



# Best Practices for IM Archiving & Compliance

# Best Practices for IM Archiving & Compliance

## Contents

<b>Abstract</b> .....	3
<b>The Growth of Instant Messaging in the Enterprise</b> .....	3
<b>IM As a Business Record</b> .....	5
<b>Current Regulatory Environment</b> .....	6
Sarbanes-Oxley Act .....	7
SEC Rule 17A-4 .....	7
Gramm-Leach-Bliley Act .....	7
Healthcare Insurance Portability and Accountability Act of 1996 .....	7
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act) .....	8
Department of Defense Rule 5015.2-STD .....	8
National Archives and Records Administration .....	8
CFR Title 47, Part 42 — Telecommunications .....	8
CFR Title 21, Part 11—Pharmaceuticals .....	8
<b>Developing Appropriate Messaging Policies</b> .....	9
<b>Message Retention</b> .....	9
<b>Deployment Best Practice</b> .....	10
<b>Technical Deployment Overview</b> .....	10
<b>About Symantec IM Manager</b> .....	11
<b>About VERITAS ENTERPRISE VAULT™ from Symantec</b> .....	11
<b>The Integrated Solution</b> .....	12
Implementation Procedure .....	13
<b>Conclusion</b> .....	14
<b>Additional Resources</b> .....	15

### **Abstract**

IM continues to be the fastest growing communications medium of all time growing at over 200% in the enterprise.<sup>1</sup> Many organizations have adopted IM as a core component of their messaging infrastructure with upwards of 85% of all organizations citing IM use.<sup>2</sup> As IM usage spreads within organizations, the need for the enforcement of corporate policies has increased. Spurred by government regulations, enterprises are coming to consider IM in much the same way as they consider email and are issuing policy statements, deploying management infrastructure and implementing enforcement processes to round out compliance with their communications policies.

The purpose of this document is to provide an overview of what Symantec believes to be best practices in managing IM as a record of business. These recommendations have been formulated from our experience and the experiences of our enterprise customers with regard to how IM should be managed. This overview is designed to provide guidance on the technical implementation of policy and is not intended to serve as a legal opinion and should not be considered legal advice.

For all questions regarding specific laws and regulatory obligations, please seek the guidance of your compliance officer or legal counsel.

### **The Growth of Instant Messaging in the Enterprise**

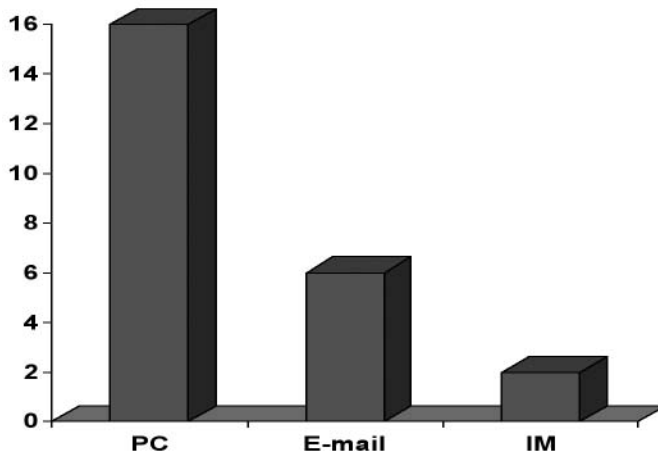
Organizations have come to rely on electronic forms of communications. Today, email makes up approximately 15 billion person-to-person emails per year. The volume of growth is expected to double by the end of 2006.<sup>3</sup> Within this context of rapid electronic communications growth, Instant Messaging (IM) has emerged as the fastest growing communications medium of all time. In comparison to email, it reached the benchmark 50 million users mark in less than half the time and has held steady at approximately 200% growth within the enterprise over the past several years. A recent survey by Radicati found that over 85% of all organizations have some amount of IM use. IM's value stems from the real time nature of the communications and the ability to identify when a person is available for conversations, combining the immediacy of the phone with the discreteness of email.

<sup>1</sup> IMlogic research, Giga Information

<sup>2</sup> Osterman 2002, Radicati Report 2004

<sup>3</sup> IDC Report, 2005

Chart: Years to 50 Million Users



Source: Jupiter Media

The rapid growth of IM in the enterprise has been spurred on by the significant productivity gains achieved. Studies by Gartner Research site that over the next couple of years IM will replace approximately 40% of email traffic and reduce phone and travel expense approximately 20%. Another study by a large software and services firm identified a 20% productivity improvement in their call center operations by adopting IM for communications. Ironically, IM adoption has grown underneath the radar of most IT organizations due to the availability of free services from AOL, MSN, and Yahoo! and because of the ease of deployment. With such strong demand from users and with the backing of the powerful ROI potential, organizations have begun to embrace IM as a mission critical business communications tool.

The rapid adoption of IM has, however, exposed organizations to the equally rapid growth in IM security and compliance threats as the necessary infrastructure for protection readily available for email does not exist in most organizations. To mitigate this risk, companies need to adopt, communicate and enforce standard policies for the use of IM.

For the purpose of this document we will focus on the compliance risks of IM.

## IM As a Business Record

Regulatory bodies lay out the rules for managing a wide variety of business records. Business records are defined broadly but the most relevant to IM is the definition of electronic communications as a form of business records. Until recently this referred primarily to email and most organizations began building their infrastructure to manage their email in accordance to the regulatory and legal statutes. Firms and individuals that do not comply with the regulations and or corporate policies are at risk of fines and in some cases jail time for individuals. In December of 2002, the following 5 firms were fined a total of \$8.35 million for records retention violations: *Deutsche Bank Securities Inc.*, *Goldman, Sachs & Co.*, *Morgan Stanley & Co. Inc.*, *Salomon Smith Barney Inc.*, and *U.S. Bancorp Piper Jaffray Inc.*

**Table: Regulatory Roadmap for Records Retention**

REGULATION	RETENTION IMPLICATIONS	PENALTIES
SEC 17a and 17a-4	Brokers/dealers must retain records for 3 to 6 years or more	Determined on a case-by-case basis
Gramm-Leach-Bliley Act	Financial institutions must ensure security and confidentiality of customer data	Fines up to \$500,000, imprisonment up to 10 years
HIPAA	Members of health care industry must retain patient information for 6 years	Fines up to \$250,000, imprisonment up to 10 years
Sarbanes-Oxley	Accounting firms that audit publicly traded companies must retain all related documents for 7 years after audit	Fines up to \$5 million, imprisonment up to 20 years

*From Network Magazine March 2004, Elizabeth Clark "Data Retention Regulations: Keeping It Legal"*

Because of its clandestine deployment and grass roots growth, IM had been largely ignored in legal and regulatory action. However, in July of 2003, the NASD provided an advisory to their member firms to specifically call out IM as a form of electronic communication similar to email with other regulatory bodies sure to follow:

*“Members must supervise the use of instant messaging consistent with the required supervision of email messaging.” The advisory goes on to state, “If a member is unable to establish an adequate supervisory program, the member must prohibit the use of instant messaging in customer communications. Members must also ensure that their use of instant messaging complies with applicable SEC and NASD recordkeeping requirements.” – NASD Notice to Members July 2003*

Often motivated by regulatory concerns, many organizations have developed relatively robust rules of conduct in the workplace surrounding not only compliance but also sexual or racial harassment, the use of profanity as well as other forms of communications standards. By calling out IM as a form of communication, the regulatory organizations are sending a clear message to businesses. IM is a business record. Policies need to be defined and enforced.

Organizations that do not want to be left behind by tech savvy employees are obligated to take control of the IM use within their organizations. These companies should establish written policies and security procedures to ensure the adherence to corporate rules. In addition, companies should manage IM with technology solutions from within their IT organizations to ensure not only regulatory compliance, but also consistent enforcement of policies.

### **Current Regulatory Environment**

There are numerous federal regulations relating to records retention which affect organizations. Many states have also enacted regulations that supersede these federal regulations, so it is important to understand how to comply with the pertinent laws in your state in addition to applicable federal regulations. Also, while the financial industry has long been overseen by the Securities and Exchange Commission (SEC) and National Association of Securities Dealers (NASD) and the health-care industry has rushed to meet the requirements of HIPAA, other types of organizations must now also respond to federal regulations. Since the enactment of more broad-reaching regulations, such as Gramm-Leach-Bliley (GLBA) and SOX, many types of businesses must focus on how they safeguard, disseminate, store, and track financial information.

Below is a short description of existing regulation and their requirements as they relate to records retention and corporate policy. The following regulations are pertinent to many organizations, however they are meant to provide an overview. Companies should rely on their legal counsel for the applicability of these regulations to their businesses.

### **Sarbanes-Oxley Act**

SOX requires that:

- Executives of publicly traded companies certify the validity of the company's financial statements.
- Financial control and risk mitigation processes be documented and verified by independent auditors.
- Companies implement extensive policies, procedures, and tools to prevent fraudulent activities.

### **SEC Rule 17A-4**

SEC Rule 17A-4 requires that:

- Original copies of all communications, such as interoffice memoranda, be preserved for no less than three years, the first two in an easily accessible location.
- Records that must be maintained and preserved be available to be produced or reproduced using either micrographic media (such as microfilm or microfiche) or electronic storage media (any digital storage medium or system).

### **Gramm-Leach-Bliley Act**

The Gramm-Leach-Bliley Act (Financial Institution Privacy Protection Act of 2001, Financial Institution Privacy Protection Act of 2003) was amended in 2003 to enhance protection of non-public personal information. It requires that financial records be properly secured, safeguarded, and eventually completely destroyed so that the information cannot be further accessed.

### **Healthcare Insurance Portability and Accountability Act of 1996**

HIPAA requires that:

- Security standards be adopted that do the following:
  - > Control who may access health information.
  - > Provide audit trails for computerized record systems.
  - > Meet the needs and capabilities of small and rural healthcare providers.
- Health data be isolated and inaccessible to unauthorized access.
- Transmission of health information is physically, electronically, and administratively safeguarded to ensure confidentiality.

### **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act)**

The Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) does the following:

- Requires that financial institutions implement reasonable procedures to maintain information used to verify the identity of a person opening an account with any financial institution.
- Provides law enforcement organizations broad investigatory rights.

### **Department of Defense Rule 5015.2-STD**

Department of Defense Rule 5015.2-STD requires systematic record management, including how records are classified, created, deleted, maintained, reproduced, and used.

### **National Archives and Records Administration**

The National Archives and Records Administration does the following:

- Oversees official government recordkeeping.
- Requires adequate and proper documentation on how U.S. government business is conducted, including the policies and procedures of government agencies.
- Defines records as machine-readable materials made or received by an agency of the U.S. government under federal law or in connection with the transaction of public business.
- Requires that electronic records on a particular subject or function be organized within a record series that facilitates the management of these records.

### **CFR Title 47, Part 42 — Telecommunications**

CFR Title 47, Part 42 requires that telecommunications requires telecommunications carriers to keep original records or reproductions of original records, including memoranda, documents, papers, and correspondence that the carrier prepared or that were prepared on behalf of the carrier.

### **CFR Title 21, Part 11—Pharmaceuticals**

CFR Title 21, Part 11—Pharmaceuticals requires that:

- Controls are in place to protect content stored on both open and closed systems to ensure the authenticity and integrity of electronic records.
- The ability to generate accurate and complete electronic copies of records so that the Food and Drug Administration may inspect them.

### Developing Appropriate Messaging Policies

Creating messaging policies involves two entities: stakeholders and deliverables.

Business stakeholders should participate in representing the primary organizations of the company, including representatives from the legal, financial, and IT departments. Involving the appropriate stakeholders helps ensure that policies are not only legally correct but also adequately protect your organization's interests and can realistically be implemented and enforced. This group should consider the risks and realities of your organization's structure and define policy implementation precisely. This stakeholder team is tasked with recommending ways that the business will meet compliance-related regulations. In particular, the team should:

- Determine what data should be considered official business communication or records
- Develop a comprehensive written policy for messaging and retention
- Educate information workers on how to follow these policies

If your organization does not already have a comprehensive electronic messaging policy, the stakeholders should develop one along with its data retention policies.<sup>4</sup>

### Message Retention

While many regulations require a specific retention period for business-specific data, not all businesses fall under these requirements; financial services organizations typically have the most stringent data retention requirements. Businesses that are not subject to specific data retention requirements should also document their particular data retention policies and, most importantly, follow these policies. One of the most frequent errors companies make is stating a policy of message purging only to ignore their own process. During investigations, companies that do not clearly follow their own stated policies are often forced to spend considerable time restoring and retrieving messages from various backup media.

As part of defining a policy, organizations should ensure that the implementation of the process for data management is in line with the policy. For example, if your plan states that e-mail and IM is kept for a year, your backup records should not be retained for more than that length of time. Centralized data storage for e-mail, IM and other types of documents ensures that you can easily recover such data in the event that you are required to recover it by legal discovery processes. The ability to preview such documentation, should it be necessary, is helpful when preparing for any legal proceeding.

<sup>4</sup> The SANS (SysAdmin, Audit, Network, Security) Institute, a cooperative research and education organization, provides sample policies for messaging at: <http://www.sans.org/resources/policies/#template>. These sample templates may help to create a more comprehensive policy for your organization.

A number of factors within an organization determine the need for a regulatory compliance solution. Understanding what these factors are and consequently whether an organization needs to implement such a solution typically requires cooperation among a number of groups within the organization. In addition, in driving the organization towards implementing information life-cycle management tools, understanding the needs and requirements of individual groups helps build support for the initiative across the organization.

### **Deployment Best Practice**

Building a repeatable process for data management often includes the implementation of software solutions. Leading software solutions make the centralized management and enforcement of the compliance and messaging policy schedulable and effective. Organizations should look for a solution that delivers a robust and integrated solution for managing all of their messaging retention and compliance needs.

Symantec delivers a tightly integrated system which enables an organization to implement and manage the message capture, archiving, recovery and retention policy required by legal and regulatory bodies through Veritas Enterprise Vault™ from Symantec and Symantec™ IM Manager.

The implementation of an integrated solution provides efficiency and management benefits across the organization:

- Best-of-breed technology and world-class support in the archiving, retention and discovery management space for email and IM.
- Utilization of current email interface for discovery processing and reporting by converting instant messages into standard email formats.
- Leverage existing corporate investments in archiving and retention technologies, hardware and software, as well as the resource requirements involved in training and configuring these systems.
- Cost savings through the consolidation of the back-end storage system decreasing the cost of hardware, software and management necessary to implement the retention system.
- Reduced training costs due to leveraging existing processing rules and lexicons for scanning instant messages.

### **Technical Deployment Overview**

Symantec IM Manager and Veritas Enterprise Vault™ from Symantec are leading solutions for the capture, archiving, review and retention of electronic messaging. Together, they provide a solution for enterprises needing to address retention mandated by statutes, regulations and corporate governance for email and instant messaging communications.

### **About Symantec IM Manager**

Symantec provides the industry's most widely deployed and trusted solution<sup>3</sup> for seamlessly managing, securing, logging and archiving IM with Symantec IM Manager. A flexible solution that enables organizations to meet compliance and corporate governance requirements, IM Manager provides comprehensive IM logging, archiving and discovery without additional levels of investment or ongoing support. Key capabilities for IM compliance include:

- **Guaranteed 100% Message Capture** — A robust architecture ensures zero message loss archiving with 100% message capture and full indexing of IM conversations and multi-party chat sessions — all without performance degradation — with direct integration to Veritas Enterprise Vault from Symantec.
- **Audit Tools with User and Reviewer Management** — Full audit tool capability results in an enhanced archive that includes keyword search, one-click message reconstruction, message annotations and random conversation review for compliance officers and supervisors — all with a specialized reviewer console for workflow management and policy reviews.
- **Consistent Policy Communication and Enforcement** — A configurable priority-based rules engine provides predictable policy enforcement while disclaimer insertion and user notification help to ensure consistent communication and reduced support calls.
- **Certified Support for Public and Enterprise IM** — Integrated, certified support for the leading public and enterprise IM systems, including AOL, GoogleTalk, MSN, Yahoo!, IBM Sametime, Microsoft Office Live Communications Server 2003/2005, Jabber and more, lets organizations use disparate IM networks and still be IM compliant.

### **About VERITAS ENTERPRISE VAULT™ from Symantec**

Veritas Enterprise Vault from Symantec provides a flexible archiving framework to enable the discovery of content held within email, file system and collaborative environments, while reducing storage costs and simplifying management. Enterprise Vault manages content via automated, policy-controlled archiving to online stores for active retention and seamless retrieval of information. The built-in powerful search and discovery capabilities of Enterprise Vault are complemented by specialized client applications for corporate governance, risk management and legal protection.

## Best Practices for IM Archiving & Compliance

Central to every organization is the creation and ongoing management of the archive and its contents. Enterprise Vault software is designed to deliver the capability to securely retain archived data in such a way that it can be fully exploited and expired when it is no longer required. The Repository is designed to:

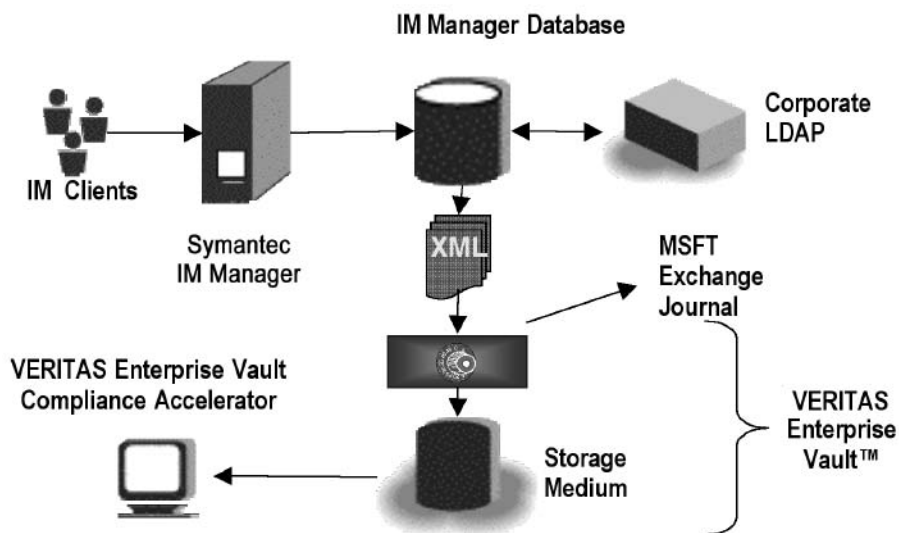
- Flexibly store archived content
- Reduce storage via compression & single-instancing
- Index content for rapid and targeted retrieval
- Secure future accessibility regardless of application by rendering an HTML copy of all archived content
- Utilize user authentication security controls
- Define and implement retention and expiration policies

Implementing Enterprise Vault helps you reduce your business and IT risks surrounding: Application Storage Management; Compliance Retention & Discovery; Operational Excellence; Knowledge Utilization; and Upgrade, Migration & Consolidation.

### **The Integrated Solution**

After deployment of Veritas Enterprise Vault from Symantec, Symantec IM Manager and the Symantec IM Manager Export tool, companies can easily archive the instant messages captured by IM Manager to Enterprise Vault. IM Manager exports IM conversations as formatted SMTP messages, and can be configured to forward those messages to a Microsoft Exchange Journaling mailbox, where they are processed, indexed, archived, and made accessible for search and review through Enterprise Vault.

Diagram: Symantec IM Manager — Veritas Enterprise Vault from Symantec Deployment Architecture



### Implementation Procedure

Deployment of the integrated solution requires 5 simple configuration steps in order to customize the integration to your environment. The steps are outlined below:

- 1. Set up Exchange Server to Accept Symantec IM Manager Messages.** In some organizations, the ability to relay messages to the Exchange server is limited to specific machines. If this is the case, ensure that the Symantec IM Manager server has the ability to deliver SMTP messages to the Exchange server.
- 2. Configure IM Manager Directory Integration.** Before configuring Symantec IM Manager to send messages to the Exchange Journaling mailbox, you must prepare your system by adding user's email addresses to the message data in the IM Manager database. This is required because Veritas Enterprise Vault from Symantec uses the email address as the user's unique identifier. In addition, this allows Enterprise Vault to associate the transcript with the user for filtering and review purposes.
- 3. Configure Symantec IM Manager Server to deliver SMTP Messages to Microsoft Exchange.** Symantec IM Manager uses the IIS SMTP service built into windows to deliver instant message transcripts to the Exchange Journaling Mailbox.

#### **4. Install Symantec IM Manager.** Veritas Enterprise Vault XSL Transformation from Symantec.

The Symantec IM Manager export tool uses an XSL transformation process to generate the final SMTP messages that are delivered to Veritas Enterprise Vault from Symantec. This file can be customized to the specific requirements outlined by the customer deployment or compliance needs.

#### **5. Configure Symantec IM Manager Export.** The Symantec IM Manager User interface enables the user to set preferences regarding schedule and provides valuable information relating to the job history and success of an individual export.

*NOTE:* Detailed implementation guides are available through the Symantec Support organization and as part of the administrator guides provided by Symantec to all of its customers.

### **Conclusion**

Instant Messaging usage continues to grow at approximately 200% in the enterprise, with many organizations adopting IM as a mission critical component within their communications infrastructure. With over 80 million corporate users, instant messaging is becoming as ubiquitous and as integral to corporate communications as email. Unfortunately, the explosive growth of instant messaging, spurred by the freely available public IM networks has created an entrenched user community that falls outside corporate electronic messaging guidelines.

The use of corporate instant messaging often goes unmonitored and unmanaged, exposing corporations to litigation and compliance risks. Further, without an enforced use policy, IM is an attractive outlet for misuse of corporate networks, heightening risks. Several federal agencies have already responded, explicitly identifying instant messaging as a regulated communication.

These trends are causing organizations to adapt their existing email policies — for permitted use, compliance, discovery and archiving — to include instant messaging. Organizations need to build consistent messaging policy which includes all electronic communications and implement solutions in order to systematically adhere to the policies they publish.

By implementing a solution that supports the capture, archiving, review, discover and retention policy enforcement companies are able to meet the increasingly stringent requirement placed on them by the existing and evolving federal and state regulations. Symantec works with organizations every day to help ensure that they comply with government regulations and assists them with implementing effective systems to enforce the messaging retention and compliance policies that are appropriate to their business.

**Additional Resources:**

***CFTC Website***

<http://www.cftc.gov>

***NASD Website***

<http://www.nadr.com>

[http://nasdr.com/conrule\\_3010](http://nasdr.com/conrule_3010)

***NYSE Website***

<http://www.nyse.com>

***SEC Website***

<http://www.sec.gov/>

***FDA Website***

<http://www.fda.gov>

***Department of Health***

<http://dchealth.dc.gov/index.asp>

***Gramm-Leach-Bliley Act***

<http://banking.senate.gov/conf/>

<http://www.epic.org/privacy/giba/>

## About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
1 408 517 8000  
1 800 721 3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. All other names may be trademarks of their respective owners. Printed in the USA. All product information is subject to change without notice.  
03/06 10536292