Guide to Establishing a Content Security Policy for E-mail and the Web

MIMEsweeper™

INDEX

Introduction

Part One: Establishing an E-mail Content Security Polic 5

1. File types 5
2. Legal Disclaimers 10
3. Virus Scanning 11
4. Text Analysis 12
5. Spam 13
6. Spoof 14
7. Portable Code 14
8. Size management 15
9. Number of Attachments 15

Part Two: Establishing a Web Content Security Policy 16

1. Detection of Web Transfers 16
2. Web based e-mail 20
3. Virus Scanning 20
4. Text Analysis 21
5. Portable Code 21
6. Authenticode 22
7. Content and Time of Day 22
8. Using Existing User Lists 23
9. Exceptions to the Rule 23

Part Three: Maintaining a Content Security Policy 24

Conclusion 26

CONTENT SECURITY
- putting the threats into perspective

For many Internet users, the utilization of e-mail and the Web represents a conflicting set of forces. On the one hand they represent immense potential benefits in business communications, productivity and market effectiveness. On the other hand, they constitute possible breaches of security with unknown but potentially devastating consequences.

Although Content Security has sometimes been positioned as a technology for countering threats to the integrity of the corporate network, such as e-mail and Web-borne viruses, its role is to also address threats to the integrity of the corporate business brought about by an organizations use of the Internet. Content Security is about business security, rather than technology security.

Information in itself may not constitute a security risk. However, the potential risk occurs when information is accessed or moved from one place to another and when controls may not be sufficient to assure its integrity. It really depends on who you are, or what your organization is, as to whether you are likely to be affected by Content Security threats.

So, you need to consider your reaction to any threat and assess the cost carefully, and this guide is designed to help you decide and consider what protection you need, and formulate a plan for combating common content-based threats.

Setting up an e-mail and Web usage policy for the first time can be a complicated business and so this policy guide will help you define a Content Security policy specific to your needs. Once completed, you can use this checklist to define the areas within which you need to apply a policy, and then use it to evaluate the Content Security solutions available.

Part One: Establishing your E-mail Policy

1. Detection of attachments by type

a) Type: Images

This is the ability to control inbound and outbound e-mail based on what type of attachment is contained in the message. The attachment type needs to be determinable by the file signature and not its extension, so as to stop users renaming files to bypass policy. This feature would allow for recognition of all files of a certain type and a certain size.

The types of image files you should consider are JPEG, DXF, DWG, PSP, PNG, PIC, TIFF, PCX, FLI, BMP and GIF. You may also want to intercept all files or only allow between specified user groups or individuals.

Once you have decided whether to detect images, you can then determine how to deal with them. Use the table below to determine this area of your e-mail policy.

Type	Size	User	Inbound E-mail Management	Outbound E-mail Management
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party

b) Type: Movies

Video files are normally large in size and may not be work related. Sending and receiving of video files could lead to resource depletion.

The types of movie files you should consider are AVI, QTM, MPEG and RT. You may also want to intercept all files or only allow between specified user groups or individuals.

Once you have decided who should be allowed to send and receive movies, you can then determine how to deal with them. Use the table below to determine this area of your e-mail policy.

Type	Size	User	Inbound E-mail Management		Outbound E-mail Management	
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party

c) Type: Compression formats

To ensure compressed files are threat free, Content Security tools need to be able to perform recursive analysis - i.e. repeatedly 'unwrapping' files – to check the compressed data in its raw state.

The types of compression formats you should consider are TAR, GZIP, ZIP, CMP, CAB, ARJ, LZH and RAR. You may also want to intercept all formats or only allow between specified user groups or individuals.

Once you have decided whether to detect compressed files, you can then determine how to deal with them. Use the table below to determine this area of your e-mail policy.

Type	*Size*	*User*	*Inbound E-mail Management*	*Outbound E-mail Management*
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party

d) Type: Executable attachments

Executable objects can be large, and may not be work related. Executables are also one of the primary sources for virus propagation, so you need to ensure that your Content Security solution can check for these types of files.

The types of executable attachments you should consider are Win32Exe, Win32DLL, Win31Exe, Win32unknown, JavaByte and DosExe. You may also want to intercept all executables or only allow between specified user groups or individuals.

Once you have decided whether to detect executable files, you can then determine how to deal with them. Use the table below to determine this area of your e-mail policy.

Type	Size	User	Inbound E-mail Management	Outbound E-mail Management
________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party

e) Type: Document files

To ensure only those personnel or departments receive files that relate to normal business activity, you might want your Content Security solution to be able to check for attachments by document type.

For example, it might be deemed that marketing can send and receive .pdf files as these are typically necessary to continue normal business activity. However, for the Accounts Department to send and receive .pdf files might be deemed as unnecessary for everyday business dealings, and you may wish to block or quarantine them for further investigation.

The types of document files you should consider are FAX, rich text, CDA, Microsoft Project, Microsoft PowerPoint, Microsoft Word, Microsoft Excel, OLE Package, 1-2-3, Acrobat (PDF), Text and HTML. You may also want to intercept all files or only allow between specified user groups or individuals.

Once you have decided whether to detect document files, you can then determine how to deal with them. Use the table below to determine this area of your e-mail policy.

Type	Size	User	Inbound E-mail Management	Outbound E-mail Management
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
____________	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party

2. Legal Disclaimers

Expanding Internet usage has meant that the legal liability of the content of an e-mail is switching from the employee to the employer. In light of recent litigation the ability to attach legal disclaimers to e-mails is becoming increasingly important.

In addition, the flexibility to adapt and customize e-mail disclaimers for the company as a whole, a department and an individual, is increasingly being implemented as part of demonstrating effective security policies.

Therefore, a Content Security solution needs to be able to allow the addition of a text or "real text" text message to the start or end of an e-mail message text body, ideally performed by default for all outbound mail.

An example disclaimer could be:
"This e-mail and any files transmitted with it are confidential and intended for the sole use of the individual or entity to whom they are addressed. If you have received this e-mail in error please notify the system manager. This e-mail message has been swept for the presence of computer viruses."

Your legal disclaimer for the Company:

_____

_____

_____

_____

_____

_____

Your legal disclaimer for _____ department:

_____

_____

_____

_____

_____

_____

Your legal disclaimer for _____ individual:

_____

_____

_____

_____

_____

_____

_____

3. Virus Scanning

The ability to scan for viruses is an important tool within a Content Security solution. The best Content Security solution should allow the use of one or more user-selectable virus tools to check attachments for viruses and Trojans. It is also wise to choose a solution that can detect behavior patterns of threats, ensuring better detection.

Some viruses are cleanable and some are not. It's key that your Content Security solution can manage files that it can and cannot clean. Use the table below to determine how, and with which tools, you want to manage the virus scanning of e-mail.

Anti-Virus Tool	User	Inbound E-mail Management of cleanable viruses	Outbound E-mail Management of uncleanable viruses
________________	❑ All ❑ By Department ❑ By Individual	❑ Clean ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender ❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender
________________	❑ All ❑ By Department ❑ By Individual	❑ Clean ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender ❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender
________________	❑ All ❑ By Department ❑ By Individual	❑ Clean ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender ❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender
________________	❑ All ❑ By Department ❑ By Individual	❑ Clean ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender ❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender
________________	❑ All ❑ By Department ❑ By Individual	❑ Clean ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender ❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender
________________	❑ All ❑ By Department ❑ By Individual	❑ Clean ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender ❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender
________________	❑ All ❑ By Department ❑ By Individual	❑ Clean ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender ❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Add Text ❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party ❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender

4. Text Analysis

The ability to analyze data streams for pre-defined key words and phrases enables organizations to eliminate a variety of threats. The type of threats that can be detected this way within e-mail include: leakage of confidential information; the spread of libelous comments; profane or unsuitable e-mail; junk or Spam e-mail; and harassment and discrimination via e-mail. Text analysis can also be a highly efficient way of managing certain types of malicious code, hoax viruses or dangerous scripts.

A Content Security solution needs to allow for the detection of text, words or phrases in e-mail via intelligent text analysis in the subject, body or text attachments of e-mail.

In addition, it is useful to be able to define complex search algorithms to detect desired and undesired content, such as the concept of 'Nearness' such as blocking e-mails with the word - not for external disclosure "Breast" but allow the word if it appears within 5 words of the word "Chicken".

Some examples of text analysis could be:

- Search for the word 'black'. Disallow, if the word 'man' is next to it
- Quarantine e-mails that contain the phrase 'Company Confidential - not for external disclosure'

You may want to perform text analysis on all files, or only those to or from specified user groups and individuals.

Use the table below to note the words or phrases your company needs to be able to search for within e-mail:

Text	***User***	***Inbound E-mail Management***	***Outbound E-mail Management***
________ ________ ________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
________ ________ ________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
________ ________ ________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
________ ________ ________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
________ ________ ________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party
________ ________ ________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party	❑ Deliver ❑ Delete ❑ Quarantine ❑ Park ❑ Forward ❑ Send alert ❑ Archive ❑ Write event to log ❑ Reply to sender ❑ Forward to 3rd party

5. Spam

Derived from a sketch in Monty Python's Flying Circus, the term Spam© has come to mean unsolicited or junk e-mail. It takes up valuable bandwidth and server space and wastes e-mail recipient's time.

Spam can be combated in a number of ways. The most common is to block the IP address of the spam source. However, if that source is a common e-mail relay or belongs to an organization that you do business with, this option is not viable. Another approach is to do a reverse domain name lookup on incoming IP connections and to block if a name is not returned.

More sophisticated approaches can be made by inspecting the header to see if the e-mail comes from any known spam source. Further controls can be implemented by using intelligent text analysis to screen out phrases like 'get rich quick'. Another way to combat spam is to subscribe to a Spam blacklist. This is usually via the Internet, and gives companies access to spam word lists, which are continuously updated. You may also want to intercept all spam, or only allow between certain user groups or individuals.

Some examples of detecting Spam within text analysis could be:

- 'If you wish to be deleted from our mailing list'
- 'reply within 3 days for your free gift'
- 'guaranteed return on investment'
- 'get rich quick'
- '100% commission'

Use the table below to note the spam words or phrases your company needs to be able to search for within e-mail:

Text	User	Inbound E-mail Management		Outbound E-mail Management	
____________ ____________ ____________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________ ____________ ____________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________ ____________ ____________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________ ____________ ____________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________ ____________ ____________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party

6. Spoof

E-mail spoofing is the way a sender or originator of an e-mail can take on someone else's e-mail identity without their knowledge or consent, thereby opening up the organization to major breaches of privacy or confidentiality.

There are a number of tell tale signs of spoof, and these can be taken together to produce an 'index' of likely spoof. The challenge for Content Security systems is to be able to identify and intelligently analyze the telltale signs of spoofing, through host lookups and sender validation.

Action	Apply to
Notify of spoof?	❑ Inbound e-mail ❑ Outbound e-mail ❑ All e-mail
Lookup connecting SMTP hosts in the DNS	❑ Inbound e-mail ❑ Outbound e-mail ❑ All e-mail
Lookup connecting hosts in the RBL	❑ Inbound e-mail ❑ Outbound e-mail ❑ All e-mail
Validate sender address in the DNS	❑ Inbound e-mail ❑ Outbound e-mail ❑ All e-mail

7. Portable Code - JavaScript, Shortcuts and Automatic Mail-to's

JavaScript, shortcuts and automatic Mail-to's can raise Content Security issues, such as having more access than perhaps the user intended, or being able to make unauthorized removal of data from the user's system. Therefore a Content Security solution needs to give a company the ability to manage the detection and removal of these threats, and also have the option of being able to add a text disclaimer to inform the recipient of the removal.

Once you have decided on whether to detect Portable Code in e-mail, you can then determine how to deal with such messages.

Use the table below to specify how you need your Content Security solution to manage these types of threats.

Type	User	Inbound E-mail Management of cleanable viruses		Outbound E-mail Management of cleanable viruses	
____________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
____________	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party

8. Size Management

The ability to manage e-mail based on size can be critical. If too many large e-mails are sent through the server, this could result in your network being exposed to a variety of performance problems that can send user productivity spiraling downwards. Therefore, any Content Security solution needs the ability to manage e-mail based on size, and also the time at which it was sent or received.

In addition, the most flexible Content Security solution will allow users to define a smaller and larger size threshold. The smaller threshold could be used to 'park' e-mail, and the larger threshold to block or delete over sized e-mail. 'Parking' allows e-mail to be held on the host until such pre-determined time when it is automatically released. The added ability of enabling thresholds on a time basis would allow any size file to be managed at the weekend or outside working hours.

Use the table below to specify how you need your Content Security solution to manage e-mail by size.

Threshold	User	Inbound E-mail Management of cleanable viruses		Outbound E-mail Management of cleanable viruses	
_____Kb	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
_____Kb	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party

9. Number of Attachments

The detection of e-mail based on the number of attachments that it has can protect a company from network congestion and reduced productivity. E-mails with a quantity of attachments are usually large in nature and need to be managed to avoid the depletion of network resources.

Once you have decided whether to detect a certain number of attachments, you can then determine how to deal with such messages.

Use the table below to specify how you need your Content Security solution to manage e-mail attachments.

Quantity	User	Inbound E-mail Management of cleanable viruses		Outbound E-mail Management of cleanable viruses	
_____	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party
_____	❑ All ❑ By Department ❑ By Individual	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party	❑ Deliver ❑ Quarantine ❑ Forward ❑ Archive ❑ Reply to sender	❑ Delete ❑ Park ❑ Send alert ❑ Write event to log ❑ Forward to 3rd party

PART TWO: Establishing your Web Policy

1. Detection of Web transfer by type

This is the ability to control the upload and download of files to and from the Internet. The file type needs to be determinable by the file pattern and not its extension, so as to stop disguised files bypassing policy. This feature would allow for recognition of all files of a certain type and a certain size.

a) File Type: Images

Once you have decided whether to detect images, you can then determine how to deal with them. Use the table below to determine this area of your Web policy.

The types of image files you should consider are JPEG, DXF, DWG, PSP, PNG, PIC, TIFF, PCX, FLI, BMP and GIF. You may also want to intercept all files, or only allow specified user groups or individuals to upload or download.

Type	*Web Site*	*Size*	*User*	*Upload Management*	*Download Management*
______________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
______________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
______________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
______________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event

b) File Type: Video

Video files are normally large in size. Downloading and uploading of video files could lead to resource depletion.

The types of video files you should consider are RM, MPEG, QTM and AVI. You may also want to intercept all files, or only allow specified user groups or individuals to upload or download.

Type	*Web Site*	*Size*	*User*	*Upload Management*	*Download Management*
______________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
______________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
______________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
______________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event

c) File Type: Container and Compression formats

To ensure compressed files are threat free, Web Content Security tools need to be able to perform recursive analysis - i.e. repeatedly 'unwrap' files – to check the compressed data in its raw state.

The types of container and compression formats you should consider are PGP, BINHEX, RAR, TNEF, UUE, LZH, ARJ, CAB, CMP, ZIP, GZIP, and TAR. You may also want to intercept all files, or only allow specified user groups or individuals to upload or download.

Once you have decided whether to detect container and compressed files, you can then determine how to deal with them. Use the table below to determine this area of your Web policy.

Type	Web Site	Size	User	Upload Management	Download Management
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event

d) Type: Executable files

Executables can be large, and may not be work related. They are also one of the primary sources for virus propagation, so you need to ensure that your Content Security solution can check for these types of files. Users downloading unauthorized executable files may cause instability problems on the network and may expose and organization to issues of legal liability if the software is unlicensed.

The types of executable files you should consider are JavaByte, DosExe, Win31Exe, Win32unknown, Win32DLL and Win32exe. You may also want to intercept all files, or only allow specified user groups or individuals to upload or download.

Once you have decided whether to detect executable files, you can then determine how to deal with them. Use the table below to determine this area of your Web policy.

Type	Web Site	Size	User	Upload Management	Download Management
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event

e) Type: Document files

Document files can be downloaded from or uploaded to the Internet. Macros in document files can be a source of virus infection and uploaded documents may contain company confidential information.

The types of document files you should consider are FAX, rich text, CDA, Microsoft Project, Microsoft PowerPoint, Microsoft Word, Microsoft Excel, OLE Package, 1-2-3, Acrobat (PDF), Text and HTML. You may also want to intercept all files, or only allow specified user groups or individuals to upload or download.

Once you have decided whether to detect document files, you can then determine how to deal with them. Use the table below to determine this area of your Web policy.

Type	Web Site	Size	User	Upload Management	Download Management
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event

f) Type: Sound files

There are many sources of digital music and sound files on the Web and this has led to many people downloading these large files. This can deplete system resource and potentially expose an organization to issues of legal liability if the sound files are illegal copies of copyright material.

The types of sound files you should consider are MIDI, AIF, VOC, AU, WAV and MP3. You may also want to intercept all files, or only allow specified user groups or individuals to upload or download.

Once you have decided whether to detect sound files, you can then determine how to deal with them. Use the table below to determine this area of your Web policy.

Type	Web Site	Size	User	Upload Management	Download Management
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event
________	❑ All Web Sites ❑ Specific URLs	❑ Over _____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Send alert ❑ Deny ❑ Log event	❑ Allow ❑ Send alert ❑ Deny ❑ Log event

g) Type: Files by byte pattern

As new or specialized files types emerge it is important that your Web Content Security solution can be taught how to recognize these new file signatures (byte patterns). You may also want to intercept all files, or only allow specified user groups or individuals to upload or download.

Once you have decided if there are files with particular byte patterns that you wish to manage, you can then determine how to deal with them. Use the table below to determine this area of your Web policy.

Byte Pattern	Web Site	Size	Download		Upload	
			User	Management	User	Management
__________ __________	❑ All Web Sites ❑ Specific URLs	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event
__________ __________	❑ All Web Sites ❑ Specific URLs	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event
__________ __________	❑ All Web Sites ❑ Specific URLs	❑ Over ____Kb ❑ All	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event

h) Files by: name

In addition to being able to manage files by type, there may be certain files with known names that should not be uploaded to or downloaded from the Web. For example, company confidential data, or files with animations that often proliferate at certain times of the year. You may also want to intercept all files, or only allow specified user groups or individuals to upload or download.

Once you have decided on particular named files that you wish to manage, you can then determine how to deal with them. Use the table below to determine this area of your Web policy.

Filename	Web Site	Download		Upload	
		User	Management	User	Management
____________________ ____________________	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event
____________________ ____________________	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event
____________________ ____________________	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event

2. Web Based E-mail

Web-based e-mail services like HotMail and Yahoo! allow e-mail usage that bypasses SMTP security at the gateway. It can therefore be used for non-work-related e-mail, or more significantly to send out confidential information undetected.

Use the table below to specify how your Content Security solution should manage Web-based e-mail.

User	*Management of Web e-mail*
❑ All ❑ By Department ❑ By Individual	❑ Deny ❑ Send alert ❑ Log event

3. Virus Scanning

The ability to scan for viruses is an important tool within a Content Security solution. The best solution would allow the use of one or more user-selectable virus tools to check Web transfers for viruses and Trojans. It is also wise to choose a solution that can detect behavior patterns of threats, ensuring better detection. Use the table below to determine how, and with which tools, you want to manage the virus scanning of Web transfers.

Downloads			
Anti-virus Tools	**User**	**Clean ?**	**Management**
_____	❑ All ❑ By Department ❑ By Individual	❑ Yes ❑ No	❑ Allow ❑ Deny ❑ Send alert ❑ Log event
_____	❑ All ❑ By Department ❑ By Individual	❑ Yes ❑ No	❑ Allow ❑ Deny ❑ Send alert ❑ Log event

Uploads			
Anti-virus Tools	**User**	**Clean ?**	**Management**
_____	❑ All ❑ By Department ❑ By Individual	❑ Yes ❑ No	❑ Allow ❑ Deny ❑ Send alert ❑ Log event
_____	❑ All ❑ By Department ❑ By Individual	❑ Yes ❑ No	❑ Allow ❑ Deny ❑ Send alert ❑ Log event

4. Text Analysis

The ability to analyze Web data streams for pre-defined key words and phrases enables organizations to accurately determine the contents of Web pages, documents or other transfers, and detect any undesirable content.

In addition, it is useful to be able to define complex search algorithms to detect content, such as the concept of 'Nearness' the use of Boolean operators. An example search phrase could be to search for the word "Company" NEAR "Confidential" in Web uploads, only allowing the upload if the words are separated by more than 5 words.

Some examples of text analysis could be:

- over 18's only
- Search for the word "black". Disallow if the word "man" is next to it
- Stop documents being uploaded if they contain the word "Not for external disclosure"

You may also want to intercept all phrases or only allow between specified user groups or individuals.

Byte Pattern	Web Site	Download		Upload	
		User	Management	User	Management
________________ ________________	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event
________________ ________________	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event
________________ ________________	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event

5. Portable Code and HTML

Code transferred during Web surfing may be malicious and able to make unauthorized removal of data from the user's system. Therefore a Content Security solution needs to give a company the ability to manage the detection and removal of these threats.

The types of code you should consider are JavaScript, VBScript, ActiveX, Java Programs, Shortcuts, Automatic Mailto's and Cookies. You may also want to intercept all code or only allow specified user groups or individuals to download.

Use the table below to specify how you need your Content Security solution to manage these types of threats.

Download					
Type	Web site Detection	Detect?	Management	Remove	Management
________________	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event
________________	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event
________________	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny ❑ Send alert ❑ Log event

6. Authenticode

Companies that publish files on the Internet for download can use Authenticode technology to digitally sign their data. Users can use the certificate to decide whether or not they trust the publisher for this and subsequent downloads.

Use the table below to specify how you need your Content Security solution to manage these types of Authenticode signed files.

Type	Web Site	User	Download Management	
Files that have an invalid signature	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny	❑ Send alert ❑ Log event
Trusted certificates that are not yet active or are expired	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny	❑ Send alert ❑ Log event
Certificates that are not trusted	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny	❑ Send alert ❑ Log event
Files that have no certificate	❑ All Web Sites ❑ Specific URLs	❑ All ❑ By Department ❑ By Individual	❑ Allow ❑ Deny	❑ Send alert ❑ Log event

7. Manage Web Browsing by Content and Time of Day

The ability to manage Web usage by URL, PICs rating and by analyzing the data stream for pre-defined key words and phrases, enables organizations to accurately determine the contents of Web transfers. Additionally you may want to restrict access to certain Web content during normal working hours but allow access at other times.

Use the table below to specify what type of content you wish to manage and whether this is managed on a 'time of day' basis.

Text/URL/PICs	User	Time of Day	Download Management	
____________ ____________	❑ All ❑ By Department ❑ By Individual	____________	❑ Allow ❑ Deny	❑ Send alert ❑ Log event
____________ ____________	❑ All ❑ By Department ❑ By Individual	____________	❑ Allow ❑ Deny	❑ Send alert ❑ Log event
____________ ____________	❑ All ❑ By Department ❑ By Individual	____________	❑ Allow ❑ Deny	❑ Send alert ❑ Log event
____________ ____________	❑ All ❑ By Department ❑ By Individual	____________	❑ Allow ❑ Deny	❑ Send alert ❑ Log event
____________ ____________	❑ All ❑ By Department ❑ By Individual	____________	❑ Allow ❑ Deny	❑ Send alert ❑ Log event

8. Managing Web usage from your existing user lists

Although the Web is a valuable business tool and provides access to a great resource of information, it is likely that there are groups of users and individuals who do not need or should not have Web access.

Use the table below to specify who should/should not have Web access.

Group/User	Management
_____	❑ via LDAP ❑ via NT ❑ via Text

9. Providing Exceptions to the Rule

You may decide that not all users should access to browse the Web, but that it may be necessary for them to access certain sites as part of their job. For example, accounts may be barred from using the Web, but they may need access to a particular money site, for example a stock exchange site. Therefore you may wish to allow them viewing to that particular site and provide Content Security checks.

Web Site Address	Exceptional Access Allowed
_____	❑ All ❑ By Department ❑ By Individual
_____	❑ All ❑ By Department ❑ By Individual
_____	❑ All ❑ By Department ❑ By Individual

Part Three: Maintaining a Content Security Policy

You have your Content Security policy written. You've selected the most appropriate Content Security solution. You've educated your employees. So now you can sit back and relax – right?

WRONG! Policy is only as good as its last revision. So, when did you last update your policy, and re-educate your employees?

Once a Content Security policy has been implemented, the key to its success is maintenance. This section of the guide is designed to help you maintain your corporate policy more effectively, and combat the potential Content Security risks posed by the Internet to your business.

1. Introduce a 'Security Awareness' culture into your offices

- Regularly review your policy
- Get Senior Management to endorse changes to your policy and advertise this endorsement
- Regularly communicate the policy. For example produce a simple Policy Booklet to highlight acceptable and unacceptable e-mail, web and encryption usage; send e-mails to remind employees of the policy; produce posters to display around your premises
- Make the Policy part of a legally binding agreement between an employee and the company, for example, create an Employee Acknowledgement Agreement
- Train your employees on the policy regularly, and allow for questions and feedback from them
- Overall, make your Security statements clear, timely and achievable

2. Regularly review sources of unwanted material

There are many web sites that aim to help companies keep abreast of the newest threats in viruses, spamming techniques and less-than-desirable web sites.

- If stopping spam is part of your policy:
  - maintain your spam list by subscribing to a spam blacklist site, so you are automatically notified of new threats. There are organizations that offer a real-time service listing spam-hosts, for example VIX, IMRSS and ORBS.
  - maintain your list of commonly used spam phrases, for example include 'free', 'reply within 30 days' and '100% guaranteed' in your text analysis of e-mail.
- If verifying the source of e-mails is part of your policy:
  - ensure your software can perform reverse address look-ups. RFC2505 'Anti-spam Recommendations for SMTP MTAs' recommends that products should be able to verify the source of the e-mail address, to check its validity

3. Be proactive and stop anti-social behaviour

Take time to analyze Web and e-mail activity – it could be violating your organizations Content Security policy, leaving you open to key business security risks and corporate liability.

- Adjust and maintain your Policy regularly, and remember that new Content Security threats are appearing all the time
- If certain file types, attachments or certain supplier's e-mails are causing problems, then amend your Policy and Content Security software to deal with them, and ensure this is communicated back to the source of the e-mail, and to your employees
- If your Policy states that employees cannot send or receive non-business related e-mails, or view non-work related Web sites, then ensure your Policy is up-to-date and communicated, and that your Content Security software can stop the activity

4. Be prepared

Every month sees a wave of e-mail jokes, pranks and viruses, and hundreds of new sites added to the Web. Consequently, you can expect to continue to see a deluge of spam attacks, viruses, e-mail with hidden and destructive payloads and disguised e-mails siphoning confidential information from your network. If your Policy includes stopping these types of attack, then:

- Ensure your Content Security software is up-to-date, and your policy scenarios include potential threats. Example key words might include:
  - 'If you wish to be deleted from our mailing list'
  - 'reply within 3 days for your free gift'
  - 'guaranteed return on investment'
  - 'get rich quick'
  - '100% commission'
- Be covered for new Content Security threats by ensuring you regularly update your Content Security solution

5. Maintain your Content Security Solution

- Make sure you have installed the most appropriate Content Security solution to manage threats according to your Policy
- Ensure you have the latest release of your Content Security software

6. Maintain your Lists

- Make sure you promptly delete the user rights of personnel who have left the company
- Ensure you regularly review the user rights for individuals, groups and departments
- Ensure you maintain your Key Revocation lists

7. Review e-mail disclaimers

If your Policy includes having an e-mail disclaimer, then:

- Ensure it is up-to-date
- Check and maintain individual and department disclaimers
- Regularly review the disclaimer(s) with your legal advisors to ensure you are maximizing the protection of the company and its employees

8. Update your Risk Analysis regularly

- Regularly analyze areas of your business which require differing levels of information security controls, and adjust your Policy accordingly
- Identify which areas are most vulnerable, and take the necessary action

9. Be a Good Internet Citizen

Of course, your Policy should apply to your outgoing, as well as your incoming communications, so check that internally you:

- Can check outgoing e-mail against your spam detectors
- Don't relay data to external sites (anti-relay)
- Inform virus senders of their problem
- Scan all e-mail and Web activity for Content Security threats

Conclusion

For organizations the challenge remains: how to harness the potential of the Internet without compromising security. As Internet usage has evolved, so have the available security technologies. The MIMEsweeper family of products is deployed in over 6,000 organizations world-wide to help provide that security.

Whether the priorities for an individual enterprise lie in protecting information, maximizing its operational effectiveness, minimizing its corporate liability or guarding against damage to its market image and presence, each organization requires a comprehensive business security policy. Business security demands inclusion of Content Security.

If you would like to know more about the MIMEsweeper family of products, contact your nearest office listed on the back of this guide. Alternatively, visit our web site at www.mimesweeper.com, or contact your local MIMEsweeper reseller.

MIMEsweeper™

Europe

United Kingdom
1310 Waterside, Arlington
Business Park
Theale
Reading
Berkshire, RG7 4SA
UNITED KINGDOM
Tel: +44 118 903 8000
Fax: +44 118 903 9000

Contact MIMEsweeper:
info@mimesweeper.com

Germany
Amsinckstrasse 67
Poseidonhaus
Hamburg, 20097
GERMANY
Tel: +49 402 399 90
Fax: +49 402 399 9100

Contact MIMEsweeper:
info.de@mimesweeper.com

America

USA
15500 SE 30th Place
Suite 200
Bellevue
Washington, 98007
UNITED STATES
Tel: +1 425 460 6000
Fax: + 1 425 460 6185

Contact MIMEsweeper:
info@us.mimesweeper.com

Asia Pacific & Japan

AUSTRALIA
Level 4, Building C
CityWest Office Park
33 Saunders Street
Pyrmont
New South Wales 2009
AUSTRALIA
Tel: +61 2 8514 7300
Fax: +61 2 8514 7301

Contact MIMEsweeper:
info@mimesweeper.com.au

JAPAN
New Otani Garden Court 8F
4-1, Kioichi-cho
Chiyoda-ku
Tokyo-to, 102-0094
JAPAN
Tel: +81 3 5212 3772
Fax: +81 3 5212 3788

Contact MIMEsweeper:
info@mimesweeper.co.jp

www.mimesweeper.com