

Enforcing Corporate Compliance Policies In Your Lotus Notes® Email



1018 Western Avenue
Pittsburgh, PA 15233
www.businessrecords.com
PH: 412-321-0600
FX: 412-321-5152
Toll Free: 877-342-5276
Email: brmsales@businessrecords.com

Table of Contents

Introduction	1.0
Regulatory Compliance: One of Today's Top Business Drivers	1.1
Purpose and Overview	1.2
Ensuring Email is Compliant	2.0
Why It's Necessary to Enforce Compliance in Email	2.1
Responsibility of Ensuring Email Compliance Lies with IT Administrator	2.2
What Organizations Need to Ensure Email Compliance	2.3
Mail Attender for Notes	3.0
Taking Email Administration to the Next Level	3.1
Email Compliance: Addressing the Requirements of Corporate Policies	3.2
Empowering Organizations to Attain the Upper Hand with Email Management	3.3
Summary	4.0
Appendix A	5.0
Technical Specifications for Mail Attender for Notes	5.1

1.0 Introduction

1.1 Regulatory Compliance: One of Today's Top Business Drivers

Compliance has become the corporate buzzword of the current decade and a concern that is deeply engrained in the corporate consciousness. Organizations in many industries are undergoing sweeping changes due to increased governmental regulations that have a dramatic impact on business processes as well as IT infrastructure. The importance of regulatory compliance has become a critical boardroom issue, as companies that don't comply risk legal action as well as stiff government fines and restrictions.

Over the past several years, numerous laws have been enacted requiring most organizations to implement a compliance strategy. The three most critical laws are:

Sarbanes-Oxley Act (SOX) – Created in response to the accounting scandals that occurred at major corporations in 2001 and 2002, SOX requires that publicly-traded companies ensure their internal business processes are under control. This includes certifying the accuracy of financial statements by an outside auditor as well as conducting an annual assessment of internal controls relating to the security of critical data, particularly financial information.

Health Insurance Portability and Accountability Act (HIPAA) – Requires that health institutions take steps to limit the disclosure of an individual's personal health information, ensuring the privacy and security of that information as it is collected, processed and transmitted to other health organizations.

Gramm-Leach-Bliley Act (GLB) – Requires that financial institutions (and persons that receive protected information from financial institutions) adopt strict measures for protecting the privacy and security of customer data.

These regulations and others, such as SEC Rule 17a-3/17a-4 and the Electronic Signatures Act, require that applicable organizations install controls to prevent unauthorized access to critical information, protect the integrity of private records, and avert the transmittal of sensitive corporate, financial, patient or customer information. As a result, an organization's IT systems must be carefully scrutinized and a compliance architecture must be erected for tracking and controlling the use and storage of specific data and reports.

A mission-critical application in organizations that necessitates close monitoring to ensure compliance is email. While the first consideration for organizations implementing a compliance strategy may be preventing unauthorized access to important information and protecting databases and certain areas of their intranet, they need to also take a close look at language, information, files, and records that are being communicated both within and outside the organization. Certainly, examining every email is not an option, but solutions do exist for organizations to set parameters on email content — identifying specific words, pieces of information, and attachments that an email cannot contain.

1.2 Purpose and Overview

This paper is a discussion on an enterprise-wide activity that should be addressed in developing and implementing your corporate compliance strategy. Ensuring that the content of email transmitted across and outside of your organization is compliant is a critical necessity. Sometimes overlooked, emails exchanged by employees internally and externally can contain inappropriate language or corporate data and file attachments that are sensitive, proprietary or confidential, and in violation of governmental regulations.

Systems for monitoring and restricting email content need to be installed to protect data and files that fall under the authority of governmental regulations, but also to insure against legal action resulting from an employee's inappropriate or damaging email communication. As with other areas of your enterprise requiring compliance procedures, the responsibility of ensuring email compliance is placed on the corporate security officer and IT management. To execute email compliance, IT administrators need a solution that enables them to manage email creation, email content, attachments used, and end-user email activity in general.

Email management solutions exist that will assist your IT department in performing and simplifying the process of email compliance, and ensure your organization narrows the risk of being non-compliant via its email transmissions. One important aspect to consider when selecting such a solution is its flexibility. The right solution should allow IT administrators to determine rules and place restrictions according to the governmental regulations that influence your organization and what you've established as your corporate security policies.

Your email management solution should also enforce compliance by allowing IT to establish rules and restrictions as granularly as necessary, and to specify groups of employees to be impacted by those rules. Most importantly of all, the email management system you install in your organization should provide comprehensive capabilities, allowing you to address all aspects of compliance to which your organization needs to adhere.

2.0 Ensuring Email is Compliant

2.1 Why It's Necessary to Enforce Compliance in Email

Because of regulatory requirements for retention of critical data and corporate governance, organizations have been compelled to develop and implement corporate compliance policies. For many organizations, these policies have in effect evolved into more than a senior-level reaction to compliance mandates. Corporate compliance may encompass the behavior of all employees, not just the CEO and CFO, as prescribed by SOX regulations.

In addition, issues have emerged from other areas that fall under the compliance umbrella: the IT security department's concerns related to maintaining security of corporate data, and the human resources and legal departments' need to monitor the use of offensive and inappropriate language and sensitive or restricted information in employee's internal and external communications. Since an email message sent by an employee using your domain name is like a letter sent on your official letterhead, human resources has the responsibility to ensure employee email actions are appropriate.

The concerns of legal are even more valid when you consider two critical factors:

1. The Supreme Court's decision that a company is responsible for the content of an employee's email; and
2. The degree to which electronic communications are increasingly being used as legal evidence in cases of sexual harassment and corporate fraud or malfeasance.

As a result, organizations want the power to protect themselves and have more control over email messages.

Mainly as a consequence of regulatory compliance, but also due to legal implications and employee conduct matters, your organization needs to be equipped to manage email risks. To satisfy regulatory requirements for data retention and security, you must have the ability to locate critical data, protect its authenticity, and keep it in a secure location where it can be maintained for long-term use. For legal requirements, employee conduct measures and internal security, you want a system for protecting the transfer of sensitive and confidential information, monitoring the

language used in email messages, placing restrictions on attachments, and managing email activity.

2.2 Responsibility of Ensuring Email Compliance Lies with IT Administrator

As an enterprise application and form of electronic communications, email administration falls under the responsibility of an organization's IT department. As your senior management develops and prepares to implement its corporate compliance strategies, IT will be called on to ensure the successful execution of all information security mandates. These mandates should involve email communications as much as network access control, authentication processes, and identity management.

Because of the constancy of email — thousands are incoming, outgoing and circulated across the enterprise everyday — managing it is a complex task. Email management systems exist that will allow organizations to archive emails and attachments based on multiple criteria, reclaim storage space, and produce reports, however, IT administrators need an automated system that will allow them to track specific aspects of emails. To ensure email compliance, administrators need to establish controls as well as monitor emails being composed and delivered in their organization.

2.3 What Organizations Need to Ensure Email Compliance

The email communications an organization's employees compose, send or forward either internally or externally need to be in line with corporate compliance policies, which may encompass compliance with one or more governmental regulations as well as management-established guidelines for employee conduct. As a result, organizations need a solution that will ensure email compliance by enabling IT administrators to manage all the various aspects of email composition and delivery.

It's important that an organization's email management system include certain capabilities that will guarantee email compliance:

1. Email creation management – Control over whether new messages composed by employees are sent.
2. Email content management – Specifying key words and phrases that will preclude an email from being sent if it contains any of the specified key words/phrases.
3. Email document management – Overseeing where emails are located and how long they are retained in the system.
4. Email attachment management – Handling actions taken based on attachment size, age, and type and document size and age.
5. End-users' email activity management – Identifying specific parameters for changing or deleting emails through the use of rule setting.

3.0 Mail Attender for Notes

3.1 Taking Email Administration to the Next Level

Achieving compliance with governmental regulations has created another issue that needs to be addressed via email management. Originally developed to handle the volume of emails produced within an organization and its impact on infrastructure, email management solutions primarily provide email archiving and server space reclamation capabilities. Because of legal implications, email management has also come to include document (email) retention and attachment retention capabilities which protect critical data and affect how email is used by employees.

Mail Attender for Notes is a Lotus Notes email administration product that allows administrators to control content, properties and activity within email databases. Mail Attender automatically archives emails and/or attachments to separate data stores based upon multiple criteria (such as

age, date/date range, message/attachment size, keywords/phrases, and sender/receiver). It also provides the ability to create and enforce automated rules or restrictions for managing several email components.

Through Mail Restrictions, the rules which are created by the Lotus Notes administrators, Mail Attender enables the management of email databases in several ways. Mail Attender can also be used to perform many different tasks, such as enforcement of document (email) retention and attachment retention policies. As a result, Mail Attender prevents overload to the email infrastructure and restricts employees from email actions that would be detrimental to the organization.

Mail Attender contains 14 different types of Mail Restrictions, which can be used to affect automatic processing of ACL (access control lists), activity (by end-user), address books (local), attachments, creation (new messages), documents, folders, full-text indexes, Out-of-Office, personal agents, preferences, properties, quotas and replication entry.

Each Mail Restriction can be configured based on the parameters required by the organization. A Mail Restriction can apply to all servers and end-users or a sub-set of servers/end-users. The subset of servers/end-users can be based upon groups (identified in address book), OU structures or explicit server/end-user names. Exclusion or inclusion lists can be created for identifying specific names. A Mail Restriction can be as granular as an organization wants it to be.

3.2 Email Compliance: Addressing the Requirements of Corporate Policies

Mail Attender can ensure that your email communications comply with all governmental regulations that impact your organization as well as any corporate compliance policies established by upper management. Mail Attender's compliance features can be found in four of its 14 types of Mail Restrictions — Activity, Attachment, Creation, and Document — all of which address the various email components that could impact an organization's ability to be compliant.

Activity Restrictions

This type of restriction will prevent an employee from deleting or editing documents in their email files. It is used to maintain the integrity of sensitive or confidential information or evidence and protect documents (emails) matching specific criteria. For example, an activity restriction can be placed on documents containing particular words in the content, or documents that are no older than a specified number of days.

Administrators can prevent users from deleting or editing using one of five criteria:

1. Content – specifying key words or phrases.
2. Correspondents – selecting a list of people who are either in the “From,” “Send To,” “Copy To,” or “Blind Copy To” fields.
3. Date – selecting a start and end date.
4. Retention – entering the retention amount and method (older/younger).
5. Subject – identifying a complete or partial subject line.

Attachment Archiving and Restrictions

The Attachment configurations allow administrators to locate attachments using four different methods (see below). This type of restriction is most useful for reclaiming server space and reducing legal liability.

Once an attachment has been located, one of five actions can be taken: Archive, Report, Collect, Copy, Delete, or Delete Document. For example, an attachment with a specific extension can be designated for archiving from the document after the employee has been notified one time.

1. Attachments can be managed according to the type of attachment. This allows administrators to create multiple restrictions and take different actions after a

specified number of processes for each type of attachment. Administrators can also specify the age of the document containing the attachment before the attachment is processed.

2. Attachments can be managed by the retention or age of the document. For example, an administrator can designate that attachments in a document older than 180 days are archived after three processes.

3. Attachments can be managed according to their size. For example, an administrator can specify that any attachment whose size is greater than or equal to 5 MB will be deleted after three processes.

4. Attachments can be managed by the size of the document. For example, an administrator can authorize that any document that contains at least one attachment and greater than or equal to 1 MB will be archived after three processes.

Creation Restrictions

The Creation Restrictions allow administrators to prevent employees from saving or sending emails that do not pass the specified rules. This type of restriction can be used to stop employees from sending inappropriate content or attachments, large attachments that could encumber the router and available server space, and emails to specific domains, groups and/or employees. Creation restrictions also help reduce the likelihood of litigation resulting from email messages that are inappropriate or non-compliant.

There are five different methods of checking emails before they are sent or saved. For each method, there are three available actions to choose from — stop, warn and prompt. By choosing “Stop,” an administrator prevents an email from being sent or saved. By selecting “Warn,” the employee/email sender receives a message on what is invalid, but is still allowed to send or save the email. Using “Prompt,” the administrator displays a dialog box asking the employee if the email should be sent/saved. Both the warning message and the dialog box title are customizable.

The five methods of checking emails are:

1. By attachment name, including attachment extensions.
2. By attachment size.
3. By document (email) content, specifying key words and phrases that aren't permitted.
4. By document size, specifying the maximum size of an email.
5. By recipients, specifying domains, groups and/or employees that should not appear in the “Send To,” “Copy To,” and Blind Copy To” fields.

Document Archiving and Restrictions

The Document configurations allow administrators to locate and manage documents (emails) using four different methods. With each document, an administrator can take one of four actions: Analyze/Report, Archive, Delete or Trash.

The four methods for locating and managing documents (emails) are:

1. By content, specifying specific words or syntax.
2. By documents' (emails') age, specifying the folder(s) in which the documents reside and the maximum age. Keywords can also be specified that will exclude a document from processing if the keywords exist.
3. By document (email) size, specifying folders, age and documents with or without attachments.
4. By document (email) type, specifying field name, values, folders and age.

With Mail Attender's mail restrictions, there are no limitations on the type of concurrent active configurations or the number of total restrictions that exist either for one employee or for all. Administrators can manage employees as collectively or individually as necessary. With each

mail restriction, administrators can also specify the priority of that restriction. The higher the priority of a restriction, the more it supersedes any other restriction of the same type with a lower priority.

3.3 Empowering Organizations to Attain the Upper Hand with Email Management

Mail Attender for Lotus Notes is the most comprehensive email management system in the market. Highly flexible and customizable, Mail Attender offers extensive functionality that it proactively executes by enforcing the restrictions created by administrators. Mail Attender is managed from a central location and does not require additional hardware, therefore it does not need to be uninstalled when server changes occur. A truly unique solution, Mail Attender is the only email management system that allows organizations to monitor employee email activity and ensure emails with certain words or attachments are not sent, as well as enforce archiving and retention policies.

4.0 Summary

The need to observe recently established governmental regulations and a fresh urgency to implement policies regarding corporate conduct has organizations very focused on compliance. To be compliant, organizations need to ensure they are protecting critical financial data and reports, and patient and customer information. They also need to watch out for the possible transfer of critical or confidential information to external sources, and internal communications that could be deemed inappropriate.

Protecting critical data involves more than controlling access via networks and storage systems; it also necessitates that organizations monitor and regulate information residing in its email systems. Organizations need an email management system that will help them with addressing email issues, but will also ensure email compliance by providing capabilities for email content management and archiving, attachment management and archiving, email activity management, and email/document location management.

Mail Attender is an email management system featuring Mail Archiving and Restrictions, which are configured by administrators to establish rules regarding how emails are sent, edited, deleted, archived and stored. With Mail Restrictions, administrators can specify key words and phrases, attachments, subject lines, and addresses that employees cannot use, providing organizations with the control they need to ensure email compliance.

Overall, Mail Attender is robust mail management software that can be used to perform many unique and necessary functions, such as reclaiming critical server and storage space, archiving documents, enforcing corporate retention policies, controlling electronic sabotage, removing non-business-related documents, and protecting authenticity. Mail Attender has truly earned the right to be called email management software — because anything that has to do with email, you can be sure Mail Attender manages it.

5.0 Appendix A

5.1 Technical Specifications for Mail Attender for Notes

Installation

- Easy, non-intrusive Lotus Notes-based installation
- Installed from a single Notes client to all servers
- Server based product – installed on Notes mail servers

Architecture

- Runs on all Domino platforms including 6.x and 6.5.x

- No Domino architectural changes required
- Uses LotusScript-based agents
- Server-based processing
- All processing is performed from a single database

###



Business Records Management

1018 Western Avenue
Pittsburgh, PA 15233

www.businessrecords.com

PH: 412-321-0600

FX: 412-321-5152

Toll Free: 877-342-5276

Email: brmsales@businessrecords.com