



MessageLabs Free Email Audit Agreement

Date		MessageLabs Account Manager	
MessageLabs Reference Number			

1. Customer Account Information

Customer Details	
Company Name	
Address Line 1	
Address Line 2	
City	
Region	
Zip Code	
Country	
Technical Contact	
Name	
Telephone Number	
Email Address	

2. Service Volume

Number of Users to be scanned	
(Number rounded up to the nearest 50)	

3. Service Selection

Please select the MessageLabs services to be provisioned.

	MessageLabs Service		
	Anti-Virus	Image Control	Anti-Spam
Services to be provisioned	✓	✓	✓

4. MessageLabs' Configuration Requirements

4.1. Customer's Inbound Email

In order for MessageLabs to scan your inbound email, the service must be configured to know which domains to scan. After an email has successfully passed through MessageLabs' control towers, it is transferred to your designated SMTP mail server using the domain name and associated IP address. Please note that only one IP address can be used for each domain name and the IP Address should be the externally visible IP Address (i.e. visible from the Internet) for your mail server.

Details of your inbound mail servers:	
Domain Name (maximum 3)	IP Address

4.2. Customer's Outbound Email

In order for MessageLabs to scan your outbound email, the service must be configured to accept email from your network's final point of exit (e.g. firewall, router, mail server, etc).



IP Addresses that you send outbound email from:	

4.3. Email Virus Alert Messages

When the MessageLabs service detects and intercepts an email containing a virus, the infected email is quarantined and an automatic alert message can be sent to both the sender and recipient. If you would also like MessageLabs to copy all virus alert messages to a specific address, please enter the email address details below in 4.4 below (recommended).

5. Provision of Service

MessageLabs will contact you shortly after this agreement has been approved to explain what changes you will need to make to your mail server to enable MessageLabs to scan your email. You are responsible to use all reasonable efforts to get the service set up promptly.

5.1. Customer's Inbound Email

To have MessageLabs scan your inbound email, it is necessary for the MX records of the relevant domain names to be changed so the inbound email is directed to the MessageLabs control towers. Instructions on how to achieve this will be sent to you by email once your request has been approved and processed.

5.2. Customer's Outbound Email

To have MessageLabs scan your outbound email, you must configure your mail servers to relay all outbound email to the MessageLabs control towers. The IP Addresses of the appropriate MessageLabs control towers will be sent to you by email once your request has been approved and processed.

6. Open Relay and Spam

Your request will not be processed if your mail server allows open relay and the Service will be suspended immediately if you send unsolicited commercial email (Spam).

Should your mail server allow open relay (i.e. you allow mail not destined for your company to be relayed through your server) you may already be or may become blacklisted. For more information see <http://www.abuse.net>.

MessageLabs will test your mail server before you receive the service, and on a regular basis thereafter, to ensure your mail server does not support open relay. Should we find that your mail server allows open relay or is blacklisted, we reserve the right to suspend service immediately. We will work with you to get the problem rectified as soon as possible and reinstate the service once the problem has been corrected.

7. Compliance

7.1 The Customer recognises that information sent to and from the Customer will pass through the Service and accordingly the Customer agrees that the Customer will use the Service for legitimate business purposes and:

7.1.1 comply with all relevant legislation applicable to use of the Internet;

7.1.2 conform to the protocols and standards published on the Internet from time to time and adopted by the majority of Internet users; and

7.1.3 indemnify MessageLabs against any liability to third parties resulting from information passing through the Service from the Customer.

8. Liability

Both parties acknowledge that during the audit period MessageLabs shall provide the services on an "as is" basis and MessageLabs 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. The Customer agrees that MessageLabs shall have no liability to the Customer for



any loss or damage however caused or arising out of the provision of the services WHETHER DUE TO MESSAGELABS NEGLIGENCE OR FAILURE TO PERFORM OR ANY OTHER REASON.

9. Termination

9.1. Timing of Agreement

The audit period shall begin from the date that you are notified that the MessageLabs services have been provisioned pursuant to section 5 above. There will be no charge made to the Customer for services provided during the audit period.

The audit shall continue for a period of no longer than 30 days. Thereafter this agreement shall terminate with immediate effect. It shall be the Customer's responsibility to re-point their MX records away from the MessageLabs service. MessageLabs shall accept no liability for loss of email due to the Customer's failure to comply with this Clause.

During the 30 day audit period MessageLabs shall produce a report which will be taken from the 7 day evaluation window during the audit period.

9.2. Cancellation

Either party may cancel this agreement at any time during the audit period upon 48 hours notice to the other party.

10. Data Protection

10.1 The Customer shall take all necessary measures to ensure that it, and all its employees, are aware of any responsibilities they have in respect of data protection and privacy laws and/or regulations and as MessageLabs has no control or influence over the content of the Emails processed by the Service.

10.2 As required by law, the Customer shall use all reasonable efforts to ensure it informs (for example via a banner message on Emails) those who use any communications system covered by the Service, that communications transmitted through such system maybe intercepted, and indicate the purposes of such interception.

11. Governing Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of England and Wales and each party hereby irrevocably submits to the exclusive jurisdiction of the Courts of England and Wales.

Audit requested by Customer:

Audit Approved by MessageLabs:

By _____
Authorised signature

Name (type or print)

Title

On _____
Date

By _____
Authorised signature

Name (type or print)

Title

On _____
Date

Implementation and Evaluation Period Success Criteria

The following table details the Email Audit Service that will be delivered.

The purpose of this Email Audit service is to help organisations and business managers to clearly understand how email is being used within their organisation. An Email Audit will quickly highlight issues such as email misuse, employee productivity, bandwidth consumption, and potential corporate governance or non-compliance with the company's 'Acceptable Usage Policy' for email.

i)	Overview For a period of up to 30 days email will be routed through the MessageLabs infrastructure. No attempt will be made to stop spam or pornographic content but we will block viruses.	
ii)	Summary of email traffic <ul style="list-style-type: none"> a. Total mail volume, by period b. Mail trends (time of day, peak periods, etc.) c. Unsolicited mail (spam) d. Viruses, trojans and malware e. Inappropriate or pornographic images 	
iii)	Network monitoring <ul style="list-style-type: none"> a. Open relays c. Denial of service (email) 	
iv)	Outputs. <ul style="list-style-type: none"> a. Assessment of compliance with best practice email policy. b. Productivity costs of unsolicited mail. c. Threat risk assessment from viruses, Trojans and malware d. Potential email bottlenecks. e. Relay testing - open relays you are unaware of. f. Potential Denial of Service or mail bomb 	