101 Ways to Use Message Logic for email archiving, compliance and analytics

Data Storage Corporation
Excellence in Data Protection and Recovery

Message Logic is a business unit of
Data Storage Corporation. 212-564-4922
www.messagelogic.net or www.datastoragecorp.com

Message Logic makes it fast and easy to respond to discovery requests, meet compliance obligations, conduct internal investigations, and manage email policy. It archives every message without changing the original message and makes them easy to find for discovery and compliance. It can even send real-time email notifications to the original sender or management when an event takes place.

With its easy web browser interface, Message Logic helps you meet the needs of the new Federal Rules of Civil Procedure, Sarbanes-Oxley, HIPAA, harassment and privacy laws with minimal IT effort.

1. Archive all email messages-inbound, outbound, internal, external, and attachments.
2. Archive unaltered messages with their original format and metadata in tact, as required by the Federal Rules of Civil Procedure.
3. Easily retrieve any message and attachment, even if the user deleted or altered it.
4. Send an email notification to the original sender or to management when something critical takes place.
5. Retrieve messages and create policy management alarms using one of Message Logic's 70 predefined categories, key words, Boolean expressions, and more with a web browser.
6. Adhere to the new amendments to the Federal Rules of Civil Procedure.
7. Retrieve email, even if the end user deletes it from the email server.
8. Retrieve all email-inbound, outbound, internal, external (and all attachments), including desktop, web-based, and BlackBerry messages sent/ received via the corporate server.
9. Retrieve the original text of email including all original metadata (headers, etc.) — even if it was changed on the server after it was sent.
10. Retrieve the original text of inbound email, even if it was altered by the recipient.
11. Place an email on litigation hold simply by viewing it
12. Retrieve all communications between specific employees and specific clients.
13. Maintain duplicate copies of emails, separate from the original, with a cryptographic key to assure the integrity of the archive copy.
14. Retrieve all messages to/from specific addresses, even if one of them was in a BCC.15.
15. Retrieve all messages to/from specific domains, even if the domain was only in a BCC.
16. Identify the employees who most frequently send potentially harassing email
17. Identify the specific messages that rank highest by offensiveness score.
18. Retrieve potentially harassing emails sent by a person about whom a complaint was received. (The search can be limited to only those identified as offensive and/or only those sent to particular people.)
19. Monitor employees AFTER that employee was given a final warning. (HR can receive an email if the monitored employee sends another offensive mail.)
20. Monitor a "heartbeat" of potentially offensive email to identify unusual activity, such as a sudden increase in offensive messages that might indicate that a joke forwarded to many people.
21. Monitor a "heartbeat" of multimedia attachments in order to identify unusual activity, such as a sudden increase in attachments that might indicate an inappropriate video
22. Monitor email between selected employees.
23. Investigate specific types of offensive content, such as ethnic slurs and sexual innuendo.
24. Find the first person to send or receive an offensive joke or other potentially harassing email that was forwarded around your company.
25. Find external sources (domains) of potentially harassing emails.
26. Meet state privacy/identity theft legal requirements by immediately sending an email notification when an email that could lead to identity theft is sent (e.g., messages that contain both the name and the matching social security, credit card, or driver's license number of any person.).

27. Notify compliance officers when any information contained on a list of confidential data is sent or received.
28. Notify officials when messages containing specific names from a list, such as names of students or family members of employees, are sent to an external domain.
29. Identify messages containing a Social Security Number.
30. Identify messages containing a Canadian Social Insurance Number.
31. Identify messages containing a Credit Card Number.
32. Identify messages containing a Driver's License Number
33. Identify messages containing a U.S. or Canadian Telephone Number.
34. Identify messages containing specific numbers (such as the home phone numbers of executives or the Board of Directors).
35. Identify messages containing a company account number (may require custom configuration of account formats).
36. Identify all messages sent to a competitor's domain and who sent them.
37. Identify the top domains where confidential information is being sent.
38. Identify the senders of messages containing the name of a confidential project.
39. Send an alert when a message that contains confi- dential information, such as the code name of a secret project, is sent to an external email address
40. Identify specific groups or departments to an external domain or to specific unapproved domains.
41. Identify messages containing a specific word, phrase, or financial amount.
42. Identify messages with a specific document attached.
43. Identify messages with specific document types attached, such as spreadsheets or presentations.
44. Notify executives when messages containing specific names from a list, such as customer lists, are sent to an external domain.
45. Identify the employees who send the most non-business email.
46. Identify the employees who receive the most non-business email.
47. Identify messages sent to or received from known non-business sites, such as dating and sports sites.
48. Identify the most frequent senders of multimedia files.
49. Identify which external domains most frequently receive emails (such as Hotmail) and who is sending messages to those domains.
50. Identify messages with many attachments.
51. Identify messages with extremely large files.
52. Identify huge messages containing multimedia files (often huge videos).
53. Identify messages with many recipients, such as on mailing lists.
54. Monitor a "heartbeat" of non-business email to identify unusual activity, such as a sudden increase in messages that might indicate that a productivity waster forwarded to many people.
55. Identify messages to/from key corporate officers.
56. Identify messages to/from the Board of Directors.
57. Identify messages to/from your accounting firm's domain.
58. Find all emails to or from a specific consultant.
59. Identify messages to/from top customer domains.
60. Identify messages to/from top vendor domains.
61. Identify messages to/from top investors.
62. Identify messages containing specific financial figures, including the ability to limit the search to those sent and received during the quiet period.
63. Identify messages containing the names of key confidential projects.
64. Identify messages containing key attachments by name or type, or containing key words or phrases in the attachments.

65. Retrieve messages by attachment name or attachment type.
66. Retrieve messages by size or attachment size.
67. Retrieve messages by MIME type.
68. Retrieve messages with many attachments.
69. Retrieve messages without any apparent business purpose (personal mail)
70. Find most frequent senders of personal mail.
71. Identify messages that contain employment information, such as resumes, are being sent to an external source. (Helps identify talent raids in the works.)
72. Identify the top external domains receiving employment information from employees.
73. Identify the top external domains sending job descriptions and employment information to employees.
74. Notify HR when messages containing specific names from a list, such as employee telephone lists, are sent to an external domain.
75. Find all email sent from a restricted group.
76. Find all email received by a restricted group
77. Find all emails from a specific group of employees to any external domain or to a specific domain.
78. Notify compliance officers when prohibited communication between specific groups of restricted individuals takes place.
79. Monitor specific file names to see if these files are sent as attachments
80. Find prohibited communications between members of selected groups (e.g., between the sales group and the research group).
81. Maintain duplicate copies of emails, separate from the original, with a cryptographic key to assure the integrity of the off-line archive copy
82. Institute supervision using random sampling of messages (i.e., NASD 3010).
83. Identify non-public information (see PRIVACY) as well as messages containing messages containing particular account number formats. (i.e., Gramm- Leach-Bliley requirements).
84. Find all emails to/from a particular client.
85. Find all emails to/from specific employees, such as brokers.
86. Retrieve all conversations between specific employees and specific clients.
87. Find emails that reference a particular stock, symbol, or CUSIP number.
88. Find emails with key words or financial figures in the message or attachment that trigger a concern.
89. Find all emails with attachments, specific attachments, or specific attachment types (e.g., spreadsheets, PDF files, etc.).
90. Messages that contain medical terminology.
91. Messages that contain medical terminology and PHI (personal health information) with individually identifiable information.
92. Identify any message sent to any external domain that contains the name of a student or any confidential information about a student (as identified on a list of confidential information).
93. Identify any message sent from or to specific internal groups contain information about a particular student (such as messages sent to a teacher with a student's name and with medical terminology).
94. Identify any message sent to any external domain that contains the name of any employee with any confidential information about that employee (as identified on a list of confidential information).
95. Retrieve messages by keyword or phrase in the message or attachment.
96. Retrieve messages using complex Boolean logic (i.e., contains "A" or "B", but not "C").
97. Retrieve messages from specific individuals.
98. Retrieve messages from specific domains.
99. Retrieve messages to specific email addresses, even if contained in a BCC.
100. Retrieve messages to specific domains, even if contained in a BCC.
101. Retrieve messages containing a specific IP addresses.