

---

# **The Real Estate Agent's Guide to Protecting Real Estate Information**



**Version 1.0**

**November 2004**

# The Real Estate Agent's Guide to Protecting Real Estate Information

## 1. Executive Summary

Consumers trust real estate practitioners to play a vital role in managing their largest single purchase and most important financial investment. Consumers also trust practitioners with information about their properties, financial qualifications and purchasing intentions.

*Agents need new management tools and technologies to better control and protect information.*

Protecting all forms of real estate information has become increasingly difficult because digital information can be so easily copied, stolen, destroyed or maliciously altered. The pervasive use of the Internet makes it possible for digital information to be transferred to many organizations without an agent's or broker's knowledge. All practitioners need new management tools and technologies to protect the information of brokers and their trading partners.

Practitioners should implement the following essential information security practices to comply with existing and future regulations and minimize exposure to liability and business disruption:

Agent Essential Information Security Practices	
1	Authenticate the identity of any party with whom you share or exchange information.
2	Label sensitive and proprietary information as company confidential in accordance with company policy.
3	Always secure client and company confidential documents.
4	Disclose the company's "standard of care" to clients and prospects.
5	Contact company officials whenever a security breach is suspected.
6	Never download any files or attachments you are not expecting.
7	Install personal firewall and virus-scanning software on personal computers.
8	Regularly back up business information according to company procedures.
9	Change personal passwords and other access codes every 90 days or more frequently in accordance with company policy.
10	Take company-specified steps to protect company information from unauthorized access, alteration, destruction, modification or disclosure.

This document provides additional guidelines that will assist agents to further reduce their risks and meet a higher standard of consumer trust.

## 2. Authenticating Identity

An agent’s personal safety and the security of company information starts by establishing the identity of (authenticating) the people you are dealing with. Agents understand the importance of making a copy of the driver’s license of an individual not known to them before visiting a property. Similarly, it is important to establish the identity of any individual before exchanging digital information in an online interaction.

Agents should take special care to never download any files or open any e-mail attachments they are not expecting. These files may contain a virus or include other forms of malicious software that can damage a company’s systems. Consider verifying the phone number or e-mail address of any individual before exchanging listing or other information.

## 3. Disclosing the Standard of Care

*Disclose the standard of care your company will apply to any personal or sensitive business information.*

Agents are involved with many disclosures in the course of their business. Agents should disclose to clients and prospective clients the company standard of care that will be applied to any personal or sensitive business information.

Disclosure Best Practices	Assessment
Agents should not collect or store any information not directly related to a real property transaction unless authorized by the consumer.	
Agents should inform consumers if their information may be used for statistical analysis or marketing purposes beyond their specific transaction.	
Agents should obtain the permission (opt-in) of consumers prior to initiating e-mail or telephone communications and collecting information from them.	
Agents should take reasonable steps to protect consumer information from unauthorized access, alteration, destruction, modification or disclosure.	
Agents should hold brokers, MLSs and other trading partners accountable for the proper handling of information.	

These disclosures should be published on an agent's Web site, should include links to the Realtor® Code of Ethics, and should identify the agent as well as the broker and any affiliate relationships.

## 4. Labeling Sensitive Information

Many forms of company information are especially sensitive and should always be labeled as confidential and, in some cases, secret. Some of the information related to a specific property or inventory information is widely available to the public. However, specific remarks, compensation terms, client contact information and addresses should be handled as confidential. Virtual tours and interior pictures should also be regarded as confidential. Access information, such as pass codes to lockboxes and passwords to information systems, should always be labeled and handled as secret.

Company information that profiles a buyer or seller or identifies purchasing interests or other attributes should also be categorized and labeled as confidential. This information may be very valuable to others and subject to theft. Social Security numbers, financial qualifications, credit information and data related to a consumer transaction should always be regarded as secret and subject to the highest level of protection.

Company business information such as financial records, market research and prospect lists should also be categorized as confidential or secret.

## 5. Keeping Personal Information Private

According to the National Association of Realtors® Code of Ethics, "Realtors® shall not knowingly use the confidential information of clients for the Realtor's® advantage or the advantage of third parties." Agents should ensure that the personal information of clients, employees and contractors that is in the agent's possession is never disclosed without their written consent.

Many forms of personal information are subject to specific federal, state and international regulation. The name, telephone number, address and e-mail address of consumers captured by agents should never be

*Many forms of personal information are subject to regulation.*

inadvertently disclosed to third parties without the approval of the broker. In some cases, agents may also create electronic files that include financial history, Social Security number and purchasing intention. Agents should employ technical solutions such as encryption to ensure that this personal consumer information remains private.

## 6. Involving Your Trading Partners

Agents exchange information with a wide variety of trading partners including agents and brokers with other firms, MLSs, appraisers, title companies, and loan origination and settlement services firms. Sensitive business information that is shared between trading partners should be subject to a confidentiality or nondisclosure agreement (NDA). Agents should ensure that all parties to a transaction take steps to adequately protect the sensitive information they create or obtain. These practices include the following:

Information Exchange Best Practices	Assessment
Identify information the broker considers confidential or secret.	
Identify what sensitive information is received from trading partners.	
Understand the standard of care your company and trading partners will apply to your company's information.	
Disclose your company's standard of care to trading partners.	
Enter into confidentiality agreements drafted by legal counsel with any organization that has access to Realtor® information systems.	
Ensure that current license agreements exist for all software programs installed on the company's owned and operated systems.	

*Digital information is most vulnerable to unauthorized copying, repackaging and theft.*

The rights of trading partners to use or repurpose company information should be defined at the time the information is created. The rights associated with many forms of company information, such as newspaper advertisements or listing publications, should be described on any documents or published materials.

Digital information is most vulnerable to unauthorized copying, repackaging and theft. It is especially important that agents ensure that they do not violate copyright protections for any digital information used in the course of business.

## 7. Securing Sensitive Information

*Agents should change the password on their systems at least every 90 days.*

Many forms of company information continue to exist on paper that must be physically secured. Access to prospect and customer lists, research, contracts and transaction documents must be tightly controlled and restricted to those who have a business need to know. Sensitive information stored on paper and computer media should reside in suitable locked cabinets or other secure furniture when not in use, especially outside working hours. Critical company business information, such as contracts and customer records, should be locked away (ideally in a fire-resistant safe or cabinet) when not required, and especially when the office is vacated.

Key locks and passwords should be used to protect personal computers, notebooks, laptops and terminals. Displays should be locked and obscured through screen savers that lock when not in use. Agents should change the password on their systems at least every 90 days, and the password should be a minimum of eight upper- and lowercase characters. Agents should never share, post or publish a password or authentication token with anyone at any time without express management approval.

Any attempt to tamper with or gain access to company or other systems or information files by an unauthorized individual should be reported to the broker, MLS or third-party service provider immediately.

Improperly installed or configured wireless access points are a major security vulnerability, potentially exposing all of your e-mail and Web communications to public view. If the access point is installed in an office, it could potentially expose all of the information resources in that office to public view. You should not install wireless access points in your home without proper technical assistance, and you should never install a wireless access point in your office without the authorization of your broker or office security manager.

Treat all communication sent through a public wireless access point ("Wi-Fi hot spot") as visible to the public unless you are using a virtual private network (VPN).

## 8. Technology

Agents have several technical solutions they can employ to reduce the risk to company information. Agents should consider several mature technologies to prevent unauthorized access and use. Agents should also discuss these solutions with their broker to ensure compatibility with the broker's systems.

Technology Best Practices	Assessment
Install personal firewall software on personal computers.	
Install and update virus-scanning and protection software.	
Utilize a secure virtual private network (VPN) whenever possible.	
Encrypt sensitive digital files.	

The Center for Realtor<sup>®</sup> Technology can assist agents with selecting commercial off-the-shelf technologies and qualified service providers to meet these needs. The Realtor<sup>®</sup> Secure Program features services from a range of providers who will test your Web site for vulnerabilities. These and other active measures will help ensure that Realtor<sup>®</sup> organizations can reduce liability and sustain a high level of consumer trust.

## 9. Responding to an Event

The effective implementation of best information security practices can prevent or reduce serious business losses or disruption. Despite an organization's best efforts, security breaches and incidents will occur. These events can be the result of natural disasters, accidental damage, sabotage, equipment failure, or loss of supplied services or utilities. A business continuity plan should help minimize the disruption to the agent's business and the potential for business loss.

The cornerstone of this plan is ensuring that critical business documents and a current version of any electronic media and software have been securely stored off-site, away from your place of business. Agents should coordinate their business continuity plans with their brokers.

## 10. A Community Responsibility

The Internet created a major shift in the way real estate practitioners collect and make listing information available to consumers. The next major shift will affect how all forms of real estate information are protected and controlled. The need for practitioners to preserve consumer privacy, protect critical business information and control the point of sale will continue to grow. Supporting industry efforts to remain as the “trusted” first point of consumer contact requires that agents continue to work to improve information security procedures and technology protections.

*All practitioners have a vital role to play in the evolution of the industry's information security infrastructure.*

Though industry business models, participants, regulation, threats and technology will continue to change, information security will remain a mandatory requirement at the center of the real estate transaction process. Sensitive information will be shared electronically between an ever-growing set of devices and organizations. Brokers will invest in technologies that provide for more efficient transactions. Greater convenience and service quality must also include preservation of consumer privacy and control of company information.

All practitioners have a vital role to play in the evolution of the industry's information security policy, practices and protection infrastructure. Real estate is an interconnected industry where the security of all systems and companies can be compromised by the weakest link. The broad adoption of information security guidelines will help practitioners secure and control all their information, continuously adapt their operations and remain the consumer's trusted adviser in an increasingly competitive marketplace.

**For more information on these or any information security topics refer to the Realtor<sup>®</sup> Information Security Guidelines.**