

Thirty-Two Instant Messaging Rules: Best Practices to Keep You in Business and out of Court

IM Rule #1: Instant Messaging Is a Form of E-Mail—Written Correspondence That Creates a Written Record.

Instant messaging is a form of turbocharged e-mail. It combines the real-time convenience and conferencing capabilities of the telephone with all the features of e-mail—and then some. As a form of e-mail, IM creates a written business record that can be subpoenaed and used as evidence in litigation or regulatory investigations. Adherence to a strategic IM management program, complete with written rules and policies, is a legal and business necessity for any organization that allows employees to use IM.

IM Rule #2: Take Control of Instant Messaging Risks Today, or Face Potentially Costly Consequences Tomorrow.

Employers who mistakenly view IM as an “emerging” technology can no longer afford to remain in the dark about employees’ IM use. Instant messaging is here, and here to stay. By 2006, e-mail usage will have declined by 40 percent, thanks to increased IM use.¹ Employers who fail to manage IM today will tomorrow face

legal and regulatory challenges and will have to make decisions that impact employee productivity and company security—that is, potentially expensive decisions.

IM Rule #3: Assume That Your Employees Are Already Using Instant Messaging—Without Your Knowledge, Authorization, Rules, or Policies.

Industry insiders estimate that up to 90 percent of businesses are already engaged in some form of IM.² That includes the 25 million employees who are using personal IM tools to communicate via public networks—without management’s knowledge, IT’s approval, or written rules or policies in place to reduce liabilities.³

IM Rule #4: Originally Intended for Home Use, Instant Messaging Poses Significant Risk to Business Users.

Nationwide, renegade employees have downloaded free personal IM software, or “clients,” from AOL, Yahoo!, and MSN directly onto their business computers, laptops, and handhelds. Without technology in place to prevent security breaches, protect confidential data, battle viruses and spam, monitor and block content, purge unnecessary messages, and retain and archive business records, consumer-grade IM tools put an organization at tremendous risk.

IM Rule #5: Apply Instant Messaging Policy, Training, and Technology Solutions to User ID and Domain Name Challenges.

The misuse of user IDs and the misappropriation of corporate domain names are among the greatest challenges facing the IM industry and users. While technology-based solutions continue to evolve, employers are advised to use policy, education, and software to give their IT department some control over user IDs and passwords, including the ability to reserve their own company and domain name and kick imposters off their system.

IM Rule #6: Unauthorized, Unrestricted Instant Messaging Use Is Simply Bad Practice.

It's not uncommon for employees to use IM without the knowledge of management. Responsible employers have an obligation to discover whether or not employees are using IM, under what circumstances they are using it, with whom they are chatting, and what type of content they are sending and receiving. The risks inherent in unmanaged IM use are too great to ignore.

IM Rule #7: Act Now to Uncover Unauthorized Instant Messaging Use.

To help get a grip on unauthorized IM use, test your network for the presence of consumer-grade IM clients. Also consider conducting an internal survey to determine the level and type of IM communications your employees are engaged in. Your survey findings will help you draft IM policies and develop employee training programs that truly meet the needs of your organization.

IM Rule #8: Ignoring Instant Messaging May Cost You More Than Using It.

In spite of the risks, IM delivers productivity-enhancing features and capabilities that cannot be denied. Use screening technology and your internal IM survey to uncover pockets of nonuse as well as unauthorized use. Educate targeted nonusers about the ways in which IM can help enhance productivity, ease communications, and better meet client needs.

IM Rule #9: Don't Rush to Ban Instant Messaging.

Although banning workplace IM may appear to be a simple and effective solution to IM risk, it may not be so easy to enforce. Employees want IM, and they have demonstrated their willingness to bring it in through the back door, without management's knowledge or IT's approval. Try banning IM completely, and you may trigger a revolt among employees and clients who view it as an effective and acceptable means of high-speed communication.

IM Rule #10: Instant Messaging Productivity Concerns May Be Overblown.

There is considerable debate among employers and users as to whether IM helps or hinders productivity. Before drawing a conclusion one way or the other, review the findings of your internal IM survey. How are your employees using IM? Are they using it primarily for business purposes or personal chat? How upset would your staff—and clients—be if you banned it completely?

IM Rule #11: Don't Rush to Standardize Instant Messaging.

Enterprise IM offers undeniable benefits including antivirus and encryption tools, as well as the ability to control user IDs, monitor content, and save and store messages. On the downside, enterprise systems limit users to internal chat with other people on the same system. Expect some defiant employees to disregard policy and attempt to download personal IM clients for external use—even after your enterprise-grade system is installed.

IM Rule #12: Meet Your Employees in the Middle with Corporate Technology That Supports Personal Instant Messaging Tools.

Server-based gateway technology manages public IM traffic at the discretion of corporate IT. With a gateway product, management can test the network to determine whether consumer-grade clients are being used, control user IDs, monitor use, block content in compliance with policy, retain and store messages, block attachments, and detect viruses among other features. Management maintains control, while employees enjoy instant chat with the outside world.

IM Rule #13: Limit Instant Messaging Access to Employees with a Legitimate Business Need.

Don't assume every employee needs or is entitled to IM access. Before making IM available across the board, consider which em-

employees truly need access to IM for legitimate business purposes. Remember, the greater the use, the higher the cost, and the larger the risk of IM-related disasters.

IM Rule #14: Don't Allow IT (or Legal, Records Management, or Human Resources) to Dictate Your Instant Messaging Management Solution. Work as a Team.

Do not assign the technology department sole responsibility for developing and implementing your strategic IM program. Allow IT to determine how long IM is stored on the system and you may expose your organization to legal challenges from litigators who claim your record retention decisions are driven by technology, not by the law. Instead, have your chief information officer work together with legal, compliance, records management, and HR professionals to develop and implement a strategic IM program—complete with clear retention, deletion, discovery, and litigation response rules—that meets the specific needs of your organization and employees.⁴

IM Rule #15: Instant Messaging Policy, Education, and Enforcement May Provide a Defense Against Vicarious Liability Claims.

Employers may be held responsible for the misconduct of their employees. Known as vicarious liability, this legal principle applies when an employee files a discrimination claim as the result of an offensive instant message sent by another employee. However, if an employer makes reasonable efforts to prevent a hostile work environment through IM policy, training, and enforcement, then the bad acts of one rogue employee may not be attributable to the employer, and the organization may have a defense against sexual harassment or hostile work environment liabilities.⁵

IM Rule #16: Protect Your Organization's Assets, Secrets, and Future by Monitoring Instant Messaging.

IM belongs to the employer, not the employee. Use written policy to notify employees that the computer system as a whole, including

the IM system, the messages, and user IDs, belong to the organization, not the individual. Clarify that the organization has the right to access and review the content of any instant message that is created, stored, transmitted, or received using resources provided by the company. If you allow the use of personal IM clients, let employees know that these messages are subject to monitoring, too.

IM Rule #17: Watch Your Language! Confidential Information and Intellectual Property Can Leave Your System—Instantly.

In the age of IM, just about any document can be sent out of the organization with a click of the keyboard. Establish and enforce an IM security policy, take advantage of technology tools to prevent security breaches, and train employees on the dos and don'ts of protecting confidential information.

IM Rule #18: Notify Employees That They Have No Reasonable Expectation of Privacy—Even When Using Personal Instant Messaging Software.

Use your written IM policy and employee training program to drive home the point that, when it comes to workplace IM, employees have no reasonable expectation of privacy. Let the staff know that management intends to exercise its legal right to monitor IM transmissions, including those sent and received via personal IM tools on public networks.

Rule #19: Use Instant Messaging Policy to Provide Clear Guidelines for Employees' Personal Use.

When it comes to personal use of the organization's IM system, employers have a broad range of choices. You can ban all personal use, allow a limited amount of authorized personal use, permit unlimited personal use, among other options. Whatever approach you select, be sure to clearly define your personal use rules and guidelines in your written IM policy. Be specific. Leave no room for employee interpretation. Make sure employees understand that

usage guidelines apply, regardless of whether the organization's IM system or employees' personal IM clients are used.

IM Rule #20: The Easiest Way to Control Instant Messaging Risk Is to Control Written Content.

By requiring employees to use appropriate, businesslike language in IM, employers can help limit their liability risks and improve the overall effectiveness of the organization's IM system. Use your written IM policy to spell out content guidelines and language rules.

The establishment of your IM policy is a good time to review (and update if necessary) the organization's sexual harassment and discrimination policies. Sexual harassment claims are not new to employers, but the use of smoking gun instant messages as evidence is. Be sure to address sexual harassment and discrimination in your IM content, language, and usage guidelines.

IM Rule #21: Instant Messaging Rules and Policies Should Guide Technology, Not Be Guided by It.

If you have any doubt about your employees' willingness to adhere to IM policy, content guidelines, and usage rules, apply a technology solution to your people problem. Install an enterprise IM system or gateway product that monitors and filters content in compliance with your organization's written rules and policies, and any applicable government or industry regulations.

IM Rule #22: Instant Messaging Creates Business Records. Treat It Appropriately.

Developing the ability to define, identify, and retain business record messages is one of the most important IM management activities you can undertake. IM business records provide evidence and help protect against spoliation problems. IM business records must be retained and preserved based on clearly written and consistently enforced policy.⁶

IM Rule #23: Retain Business Record Instant Messages According to Clear Rules and Written Policies.

Many organizations rely on IM for legitimate business communications and activities. At least some of that IM should be classified as a business record and retained and managed according to written rules and policies. The courts appreciate consistency. If you have a policy of retaining certain paper records for three years, be sure to retain similar IM business records for thirty-six months as well.⁷ You should also familiarize yourself with regulators' retention rules.

IM Rule #24: Retain Only Business Record Instant Messages. Delete Messages That Are Personal or Lack Value as Business Records.

Disposing of old IM, e-mail, and other records when they reach the end of their lifespan ensures old information cannot return to harm you. Have your legal/records management team purge old management records and insignificant, nonbusiness-record messages.⁸

IM Rule #25: Be Strategic. Manage Instant Messaging with Litigation and Regulatory Investigations in Mind.

Manage IM strategically. Combine IM rules and policy with employee education and technology to ensure business record IM is identified, saved, and stored in accordance with business, legal, and regulatory needs and requirements. Your goal is to guarantee you can produce necessary IM and e-mail and to prevent the likelihood of a spoliation problem.⁹

IM Rule #26: Beware: Destroying Instant Messaging Evidence After a Lawsuit Is Filed Is Illegal.

Employees who destroy instant messages and other evidence after they know about a lawsuit or an investigation put the organization

and themselves at risk of civil and criminal penalties. Establish a litigation response team and strategy to ensure that employees hold onto instant messages that are related to a lawsuit or an investigation, and which would normally be disposed of in the course of business.¹⁰

IM Rule #27: You Cannot Hide from Instant Messaging Discovery. Be Prepared.

Use your litigation response plan to ensure that all employees and executives clearly understand the discovery process and the individual roles they play in IM retention and deletion. Use software technology to locate and turn over subpoenaed instant messages in a timely manner.¹¹

IM Rule #28: Training, Training, and More Training.

To be successful, your organization's IM rules and policies must be embraced by all employees, from summer interns to the CEO. Use your training program to address IM risks, rights, rules, responsibilities, and regulations. Stress the fact that complying with IM policy is a requirement, not an option. Enforce policy compliance with a combination of software and discipline.

IM Rule #29: Continuing Education Is Directly Linked to Successful Instant Messaging Risk Management.

Ensure IM policy compliance by implementing a program of continuing education. Do whatever it takes to raise employees' e-consciousness, and keep them focused on their individual roles in making the organization's IM risk management initiative a success.

IM Rule #30: As Wall Street's Use of Instant Messaging Grows, Regulatory Oversight Grows Right Along with It.

Wall Street was an earlier adopter of IM, and its popularity continues to soar. In 2003, the NASD joined the SEC and NYSE in an-

nouncing that all IM communications between brokers and their clients must be retained for a period of three years, just like e-mail and printed correspondence. Thanks to new IM retention regulations, prosecutors and investigators digging into Wall Street scandals and white-collar crime now have a new evidence pool to dive into: instant messages.

IM Rule #31: Install the Right Technology to Ensure Regulatory Compliance.

Regulated firms (and unregulated businesses alike) are advised to install technology that automates the archiving, retrieval, monitoring, purging, and retention of IM in compliance with regulatory guidelines and company policy.

IM Rule #32: Instant Messaging Compliance Impacts a Broad Range of Industries, Not Just Wall Street.

The need to produce IM evidence is not restricted to Wall Street, nor is it limited to litigation. The FDA, the IRS, and other government and industry regulators regularly request copies of, and in-house access to, e-mail and other electronic records. Expect to start receiving requests for IM—if you haven't already.

If you are unclear on which government and industry regulations govern your industry and your employees' use of IM, now is the time to find out. Your legal, compliance, and IT professionals should work together to determine where IM fits into the organization's regulatory puzzle, and how a program that combines written policy, employee education, and enforcement technology (the three Es of IM risk management) can help ensure compliance and minimize costly IM-related disasters.