



Information  
Management

# Managing Instant Messages

August 2005

**Alberta**  
Government

*Produced by*

Information Management Branch  
Government and Program Support Services  
Alberta Government Services  
3<sup>rd</sup> Floor, Commerce Place  
10155 - 102 Street  
Edmonton, Alberta, Canada  
T5J 4L4

Office Phone: (780) 422-2657

Fax: (780) 427-1120

Web site:

[www.im.gov.ab.ca](http://www.im.gov.ab.ca)

©Government of Alberta

ISBN 0-7785-3684-X

# Contents

<b>Contents .....</b>	<b>i</b>
<b>Executive Summary .....</b>	<b>ii</b>
<i>Overview of instant messaging .....</i>	<i>ii</i>
<i>Government policies related to instant messaging .....</i>	<i>iii</i>
<i>Establishing ministry policies and guidelines for instant messaging .....</i>	<i>iv</i>
<b>1. Introduction .....</b>	<b>1</b>
<i>Scope .....</i>	<i>1</i>
<i>Purpose .....</i>	<i>1</i>
<i>Overview.....</i>	<i>3</i>
<b>2. Overview of Instant Messaging .....</b>	<b>4</b>
<i>Business advantages.....</i>	<i>4</i>
<i>Types of instant messaging services.....</i>	<i>6</i>
<i>Developing a strategy for instant messaging.....</i>	<i>10</i>
<i>Conclusion.....</i>	<i>12</i>
<b>3. Government of Alberta Policies Related to Instant Messaging.....</b>	<b>13</b>
<i>Authorized use of Government of Alberta systems.....</i>	<i>13</i>
<i>Acceptable use of Internet and e-mail .....</i>	<i>13</i>
<i>Transmission of personal information via e-mail.....</i>	<i>14</i>
<i>Managing instant messages as records .....</i>	<i>15</i>
<b>4. Establishing Ministry Policies and Guidelines for Instant Messaging.....</b>	<b>17</b>
<i>Acceptable use of instant messaging services .....</i>	<i>17</i>
<i>Appropriate types of content for instant messaging .....</i>	<i>19</i>
<i>Managing instant messaging records .....</i>	<i>20</i>
<i>Transmission of personal information via instant messaging .....</i>	<i>21</i>
<i>Storage of government information on home computers .....</i>	<i>21</i>
<i>Appropriate style and effective business use.....</i>	<i>22</i>
<i>Conclusion.....</i>	<i>22</i>
<b>Appendix 1: Model Policy and Guidelines for Instant Messaging .....</b>	<b>23</b>
<i>Policy.....</i>	<i>23</i>
<i>Guidelines .....</i>	<i>25</i>
<b>Appendix 2: Resources .....</b>	<b>27</b>
1. <i>Introduction.....</i>	<i>27</i>
2. <i>Standards.....</i>	<i>27</i>
2. <i>Government Information.....</i>	<i>28</i>
3. <i>Other Government Documents.....</i>	<i>29</i>
4. <i>Research Documents.....</i>	<i>29</i>

## Executive Summary

Instant messaging is an easy-to-use computer-based messaging service. In some ways, it is like a conversation, but one that uses text-based rather than voice-based communication. In another sense, it is like “live e-mail,” where a “sender” (the person who initiates the conversation) and a “receiver” (the person contacted) can carry on a conversation in real time.

Gartner Research estimated that in 2003 over 90% of enterprises were using instant messaging to some extent – often without the organization’s information management and information technology staff knowing about it. In April 2005, there were almost 90,000 instant messaging logins across the Government of Alberta.

Instant messaging can be an effective business tool. However, there are significant risks associated with using public instant messaging services outside the control of the Government of Alberta (GoA). Also, instant messages (like e-mail) are government records, and must be managed to meet government recordkeeping requirements.

Without appropriate business rules, instant messaging (like other tools such as e-mail) can be misused and increase risks related to inadequate protection of sensitive information, not adequately documenting business decisions, and not managing government records throughout their life cycle. Ministries will need to consider legal and policy requirements as well as good information management practices when developing their instant messaging strategy.

## Overview of instant messaging

Instant messaging is used in a business environment because it enables users to see who is online (and thus contactable for a conversation), provides instant communication, and allows users to hold several conversations at one time.

There are three main types of instant messaging services. These are:

- **Public services:** Public services are provided by third parties, such as AOL and Microsoft. Services are hosted on servers external to the organization and servers can be reached via the Internet. A public service provides basic functionality and requires no technical input from the organization, but does require a desktop policy that allows the downloading and installation of software by users or administrators. These services are also easily installed on notebooks and home computers. These services are not under the control of your ministry.

- **Third-party hosted service:** Some instant messaging services (e.g., AOL Enterprise and Yahoo! Business Messenger) are hosted by third parties. These hosted services are similar to public services in the way in which they are provided. However, service providers typically offer enhancements, such as logging and audit functionality. A third-party hosted service permits a degree of control over issues such as change control and authentication. Many of these services link to corporate directories, allowing easy location and authentication of users.
- **Self-hosted service:** Other instant messaging services can be hosted internally. These would include collaboration functionality in electronic information management (EIM) applications as well as other standalone applications such as IBM Lotus Instant Messenger, Microsoft Live Communications Server 2003, NetMeeting, E-Room, or Peak. These services are totally under the control of the organization. They could be running within a single ministry or multiple ministries.

Using public instant messaging services, and to a lesser extent third-party messaging services, for business can pose risks to ministries. While these risks are mitigated within the GoA by firewalls and up-to-date virus protection, the risks are very much present if employees are using public instant messaging services on either a notebook computer or a home computer. These risks include security threats to the system (including viruses and worms), impersonation of government employees, message theft and access to sensitive information. Moreover, public messaging services do not allow the capture and management of official government records.

## Government policies related to instant messaging

While instant messaging is a relatively new business tool, there are a number of Government of Alberta policies that relate to the use and management of instant messaging. These include:

- acceptable use of the Internet and e-mail;
- transmission of personal information via e-mail and facsimile;
- Government of Alberta information technology security policy; and
- government recordkeeping requirements.

## Establishing ministry policies and guidelines for instant messaging

The combination of the risks associated with public instant messaging services and the legal requirements for recordkeeping and the protection of personal information require that clear policies and guidelines be established related to instant messaging.

Ministries need to consider the following:

- whether they will allow employees to use public instant messaging services in the workplace or when working outside the office;
- if they allow the use of public messaging services, under what conditions or for what purposes should instant messaging be used or not be used;
- how appropriate records of business decisions recorded in instant messages will be captured; and
- guidance for employees on the effective use of instant messaging.

In all cases, if the ministry does not have the capability to capture and properly manage instant messages that are official records of government, then instant messaging should not be used or only be used for conversations that are transitory in nature.

Instant messaging, like e-mail, is only one of many business tools. It needs to be part of an integrated and coherent strategy that incorporates the management of instant message records into an electronic information management (EIM) system. Instant messaging should not be considered a solution in itself, but a component of an organization's electronic information management environment.

By developing clear policy and guidelines, ministries can mitigate risk, support the effective use of instant messaging as a business tool, and ensure the use of instant messaging meets legal and policy requirements.

# 1. Introduction

Instant messaging is being used more and more in the conduct of business. Gartner Research estimated that in 2003 over 90% of enterprises were using instant messaging to some extent – often without the organization’s information management and information technology staff knowing about it. In April 2005, there were almost 90,000 instant messaging logins across the Government of Alberta.

Instant messaging originated as a free software download for consumers in 1996. The technology provides the ability to chat online, as well as to share files. Even if the software is not downloaded in a work environment, instant messaging can still be accessed by sending messages directly from a web browser, such as Microsoft Internet Explorer.

Without appropriate business rules, instant messaging, like other tools, can be misused and increase risk to your ministry – risks associated with inadequate protection of sensitive information, not adequately documenting business decisions, and not managing government records throughout their life cycle.

## Scope

This guide has been developed for information management professionals in the Government of Alberta. It is designed to help ministries identify the major issues surrounding the deployment and use of an instant messaging system. It identifies areas where guidelines may be needed and provides an example of an instant messaging policy.

## Purpose

The purpose of this document is to:

- explore the more significant risks associated with using public instant messaging services;
- bring together existing policies and legislation that govern the management of information that would affect the use of instant messaging; and
- identify guidelines and practices that should be established at the ministry level.

The advice given in this document will help ministries develop effective practices that comply with relevant legislation related to government records:

- [Records Management Regulation](#) governs how records must be managed and the process for approving how long they must be retained. This Regulation also governs the disposition of records – either through destruction, or transfer to the Provincial Archives of Alberta.
- [Historical Resources Act](#) establishes the Provincial Archives and governs the permanent preservation of government records of archival value to ensure they are available to Albertans in the future.
- [Freedom of Information and Protection of Privacy Act](#) (FOIP) governs the collection, use and disclosure of personal information, how personal information must be handled and protected, and the right of the public to access records in the custody or under the control of ministries.
- [Health Information Act](#) (HIA) governs the collection, use and disclosure of health information, how health information must be handled and protected, and the right of the public to access their own health information in the custody or under control of custodians defined under the Act, including the Ministry of Health and Wellness. The Act does not apply to health records retained by other ministries.
- [Electronic Transactions Act](#) gives electronic signatures and records the same legal status as their paper-based counterparts.
- [Alberta Evidence Act](#) provides rules on the admissibility of paper records in court proceedings. The Act also includes electronic records.
- [Government Emergency Planning Regulation](#) requires ministries to create plans for business resumption, including the identification and handling of records needed for business resumption after emergencies and the protection of assets, financial records and other records maintained by the ministry.

All of this legislation means that ministries must have in place recordkeeping practices and procedures. This document places instant messaging within the context of these recordkeeping requirements.



## Overview

This guide contains three main sections:

- The [Overview of Instant Messaging](#) briefly discusses what instant messaging is, the business reasons for using instant messaging, the types of services available and the main security risks associated with using public instant messaging services.
- The [Government of Alberta Policies Related to Instant Messaging](#) describes existing government policy and legislation that affect the use and management of instant messages.
- [Establishing Ministry Policies and Guidelines for Instant Messaging](#) provides advice on practices related to managing instant messaging within ministries. Ministries are responsible for developing appropriate recordkeeping systems and user guidelines that include the handling of records created using instant messaging.

An [example of a ministry policy and guideline](#) on instant messaging is presented in Appendix 1 and [additional resources](#) on instant messaging can be found in Appendix 2.

## 2. Overview of Instant Messaging

Instant messaging is an easy-to-use, computer-based messaging service. It is like a conversation, but one that uses text-based rather than voice-based communication. In another sense, it is like “live e-mail,” where a “sender” (the person who initiates the conversation) and a “receiver” (the person contacted) can carry on a conversation in real time. It enables two-way conversations as well as including more than two people in the same conversation – all online, and without requiring the participants to be in the same place.

The technology that delivers instant messages is maturing to the point where it can now achieve not only text-based conversation but also host online audio and video meetings as well as other collaborative tools.

### Business advantages

Instant messaging is used in a business environment for collaboration and communication because it:

- enables users to see who is online, and thus contactable for a conversation;
- provides instant communication;
- is easy to use;
- allows users to hold several conversations at one time;
- is less intrusive than the telephone as an immediate response is not required; and
- provides greater functionality – such as e-conferencing, chat rooms and file transfer – than other messaging techniques such as e-mail or the telephone.

The following scenario illustrates how instant messaging can be used in an organization.

---

#### *Scenario*

Bob works in Edmonton. Today when he arrives at work, he logs onto the network. He sees that his boss, Susan, who is in Red Deer for a meeting, is already online. He sees this because instant messaging shows the “status” of all of his contacts – whether they are “online,” “busy,” “away,” or “offline.”

When Bob signs on to the network, Susan receives an alert that lets her know Bob has just come online. She starts a conversation with him. “Good morning Bob. Hope you’re well. I have a quick question...what’s the status of the annual report...how close are we to finishing the final edits?”

Bob replies, “Hi Susan...I’m not sure, but I’ll find out...I know Kim in Calgary was working with the editor yesterday...but she’s not in yet...I’ll check with her when she gets in and get back to you. Wait, here she is now, let’s ask her to join us.”

Bob invites Kim into the conversation. “Good morning, Kim. I’m talking to Susan” (Kim writes, “good morning to Susan.”). Bob continues, “what is the status of the edits on the final report?”


Kim replies, “I was working with the editor yesterday...we’re very close...he says he can get the final edit back to me this afternoon.”

Susan replies, “Great...and thanks.” Kim writes, “Susan, do you want me to send you the final edit when it gets here.” Susan replies, “Yes...thanks. I’ve got to run now...have a breakfast meeting to go to...have a great day, both of you.” Bob, writes, “You, too, Susan. Bye.” “Kim, do you have a couple of minutes?” Kim writes, “Bye Susan... sure Bob.”

Bob writes, “What’s on the agenda for tomorrow’s meeting...is there anything I have to prepare?” Kim replies, “No Bob, not from your area...unless you’ve got something for the round-table, which is item 5 on the agenda.” Bob replies, “Thanks, I haven’t seen the agenda yet.” Susan writes...“It’s posted on the work group section of the intranet.” Bob replies, “Great, I’ll check it out now. Thanks Susan, have a great day.” Susan replies, “thanks...you too...bye for now.”

While Bob is talking to Kim, Jim, who works in Red Deer starts a conversation with him. “Morning, Bob.” Bob replies, “Morning, Jim.” “Bob,” writes Jim, “are we still on for the team meeting at 2 o’clock this afternoon?” Bob replies, “Yes, Jim, everyone should be on the conference call except for Cathy who is on holidays.” Jim writes, “Bob, how long do you think the meeting will last?” Bob, responds, “should be a quick one, because we only have the three agenda items, and none of them is complicated – maybe 45 minutes.” Jim replies, “that’s great...I’m trying to set up a 3 o’clock meeting with a client of ours. Talk to you this afternoon. Bye.”

Bob is getting ready to go off to a 9 o’clock meeting. He sets his status to “away.” This alerts people that he is not at his computer. They can still send him instant messages, but by seeing that he is “away,” they at least know not to expect an immediate response. Bob can get back to them when he is back from his meeting. Because he is “away,” his contacts may choose to send him an e-mail instead, which Bob can respond to later.



This simple scenario shows some of the benefits of instant messaging – real time conversation, especially with people who are not located in the same office; the ability to see who else is available (without having to dial the telephone and get voice mail); and the ability to carry on multiple conversations at once.

### ***Time management***

Being faster than a phone call in most cases and unlike e-mail, which may not be noticed for hours, instant messaging has become a useful tool in the fast-paced business environment of today.

In order to receive an answer to a question, the easiest way seems to be instant messaging. The user can see who, among their contacts, is online. They can initiate a conversation and ask the question and receive the reply.

Users can also manage their availability to others. By using the online status option you have the capability to change your online status to options such as “away”, “busy”, “out to lunch”, and “on the phone”, therefore reducing the interruptions that are caused by walk-ins or phone calls while you are otherwise occupied. This also alerts contacts that you may not be participating in the conversation immediately. Unless your online status is set to “offline,” instant messages continue to be received and can be responded to at a later time.

### ***Productivity enhancement***

The main reason that instant messaging has been adopted in today’s business environment is that it can enhance productivity. It has been shown that “43% of daily users send less e-mail and 59% make fewer phone calls since using instant messaging. But almost two thirds of daily users contact more people, more frequently since adopting instant messaging”<sup>1</sup>

Why is this? There are many reasons. One is the ability to contact colleagues via a mobile device such as a mobile phone or a personal digital assistant (PDA). With this technology, it is easier to get the assistance you need immediately if your colleague is out of the office or in a meeting, at which time your colleague can either send a message back or wait until he or she is not busy. Another reason is that by using instant messaging, the user can easily carry on more than one conversation at once, and continue to work on other things.

## **Types of instant messaging services**

The three main types of instant messaging services are:

- public services;
- a third-party hosted service; and

---

<sup>1</sup> Larry Schlang, Bantu Incorporated, *Instant Messaging for the Business Market*, 2001.

- a self-hosted service.

These main types of instant messaging services are able to run on commonly used operating systems, including Windows, Mac OS, Unix and Linux. Furthermore, they provide similar basic functionality, including:

- wireless support for personal digital assistants (PDAs) and mobile phone use of text;
- voice and video communication;
- file transfer and sharing;
- collaborative tools, such as whiteboards, e-conferencing and chat rooms; and
- entertainment features such as gaming.

### ***Public hosted instant messaging services***

Public services are easily accessible and provided by companies such as AOL and Microsoft. Services are hosted on servers external to the organization and servers can be reached via the Internet.

Public services are usually free and can be installed with a minimum of technical expertise. The most well-known examples are:

- AOL Instant Messenger and AOL ICQ;
- Microsoft MSN Messenger; and
- Yahoo! Instant Messenger.

A public service provides basic functionality and requires no technical input from the organization, but does require a desktop policy that allows the downloading and installation of software by users or administrators. They are also easily installed on notebooks and home computers and can also be accessed through web browsers. These services are not under the control of your ministry.

### ***Third-party hosted instant messaging service***

Some instant messaging services (e.g. AOL Enterprise and Yahoo! Business Messenger) are hosted by third parties. These hosted services are similar to public services in the way in which they are provided. However, service providers typically offer enhancements, such as logging and audit functionality.

A third-party hosted service requires little technical input from your ministry but does permit a degree of control over issues such as change control and authentication. Many of these services link to corporate directories, allowing easy location and authentication of users.

### ***Self-hosted instant messaging service***

Other instant messaging services can be hosted internally. These would include collaboration functionality in electronic information management (EIM) applications as well as other standalone applications such as IBM Lotus Instant Messenger, Microsoft Live Communications Server, NetMeeting, and E-Room. These services are totally under the control of the organization. They could be running within a single ministry or multiple ministries.

### ***Mitigating risk associated with public instant messaging services***

Of the three types of service, a self-hosted service provides the greatest level of management control, but is the most likely to have a cost, and requires an investment in technical expertise, software and hardware. Instant messaging is only under an organization's control if it adopts a self-hosted service. Public and third-party services do not offer direct control of the services.

To date, the various public services have not been interoperable – someone using a public instant messaging service such as AOL cannot send a message to someone using Yahoo instant messenger or to an MSN user. However, this may be changing.

The only roadblock to complete interoperability of these systems is the unwillingness of the major players to agree on a standard for instant message systems. The body responsible for setting standards for the internet, the Internet Engineering Task Force (IETF), is reviewing the two standards that are emerging: SIP/SIMPLE and Jabber/XMPP.

SIP/SIMPLE is being adopted by the organizations like Microsoft and IBM who have incorporated it into their instant message systems. SIP/SIMPLE is capable of incorporating multimedia transmission into an instant messaging system.

Jabber/XMPP is designed to be open-source and uses XML. It is suited towards leveraging across disparate systems and could potentially be cheaper. One of the major strengths of Jabber is that it is server-based and thus all messages are both logged and audited independent of the user. The downside to this is that it places more load on servers and does not manage the life cycle of messages.

Public instant messaging services (and to a lesser extent) third-party messaging services can pose risks to ministries. While these risks can be mitigated by using a

self-hosted service, (and the additional security protection within the GoA domain), the risks are very much present if employees are using public instant messaging services on either a notebook or a home computer. The primary risks posed by the use of **public** instant messaging services are:

- **Security.** First, file-transfers, image transfers, voice chat and other features may reveal a user's Internet Protocol (IP) address. Once your IP address is known, it is possible for a malicious user to concentrate on your system for the purpose of cracking it. Another security threat is worms. Worms may propagate by instant contact lists, sending an infected file to each person on the contact list – in this case, a virus masquerading as an instant message from a contact. Finally, as with any Internet-based program, instant messaging raises the risk of receiving files that are infected with a virus and the invisible launching of viruses. While firewalls and up-to-date virus detection can mitigate these risks, many notebook computers and home computers do not always have up-to-date protection. For further information, the Information Security Forum report on Securing Instant Messaging is available at [www.sharp.gov.ab.ca/secure/search.cfm?Category=7&Term=4963](http://www.sharp.gov.ab.ca/secure/search.cfm?Category=7&Term=4963)
- **Identify Theft/Impersonation.** To register as a user of an instant messaging service requires only an e-mail address (and a password), but the e-mail address can be chosen by the user when they register. And, users can sign-in using an alias. Although a user would need to be added to someone else's contact list there is a possibility of impersonation – someone signing on pretending to be a government employee when, in fact, they are not and, thus, placing the ministry at risk.
- **Message theft and access to sensitive information.** Instant messages are transmitted as clear text (as are e-mail messages), using simplistic, and unsecured protocols making it possible for third parties to sniff, or grab, these messages while in transit to view them. While this is extremely unlikely, it is possible that sensitive information, if not encrypted, may be intercepted.
- **Lack of a record of decision-making.** Instant messaging logs often have to be enabled by the user (or forced by desktop policy), or can simply be captured by the server automatically. Even once they have been enabled, these logs are typically limited to a record of conversations held and do not always include contents of transferred files or the sharing of files. Without the logging of business conversations, organizations will have difficulty confirming or denying that a message or file was sent or received.
- **Spam and SPIM.** SPIM is a new form of electronic junk mail. Until recently, instant message users were completely free from the junk mail that

is so prevalent in e-mail. However, the increased popularity of instant messaging means individuals have begun barraging instant messaging systems with junk messages and pop-ups. While messaging services can eliminate this annoyance by only allowing people on a user's contact list to send messages, if one of the contacts is receiving SPIM, this could potentially spread SPIM to all of a user's contacts as well.

- **Unintentional Messaging to Non-Business Contacts.** Software exists that can facilitate the use of multiple instant message services at the same time. The technology has matured to point where products are providing the ability to import contact lists from a public system into a self-hosted instant messaging service. As a result, non-business instant messaging contacts could be mistakenly brought into a thread with the potential of sending business information out into the public domain. This risk can be mitigated by managing business contacts and personal contacts separately.

The risks of using public instant messaging services within the GoA domain are mitigated in the sense that the IP address is not detectable, and virus scanning is up-to-date. However, these messages, like e-mail messages may be at risk once they leave the GoA domain.

A self-hosted instant message solution, coupled with an effective electronic information management (EIM) solution and clear business rules, can provide the control and the infrastructure needed to manage instant messaging to mitigate these risks.

With its business advantages, instant messaging is here to stay. However, there are significant risks and threats to using either a public instant messaging service or a third-party hosted service. As such, there is a need to raise the control of instant messaging to that of similar systems like e-mail by addressing issues such as authentication, security, anti-virus capabilities and the logging of messages.

## Developing a strategy for instant messaging

Instant messaging, like e-mail, is only one of many business tools. It needs to be part of an integrated and coherent strategy that incorporates the management of instant message records into an electronic information management (EIM) system. Instant messaging should not be considered a solution in itself, but a component of an organization's electronic information management environment.

Policy and existing business processes need to guide how instant messaging technology will be implemented for both personal and business use. When developing an instant messaging strategy, stakeholders from all parts of the ministry



need to be involved in the process. Because of the range of issues involved, input should be sought from Information Technology, Legal Services, FOIP, Records Management and Human Resources.

Some of the issues that need to be addressed include:

- whether the ministry will allow employees to use public instant messaging services, and under what conditions;
- when to use and when not to use instant messaging for different types of content;
- acceptable use of instant messaging for business and personal content;
- how the ministry will capture records of business decisions;
- the internal resources, both financial and staffing, allocated to the implementation, training and long-term maintenance of the instant messaging program;
- how to apply retention and disposition schedules to business instant messages that are official records of the ministry;
- procedures for the protection of personal information;
- the method(s) to be used for identifying and locating records and how to suspend their destruction during FOIP requests or litigation;
- how to comply with the GoA security standard for encrypting personal information if it is to be transmitted outside of the government;
- training staff in the appropriate use of instant messaging as a business communication tool; and
- the monitoring and audit of the use of instant messaging in the ministry.

The business use of instant messaging will breach legal and regulatory requirements if messages or conversations that contain business decisions are not retained as records.

In order to meet these obligations, a holistic approach to implementing instant messaging is needed and should integrate with an organization's electronic information management (EIM) system.

## Conclusion

Instant messaging can be an effective business tool. However, there are significant risks associated with instant messaging, especially when using public and third-party hosted services. Moreover, it is a relatively new tool in the business environment. As with other tools (portable computers, e-mail, PDAs, and even the telephone) instant messaging needs to be managed and employees will need guidance on the most effective use of the tool. Ministries need to consider legal and policy requirements related to the use of instant messages when developing their instant messaging strategy.

### 3.

## Government of Alberta Policies Related to Instant Messaging

Several policies relate to the use and management of messages created through instant messaging in the Government of Alberta. These policies relate to:

- the authorized use of the Government of Alberta systems;
- the acceptable use of Internet and e-mail;
- the handling of personal information; and
- government recordkeeping requirements.

It should be noted that none of these policies explicitly mentions instant messaging. In some cases (e.g., acceptable use and government recordkeeping), the policies and legal requirements are broad enough to apply to instant messaging. In other cases (e.g., the transmission of personal information), the policy can be inferred to apply to instant messaging because of its application to the technology used to transmit instant messages.

### Authorized use of Government of Alberta systems

Access to Government of Alberta systems will be based on business needs and will normally be provided to all employees of the Government of Alberta.

The [Government of Alberta Information Technology Security Policy](#) allows access to government systems by staff of other organizations if there is a clear business need for the services, and the individuals are contracted by or acting as an agent for a ministry.

### Acceptable use of Internet and e-mail

Instant messaging, like any other Internet tools, falls within the recently updated policy on the [Use of Government of Alberta Internet and E-Mail](#). GoA employees should be reminded and educated of the risks and proper use of instant messaging. The policy describes the conditions of use by Alberta government employees of both the Internet and e-mail. Key components of this policy are:

- Authorized users of government systems are encouraged to use these systems and tools to fulfill their employment duties and to support their ministry's business goals.
- Personal use of systems is permitted, provided the use is consistent with professional conduct, does not detract from the performance of employment duties, and is not used for personal financial gain.
- Users must not bring disrepute to the Government of Alberta.
- Use of the network must not conflict with responsibilities outlined in the [Official Oath of Office](#) and the [Code of Conduct and Ethics for the Public Service of Alberta](#).
- Users must not violate applicable laws and are expected to use discretion and good judgment when using systems.
- All users, including remote access users connecting to government systems through the Internet, must take reasonable precautions to safeguard government systems and not to cause damage to government systems.

## Transmission of personal information via e-mail

The [Government of Alberta Policy for the Transmission of Personal Information via Electronic Mail and Facsimile](#) was adopted by Deputy Ministers in September 2001 and later updated in July 2002 to include implementation guidelines for ministries.

Any instant messaging outside a ministry's network (or the GoA domain) will be using the Internet for transmission (like electronic mail). Thus, this policy is also applicable to instant messaging.

The policy states that any documentation or records containing personal information must not be transmitted by electronic mail or facsimile unless

- personal identifiers have been removed;
- the message is encrypted in such a way that the message sender and recipient can both be authenticated; or
- other means are employed by both the sender and the recipient to ensure confidentiality is maintained.

## Managing instant messages as records

In addition to these policies, various statutes and regulations affect the management of instant message records.

Messages created or compiled on, or sent or received on Government of Alberta systems are records of the government. These records:

- are the property of the Government of Alberta;
- must be managed according to the provisions of the [Records Management Regulation](#) and any records management policies, standards and procedures issued by the Alberta Records Management Committee (ARMC) and Alberta Government Services (the ministry responsible for the Government's records management program);
- are bound by the [Historical Resources Act](#) which ensures the permanent preservation of government records of archival value so that they are available to Albertans in the future;
- are subject to both the access provisions and the protection of privacy provisions of the [Freedom of Information and Protection of Privacy Act](#); and
- can contain personal health information and as such may be bound by the [Health Information Act](#) which governs the collection, use and disclosure of health information, how health information must be handled and protected, and the right of individuals to access their own health information in the custody or under control of custodians as defined under the Act, including the Ministry of Health and Wellness. The Act does not apply to health records retained by other ministries.

Ministries are responsible for collecting, creating and capturing records that adequately and properly document their organization's:

- functions;
- policies;
- decisions;
- procedures;
- resource expenditures;
- operations; and
- delivery of services.

Ministries are also responsible for storing, organizing and retaining these records in such a way that they are available for:

- planning and decision-making;
- program and service delivery;
- meeting their obligations to the Legislature to account for their activities, including audits where applicable;
- meeting requests for access to government records by the public, business and other external groups; and
- recovery and business resumption in cases of emergencies or disasters.

Like other records, instant messaging records must be managed to meet these requirements.

## 4. Establishing Ministry Policies and Guidelines for Instant Messaging

Given the risks associated with public instant messaging services and the legal requirements of ministries for recordkeeping and the protection of personal information, ministries should develop clear policies and guidelines related to the use of instant messaging.

Ministries should address the following issues in their design of instant messaging policies and guidelines:

- acceptable use of instant messaging services;
- appropriate content for instant messages;
- responsibilities for managing records of instant messages;
- transmission of personal information via instant messaging;
- storage of government information on non-government equipment that may have instant messaging services loaded on them;
- appropriate style and effective use of instant messages in the context of government business; and
- procedures for capturing instant messages as complete records.

As with any new policy and associated guidelines, ministries will also want to develop a communications plan for the policy and an education and training program on the policy and guidelines.

### Acceptable use of instant messaging services

The policy should clearly define its scope – what services are acceptable (e.g., public instant message services, third-party instant messaging services, self-hosted services and text-messaging) and what devices the policy applies to – government computers, non-government computers, mobile phones and PDAs.

There are two aspects of acceptable use of instant messaging to consider – the use of public instant messaging services in conducting government business and the personal (non-business) use of instant messaging.

### *Use of public or third-party messaging services*

Ministries will want to consider, based on a risk assessment, whether to allow use of public instant messaging services.

**Business use:** While ministry and GoA firewalls and virus protection mitigate many of the risks associated with these services, there continue to be risks of business messages outside the ministry (sending messages to non-government personnel) or using public services for conducting government business (e.g., on a notebook or home computer). The most restrictive policy would be to prohibit employees from using public or third-party hosted services (that is, only services hosted by the ministry would be allowed) for business. A somewhat less restrictive policy would be to allow employees to use public services for business, but only for conversations that are transitory in nature and not for file transfer or decision-making.

**Personal use:** Ministries will also need to define the degree to which instant messaging can be used for personal use. For example, a ministry may allow personal use of public instant messaging services as long as it does not interfere with staff productivity, or affect any other business activities. Or, a ministry may itemize specific types of personal uses that are prohibited. Examples of prohibited personal uses may include chain letters, commercial or personal advertisements, solicitations, and political materials. The GoA policy on the acceptable use of the Internet identifies the types of use and content that are prohibited.

### *Use of self-hosted instant messaging services*

**Business use:** Many ministries have adopted instant messaging for use within the ministry. In these cases, the security risks associated with public messaging services have been mitigated. However, the conduct of business using self-hosted services will require the capability of capturing official government records and managing them according to the appropriate retention and disposition schedule. If the ministry's messaging system is integrated with its electronic information management (EIM) system such that users are able to classify records and manage them throughout their life cycle (based on the content of the message), then business use of these systems is appropriate. If ministries do not have the capability to capture and manage official instant messaging records, then self-hosted instant messaging systems should only be used for business communications that are transitory in nature.

**Personal use:** Ministries may want to allow personal use of self-hosted instant messaging systems. However, in some cases, public and self-hosted instant messaging systems have the ability to share information such as contact lists, files or even messages themselves. In these cases, actions **must** be undertaken to preserve the integrity of the ministry's systems. These actions would include the requirement



that business contact lists and personal contact lists be kept separate and locking desktops to prevent the installation of public instant messaging programs (and requiring employees to use the only the self-hosted system).

## Appropriate types of content for instant messaging

Providing guidance to employees about what to use instant messaging for will depend on the decisions made around appropriate use of instant messaging services.

If your ministry is using a **self-hosted service**, but does not have the capability of capturing official records, then conversations should NOT include information that is a record of decision-making or anything that would constitute an official record. In these cases, messages should contain only content that is transitory in nature. In these cases, any conversation that includes decision-making, should be followed-up with an e-mail or other documentation.

If your ministry is able to capture official records (and manage these records according to government recordkeeping requirements) then instant messaging can be used for decision-making and the conduct of government business.

If your ministry allows the use of **public** instant messaging services, then the following guidance would be useful for employees about what to use instant messaging for and what NOT to use instant messaging for:

<b>Use</b>	<b>Do NOT Use</b>
✓ Casual conversations; informal chat and questions	✗ Sensitive information or content (including file transfer, where the content is personal or sensitive)
✓ Substitute for phone-calls and e-mail regarding routine matters where business decisions are not made	✗ Conversations where there is a need for documentation
✓ Exchange of technical information	✗ Conversations where there is a need to maintain authentic evidence.

## Managing instant messaging records

The government's [Official and Transitory Records: A Guide for Government of Alberta Employees](#) includes a more detailed description of the various categories of government records and requirements for managing them. The categories that relate most to instant messages are:

- **Official Records:** This includes instant messages containing information that is required to support business operations, to document or provide evidence of business transactions, is required by legislation or to protect the rights of citizens and the government, to provide evidence of compliance with accountability or other business requirements, or has some future business, financial, legal, research or archival value to the government and people of Alberta. These messages must be managed within the ministry's recordkeeping system.
- **Transitory Records:** This includes instant messages containing information that is either of no importance or value to a ministry, or that is only of immediate or short-term use and has no future value. This category would include personal messages and announcements that are not related to the conduct of ministry business. These messages should be routinely deleted as transitory records.

Regardless of whether the ministry allows use of public services or whether use is limited to a service hosted by the ministry, government recordkeeping requirements still apply. Instant messages that contain official information are considered government records and therefore must be captured in a recordkeeping system so their life cycle can be managed according to an approved retention and disposition schedule. Those that do not contain official information should be considered transitory information and deleted from the system.

Ministries will need to outline how instant messages will be managed to meet government FOIP and recordkeeping requirements. These guidelines would cover such things as:

- how the instant messages will be captured as records – how they can be captured in an electronic information management (EIM) system and managed according to the appropriate retention and disposition schedule (based on the content of the message);
- who is responsible for capturing the message as a record – will it be the initiator of the thread, the person that ends it or will someone be designated to capture the thread;

- the need to delineate where the record will begin and end – as instant message conversation are open and can go on indefinitely, everyone must understand and agree on the boundaries of these instant message as records;
- the issues surrounding mixed-threads (conversations) which contain multiple topics and how these messages will be managed – either with a practice of one-topic conversations or through a procedure to register a thread with multiple topics in multiple files;
- and the requirements around handling instant messages that have been captured (and therefore in the custody and control of the ministry) when an access request under the *Freedom of Information and Protection of Privacy Act* (FOIP) has been received – that messages are not to be deleted and instant messages responsive to the request must be included in the review and response.

## Transmission of personal information via instant messaging

Like e-mail, personal information (other than the names of the conversation participants or sender/receiver, of course) should not be transmitted, including file sharing, via instant messaging unless it is adequately protected. It is good practice never to send sensitive personal information via instant messaging if a public or third-party service is being used. Even if the ministry hosts the messaging service, if personal information is sent external to the ministry, it will be transmitted via the Internet. Because privacy cannot be guaranteed, confidential and other sensitive information must not be sent via instant messaging without using a security solution approved by the ministry and that meets the GoA standards for the transmission of personal information outside of a ministry system.

## Storage of government information on home computers

Most home computers have public instant messaging services on them. Therefore, ministries will need to provide guidance to employees as to what, if any, government information should reside on home computers. Sensitive information, stored on home computers, is subject to corruption and theft when public instant messaging services are used. If the home computer does not have adequate firewall, spyware and virus protection, this risk increases to an unacceptable level.

If home computers are to be used for work and also contain instant messaging software, users need to understand that additional measures must be taken to secure the computer and protect the information stored on it – such as ensuring that instant messaging is not activated when working on government work or removing all

government records when finished. The actions to be taken may even need to be extended to removing the public instant messaging software or partitioning it on a separate part of the computer.

## Appropriate style and effective business use

Instant messaging can be a valuable business tool. However, as with other tools, guidelines to help employees use the tool effectively and mitigate risks will be needed. Some examples of these guidelines are:

- **Style.** Instant messaging, like e-mail, is a business tool and as such users should employ a style of writing that is business-like and does not include the often-used abbreviations, emoticons and slang often used in personal instant messaging.
- **User names.** Pseudonyms like “HotPants” or “BankRobba,” “or RobertGold0123™” which may be an accepted in personal instant messaging, are unacceptable in the business situation. Users should only use their real name and GoA email address.
- **Encryption.** Employees will need to know what encryption services are available in the ministry to protect sensitive information and how to use them.
- **Managing contacts.** Guidelines will be needed on how to manage personal and business contacts separately and accepting invitations to be added to contact lists.

## Conclusion

By developing a clear policy and guidelines, ministries can mitigate risk, support the effective use of instant messaging as a business tool, and ensure use of instant messaging is consistent with legislative and policy requirements.

## Appendix 1: Model Policy and Guidelines for Instant Messaging

This section contains an example of ministry policy and related guidelines for instant messaging. Based on their business needs, ministries may want to implement alternate (or additional) policy statements and guidelines.

### Policy

#### *Scope*

This policy applies to all employees, contractors, vendors and agents (i.e., “users”) who have access to [insert ministry name] instant messaging system.

This policy applies to desktops, notebooks, home computers where ministry business is transacted, and all portable devices (e.g., PDAs and mobile phones) with instant messaging capability.

#### *Authorized services*

- Users will only use [insert ministry name] authorized instant messaging services.
- Downloading of public instant messaging software (e.g., MSN, Yahoo!, AOL) on government-owned computers and other devices is prohibited.

#### *Acceptable use*

- Users will use instant messaging to fulfill their employment duties and to support the ministry’s business goals.
- Personal use of instant messaging is permitted, provided the use is consistent with professional conduct, does not detract from the performance of employment duties, and is not used for personal financial gain.
- Users must not bring disrepute to the Government of Alberta.
- Use of instant messaging must not conflict with responsibilities outlined in the [Official Oath of Office](#) and the [Code of Conduct and Ethics for the Public Service of Alberta](#).

- Users must not violate applicable laws and are expected to use discretion and good judgment when using instant messaging services.
- All users, including remote access users connecting to government systems through the Internet, must take reasonable precautions to safeguard government systems and not to cause damage to government systems.
- [insert ministry/branch name] may initiate investigations of instant messaging as warranted.

### ***Recordkeeping requirements***

Instant messages created or compiled on, or sent or received on Government of Alberta systems are records of the government. These records:

- are the property of the Government of Alberta;
- must be managed according to the provisions of the [Records Management Regulation](#) and [insert ministry name] records management policies, standards and procedures.

All instant messages that are official records must be captured in the [insert ministry name] records management system and managed throughout their life cycle.

[**Note:** This assumes the ministry has integrated instant messaging into an electronic information management (EIM) system. If not, users should be told to use instant messaging only for conversations that are transitory in nature and not a record of government business.]

### ***Roles and responsibilities***

Messages sent to, or received by, and retained in [insert ministry name]'s instant messaging system are in the custody and control of the department. Therefore, instant messages are subject to the access and privacy rules of the *Freedom of Information and Protection of Privacy (FOIP) Act* and must be managed according to the Records Management Regulation. Individual users are responsible for managing the messages in the instant messaging system according to the rules set out in legislation, GoA and department policies and related procedures:

Users will assume responsibility for instant message records as follows:

- The person who starts an instant message conversation must manage the record.

- If instant messages are received from outside the ministry, the recipient of the message from outside of the ministry must manage the record or the conversation.
- Messages should, if possible, be kept to one topic. This will simplify managing the record of the conversation. If an instant message conversation contains more than one topic, the message will need to be filed on all pertinent files.

Business unit managers may establish rules or processes, or assign responsibility, for managing instant messages within their unit.

### ***Monitoring of instant messages***

[Insert Ministry Name] will not monitor instant messages unless there is cause to do so under the policy on Use of Government of Alberta Internet and E-Mail.

### ***Review process***

This policy will be reviewed yearly or earlier, if necessary. The policy has been approved by [insert position title].

## **Guidelines<sup>2</sup>**

### ***Names***

Users should only use their actual name and GoA e-mail address. Users should NOT adopt pseudonyms or aliases.

### ***Contact lists***

Business and personal contact lists should be managed separately. [insert procedure]

Do NOT accept being added to a contact list unless you can verify the identity of the person making the invitation.

### ***Style***

Users will employ a style of writing that is business-like and does not include the often-used abbreviations and emoticons used in personal instant messaging.

---

<sup>2</sup> These guidelines are examples of areas where employees will need guidance. Each will need to be accompanied by procedures the ministry will use in its particular records, systems and information management environment.

### ***Forwarding messages***

Users will not forward business-related messages to public messaging systems.

Personal contact lists from outside instant messaging systems should NOT be imported.

### ***Managing official records***

Users will file instant messages that qualify as official records in the electronic information management system. [insert ministry procedure]

Users will delete unneeded transitory instant messages on a regular basis.

### ***Security***

If a user is working on a home computer that has instant messaging capability, make sure instant messaging is “offline” or closed while working with government documents. Remove government documents from the computer when finished.

If users leave their desk they should set their status to offline. It is also a good idea to set your instant messaging settings to automatically switch to “away” after a period of inactivity.

### ***Privacy***

Messages containing personal information must not be transmitted outside of the ministry by instant message unless

- personal identifiers have been removed;
- the message is encrypted in such a way that the message sender and recipient can both be authenticated; or
- other means are employed by both the sender and the recipient to ensure confidentiality is maintained.

[Insert recommended ministry procedure.]

### ***FOIP and litigation***

If the ministry receives a FOIP request or becomes involved in litigation, users must not delete any instant messages related to the request until advised by the FOIP coordinator or the ministry’s solicitor that the request or the legal action is complete.



## Appendix 2: Resources

### 1. Introduction

This guide contains resources selected to support the development of standards and practices related to instant messaging in the Government of Alberta.

### 2. Standards

#### *2.1 American National Standards Institute*

##### **Requirements for Managing Electronic Messages as Records (ANSI/ARMA 9-2004)**

<http://www.arma.org/bookstore/productdetail.cfm?ProductID=1499>

Approved by the American National Standards Institute as an ANSI standard on October 7, 2004, this publication defines requirements for developing a corporate policy for managing information content in any type of text-based electronic message or communication such as e-mail or instant messaging. It also includes recommended provisions for an electronic message records management policy useful throughout the life cycle from message creation to final destruction or disposition.

#### *2.2 International Standards*

##### **International Standard ISO 15489 – Part 1: Information and Documentation – Records Management: General**

<http://www.arma.org/bookstore/productdetail.cfm?ProductID=1187>

This ISO standard was developed to standardize international best practice in records management. It provides guidance on managing records of originating organizations, public or private, for internal and external clients to ensure that adequate records – in all formats and media – are created, captured and managed.

## **International Standard ISO 15489 – Part 2: Information and Documentation – Records Management: Guidelines**

<http://www.arma.org/bookstore/productdetail.cfm?ProductID=1188>

The international records management standard, ISO 15489-1, specifies the elements of records management and defines the necessary results or outcomes to be achieved. This technical report, ISO/TR 15489-2, is supplementary to the standard, providing further explanation and a methodology for implementation of the standard. Both ISO 15489-1 and this technical report apply to records in any format or media, created or received by any public or private organization during the course of its activities.

## **2. Government Information**

### **Alberta Infrastructure Instant Messaging Pilot with Infrastructure HR**

Accessible through SHARP (for GoA employees only)

<https://www.sharp.gov.ab.ca/secure/DocDisplay.cfm?DocID=4573>

Results from a small pilot study concerning the use of MSN Messenger in the Government of Alberta. The pilot was conducted September – October 2003.

### **Alberta Infrastructure Instant Messaging: The New Business Tool**

Accessible through SHARP (for GoA employees only)

<https://www.sharp.gov.ab.ca/secure/DocDisplay.cfm?DocID=4240>

This document written by Alberta Infrastructure provides recommendations about instant messaging adaptation in the GoA.

### **Information Security Forum (ISF) Securing Instant Messaging - Research Report**

Accessible through SHARP (for GoA employees only)

<https://www.sharp.gov.ab.ca/secure/DocDisplay.cfm?DocID=4963>

ISF research report concerning many aspects of instant messaging.

**Information Security Forum (ISF)  
Securing Instant Messaging - Security Control Checklist**

Accessible through SHARP (for GoA employees only)

<https://www.sharp.gov.ab.ca/secure/DocDisplay.cfm?DocID=5007>

Security Control Checklist from the ISF “Securing Instant Messaging-Research Report”.

### 3. Other Government Documents

**State Records, New South Wales, Australia  
Managing the Message Guidelines**

<http://www.records.nsw.gov.au/publicsector/rk/guidelines/message/make.htm>

Strategies for making sure that adequate records of messages (including instant messaging) are made.

### 4. Research Documents

#### ***4.1 ARMA International***

**ARMA International  
E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal  
Issues (Online course)**

<http://216.197.111.111/learningcenter/onlinecourses/courselisting.cfm?CourseID=20>

Course covers instant messaging as records from a legal perspective, examples of messaging restrictions and guidelines in the United States and worldwide, and considerations for policies for managing messaging data.

**ARMA International  
Got IM? Management, Security, Archiving and Compliance for Instant  
Messaging**

<http://216.197.111.111/learningcenter/webseminars/archive.cfm>

In this web seminar (for ARMA members only), learn about the explosive growth of instant messaging in companies and the challenges created by this growth for IT and Records Management Professionals.

**ARMA International**

**Instant Messaging: A Boat Records Managers Can't Afford to Miss!**

<http://216.197.111.111/learningcenter/webseminars/archive.cfm>

This web seminar (for ARMA members only) highlights the records management issues surrounding instant messaging as well as the strategies records managers can use to position themselves as the instant messaging experts within the organization.

**ARMA International**

**Instant Messaging: The Perfect Storm**

(Streaming video and CD)

<http://216.197.111.111/bookstore/productdetail.cfm?ProductID=1448>

This session from ARMA's 2003 post-conference seminar in Boston deals with controlling and managing instant messaging on company systems.

**ARMA International**

**Instant Messaging and Regulatory Compliance**

<http://www.arma.org/pdf/conference/sessions/Cisco.pdf>

This session from ARMA's 2004 conference seminar in Long Beach deals with how instant messaging technology works and an approach for developing a practical, prudent, and consistent policy for managing instant messaging that is responsive to regulatory requirements and an organization's corporate culture.

***4.2 ePolicy Institute***

**ePolicy Institute**

**2004 Workplace E-mail and Instant Messaging Survey**

<http://www.epolicyinstitute.com/survey/survey04.pdf>

Survey of instant messaging use in American businesses.

**ePolicy Institute**

**Instant Messaging Rules (book)**

[www.epolicyinstitute.com](http://www.epolicyinstitute.com)

This book, written by ePolicy Institute Executive Director Nancy Flynn, includes the chapter "32 IM Rules: Best Practices to Keep You In Business and Out of Court".

### ***4.3 Forrester Research***

#### **Forrester Research Adopt Enterprise IM Or Go To Jail**

<http://www.forrester.com/ER/Research/Brief/Excerpt/0,1317,32907,00.html>

Firms have deferred institutionalizing instant messaging long enough. Widespread rogue instant messaging adoption and new regulations like Sarbanes-Oxley make further delay a recipe for disaster.

#### **Forrester Research Consider a Single Solution for E-Mail and Instant Message Archiving and Compliance**

<http://www.forrester.com/Research/LegacyIT/Excerpt/0,7208,29182,00.html>

An important evaluation criterion when choosing an e-mail archiving or compliance solution that supports instant messaging is whether messages are stored in the same repository as e-mails, attachments and other forms of content.

#### **Forrester Research Evolving Toward Enterprise Instant Messaging**

<http://www.forrester.com/Research/LegacyIT/Excerpt/0,7208,27264,00.html>

Real-time communication with awareness will become a mission-critical business tool by the end of 2004, with instant messages surpassing e-mail traffic by 2006. Organizations should deploy secure auditable enterprise instant messaging.

### ***4.4 Gartner Research***

#### **Gartner Research The Coming Revolution in Real-Time Collaboration**

[http://www.gartner.com/DisplayDocument?ref=g\\_search&id=395786](http://www.gartner.com/DisplayDocument?ref=g_search&id=395786)

Web conferencing and instant messaging are increasingly being used in enterprises to enable people to communicate, collaborate and learn in real time. This document reviews how real-time collaboration will change the way people work and learn.

**Gartner Research****Free Instant Messaging: Taming the Wild Beast**

[http://www.gartner.com/DisplayDocument?ref=g\\_search&id=338764](http://www.gartner.com/DisplayDocument?ref=g_search&id=338764)

Free instant messaging services provide satisfactory reliability for ad hoc employee collaboration, but aren't strong enough for revenue or customer-satisfaction dependent interactions. This document presents guidelines for moving to business strength instant messaging.

**Gartner Research****Location and the Future of Interpersonal Messaging**

Accessible through SHARP (for GoA employees only)

<https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=5277>

This document explores how mobile device features complement or conflict with current instant messaging applications and services.

**Gartner Research****Public IM Clients Provide Challenges for FSPs**

Accessible through SHARP (for GoA employees only)

<https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=5275>

This document examines the architecture models and technologies that will enable Financial Service Providers (FSPs) to adapt to major industry trends in communication tools.

***4.5 META Group Research*****META Group Research****Instant Messaging Considerations**

<http://www.metagroup.com/us/displayArticle.do?oid=32519>

Organizations are increasingly using instant messaging systems without appropriate user policies, security, or management practices. Companies must address instant messaging shortcomings, or they will face system outages, compliance issues, and unauthorized disclosure of sensitive data.

#### ***4.6 National Association of Securities Dealers (NASD)***

##### **National Association of Securities Dealers (NASD)**

##### **Notice to Members: Clarification for Members Regarding Supervisory Obligations and Recordkeeping Requirements for Instant Messaging**

[http://www.nasd.com/web/groups/rules\\_regs/documents/notice\\_to\\_members/nasdw\\_003249.pdf](http://www.nasd.com/web/groups/rules_regs/documents/notice_to_members/nasdw_003249.pdf)

This NASD document clarifies for members their supervisory obligations and recordkeeping requirements with respect to instant messaging.

#### ***4.7 Osterman Research***

##### **Osterman Research**

<http://www.ostermanresearch.com/research.htm>

This company's web site contains a variety of instant messaging surveys conducted by Osterman Research.

#### ***4.8 The Information Management Journal***

##### **Patrick J. Cunningham, "IM: Invaluable New Business Tool or Records Management Nightmare?"**

Order this article through the ARMA international web site.

<http://www.arma.org/bookstore/productdetail.cfm?ProductID=1398>

If businesses and technology partners can shore up all the potential security risks and recordkeeping challenges, instant messaging could become a valuable communications tool for millions of corporate users. (The Information Management Journal; PDF download; English; 6 pages; November/December 2003, Vol. 37, No. 6; Copyright ARMA International, 2003.)

##### **Tracy Caughell, "The Corporate Records Conundrum"**

Order this article through the ARMA international web site.

<http://www.arma.org/bookstore/productdetail.cfm?ProductID=1318>

E-mail is striking fear into the hearts of many in the records management world because they can haunt an organization for years and provide damning evidence that may result in expensive fines and settlements. Increasingly, companies are being forced to more effectively manage their e-mail and even integrate the technology into their overall records management program to reduce the risk. How companies

handle e-mail records should shape their retention policies for voice mail and instant messaging. (The Information Management Journal; PDF download; English; 4 pages; May/June 2003, Vol. 37, No. 3; Copyright ARMA International, 2003.)

**John C. Montana, “E-mail, Voice Mail and Instant Messaging: A Legal Perspective”**

Order this article through the ARMA international web site.

<http://www.arma.org/bookstore/productdetail.cfm?ProductID=1450>

The use of e-mail and voice mail has become ubiquitous worldwide. More recently, instant messaging has achieved a similar status. Many businesses are dependent on these technologies as a means, or even as a primary means, of communication with others. But these business tools pose many challenges for records managers. An organization that uses messaging faces a legal landscape that urges, if not demands, a rational policy for managing messaging data. (The Information Management Journal; PDF download; English; 4 pages; January/February 2004, Vol. 38, No. 1; Copyright ARMA International, 2004.)