Latency SLA does not apply to:

a. any Virus outbreak where the Virus to e-mail ratio is greater than 1:200;

b. a denial of service attack caused by you upon yourself, or such an attack from a third party; or

c. delays caused by a mail loop from/to your systems.

Average roundtrip time of < 95% of measurements (in minutes)	**Percentage credit of Monthly Charge**
Greater than 2 but less than 4	5
Greater than 4 but less than 6	10
Greater than 6 but less than 8	15
Greater than 8 but less than 10	20
Greater than 10	25