
The Residential Broker's Guide to Protecting Real Estate Information



Version 1.0
November 2004

Contents

1. Executive Summary	3
2. Business Principles	4
3. Information Ownership	5
4. Managing Information Security	6
5. Acceptable Use	7
6. Authenticating Identity	8
7. Disclosing Your Standard of Care	9
8. Labeling Sensitive Information	10
9. Keeping Personal Information Private	10
10. Involving Your Trading Partners	11
11. Securing All Sensitive Information	13
12. Technology	14
13. Responding to an Event	15
14. Education and Training	16
15. A Community Responsibility	16

The Residential Broker's Guide to Protecting Real Estate Information

1. Executive Summary

Trust is based upon the expectation of fair and honest dealings between parties. Consumers trust real estate professionals to play a vital role in managing their largest single purchase and most important financial investment. Consumers also trust brokers with information about their properties, financial qualifications and purchasing intentions. Protecting all forms of company information has become far more 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 a broker's knowledge. Brokers need new management tools and technologies to protect the information they create, exchange and publish.

Brokers need new management tools and technologies to protect the information they create, exchange and publish.

Consumer expectations are changing. Customers are increasingly aware of the importance of protecting their personal information. We all understand that the careless handling of health and financial information can lead to identity theft, fraud and harm to individuals and business operations. Furthermore, new and proposed government regulations impose penalties on organizations that don't secure or improperly use the personal information in their care. Brokers are accountable to consumers, trading partners and, increasingly, regulators for the protection of personal and business information.

All brokers should implement the following essential information security practices to reduce the risks of liability and business disruption from growing internal and external threats.

Broker Essential Information Security Practices	
1	Enter into confidentiality and intellectual property agreements that specify broker ownership of, rights regarding and consideration for all information, pictures and other intellectual property of the brokerage.
2	Apply copyright protections for all information created, integrated, compiled and published by the brokerage.

3	Develop and publish acceptable use guidelines to establish the approved practices for using information, accessing information systems and ensuring compliance with applicable laws and regulations.
4	Define the process for establishing the identity of an individual based on the sensitivity of the information that the person will have access to or the potential risk to employees and contractors.
5	Establish the company's "standard of care" that will be applied to all consumer personal information and trading partner business information.
6	Categorize and label all company sensitive information as either confidential or secret.
7	Develop and implement business continuity plans.
8	Establish a training and education program for staff and third parties that use, administer and maintain sensitive information and systems.
9	Specify company procedures, like encryption, to protect company and consumer information from unauthorized access, alteration, destruction, modification or disclosure of data.
10	Conduct an independent review of information controls periodically to determine compliance with the organization's security policies and practices. This review should be performed by an external organization not responsible for implementing and maintaining information security controls.

These and the additional guidelines included in this document will help brokers to assess their information security readiness, better secure their information, reduce costs and improve the effectiveness of their business operations. Brokers will also be contributing to industry efforts to control the activities of third parties who attempt to acquire broker information for unauthorized commercial purposes.

2. Business Principles

The National Association of Realtors® has defined a set of principles to assist brokers in developing and implementing their information protection policies and practices. These principles should help assure users, partners and third parties that brokers will exercise care in the creation, maintenance and distribution of all forms of company information. The principles are as follows:

Business Principles

Customer Trust	Customer trust is critical to Realtors'® success. Realtors® should inform customers how they will use and protect the information customers provide.
-----------------------	--

Responsible Care	The business and personal information of customers and trading partners should be protected.
Asset Value	Realtors [®] should take active measures to preserve the confidentiality and integrity of valuable information.
Ownership and Rights	Brokers own the information created within their business. They should protect and enforce their rights to intellectual property and ensure authorized access and use.
Standards	The broad adoption of information and transaction standards will improve the service, quality and efficiency for Realtor [®] customers.
Infrastructure	Creating an industry infrastructure to protect information will enable a more efficient market and better protect the privacy of consumers and the rights of Realtors [®] .
Consideration	Brokers should work together to protect the information they create, add value to it and receive consideration when it is used for commercial purposes.

Brokers should become familiar with these principles and educate their employees and independent contractors about the importance of protecting company information. Brokers who are members of the National Association of Realtors[®] have a vital role to play in implementing effective programs to improve information security for all practitioners and their customers.

3. Information Ownership

Third parties may use broker information to encroach on the position of brokers, capture market share and erode broker profitability. The ability of brokers to operate in a secure manner that preserves their rights to information and serves consumer privacy interests is fundamental to retaining brokers' competitive advantage in a rapidly changing market.

The ability of brokers to operate in a secure manner is fundamental to retaining competitive advantage.

Real estate information has commercial value to many inside and outside the real estate industry. Brokers should assert their ownership to the databases, documents, records, files, pictures and other information they create in order to control the information "chain of custody" that extends from the agent to third-party information aggregators such as MLSs, portals and commercial information providers. Brokers should take several actions to assert their ownership to their information.

Ownership Best Practices	Assessment
Enter into confidentiality and intellectual property agreements with third-party contractors that specify broker ownership of all information, pictures and other intellectual property created by agents and others while in the employ of a brokerage.	
Identify the information collected, assembled and arranged by the brokerage. Identify the information where the organization adds creative expression (e.g., remarks and descriptions created by an agent).	
Apply copyright protections for all information created, captured, compiled and published by the brokerage.	

Brokers should establish the information “owner” for all information under a broker’s control. The owner should ensure that ownership has been clearly identified and specify the security classification, access rights and retention policies for broker’s information.

4. Managing Information Security

Responsibility for information security on a daily basis rests with every broker and agent. Brokers should identify a “security manager” to oversee the physical and information security needs of their firms. The security manager should coordinate efforts to prevent loss or compromise of the broker’s business-critical and sensitive information. The responsibilities of the security manager should also include the following best practices:

Security Manager Best Practices	Assessment
Perform information security risk assessments.	
Prepare information security management action plans.	
Develop information security mitigation and remediation plans.	
Communicate incident alerts through appropriate channels.	
Participate in the development of business continuity plans.	
Investigate information security breaches.	
Participate in information security training and awareness programs.	

All consultants, contractors and temporary workers who perform duties for and on behalf of brokers should be subject to the same information security responsibilities as brokerage employees.

Brokers and/or the designated security manager should also create, maintain and periodically reconcile an inventory of information resources including all hardware and software. All microcomputer

equipment should be marked with visible identification that clearly indicates that it is company property.

Specific information security responsibilities should be incorporated into all job descriptions for employees or contractors who have access to critical or sensitive information. Compliance with information security procedures should be incorporated into employee evaluations.

5. Acceptable Use

Information should be treated and managed as a valuable business resource. Brokers provide information and access to information systems to employees, contractors, trading partners, temporary workers and customers. Brokers should develop and publish acceptable use guidelines to establish the approved practices for using information, accessing information systems, ensuring compliance with applicable laws and regulations and educating employees and contractors. At a minimum, brokers should direct users to abide by the following restrictions:

Acceptable Use Best Practices	Assessment
Do not attempt to access any data, documents, e-mail correspondence and programs contained on any systems for which you do not have authorization.	
Do not share your account(s), passwords, personal identification numbers (PINs), security tokens (e.g., Smartcard), or similar information or devices used for identification and authorization purposes.	
Do not make unauthorized copies of copyrighted software or copyrighted documents.	
Do not use nonstandard software without the appropriate management approval.	
Do not engage in activity that may harass, threaten or abuse others or intentionally access, create, store or transmit material that may be deemed offensive, indecent or obscene.	
Do not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of the information systems.	
Do not use information systems for personal benefit, unsolicited advertising, unauthorized fund raising or the solicitation or performance of any activity that is prohibited by any local, state or federal law.	
Do not allow family members or other nonemployees to access the organization's information systems.	

Brokers should specify the incidental or personal uses of information systems that are permitted. These may include electronic mail, Internet access, fax machines, printers, copiers, and the storage of personal e-mail messages, voice messages, files and documents.

Brokers should include language supporting the acceptable use guidelines in applicable agent, contractor, trading partner or other third-party business agreements.

6. Authenticating Identity

The ability of brokers to operate in a secure manner that preserves their rights to information and serves consumer privacy interests is fundamental.

The safety of company employees and the security of company information start by establishing the identity (authentication) of the individuals the company is dealing with. Practitioners understand the importance of making a copy of the personal identification, such as a driver's license, of individuals not known to them before visiting a property. Similarly, in an online interaction it is important to establish the identity of any individual before exchanging digital information.

Brokers should consider screening the background of prospective employees prior to extending an offer of employment or entering into an independent contractor agreement. The level of screening should be commensurate with the value of the broker assets the prospective employee or contractor will have access to.

Establishing identity is also the first step in managing access to information and information systems. Brokers should define the process for establishing the identity of an individual based on the sensitivity of the information that the person will have access to. This process may involve inspecting government documents, establishing a password or PIN based on shared secrets or simply establishing a destination (address or e-mail). Brokers should take extra care in safeguarding information about identity and the credentials that are used to access information and systems.

Employees and contractors should be instructed never to download any files or open any e-mail attachments they are not anticipating. These files may contain a virus or include other forms of malicious software that can damage the company's systems. Consider verifying the phone number or e-mail address of any individual registering at a Web site before exchanging listings or other information.

7. Disclosing Your Standard of Care

Practitioners are involved with many disclosures in their business. Brokers should define and disclose the standard of care they will apply to protecting a consumer's personal information and the business information of trading partners.

Disclosure Best Practices	Assessment
Brokers should not collect or store any information not directly related to a real property transaction unless authorized by the consumer.	
Brokers should inform consumers when their personal information will be used for statistical analysis or marketing purposes beyond their specific transaction.	
Brokers should obtain the permission (opt-in) of consumers prior to initiating e-mail or telephone communications and collecting information from them.	
Brokers should offer consumers access to the information they have collected about them, including a reasonable opportunity to review information and to correct inaccuracies and delete information.	
Brokers should take active measures to protect consumer information from unauthorized access, alteration, destruction or disclosure.	
Brokers should ensure that personal information is protected in transit over the Internet and that physical and technical safeguards are in place to permit only authorized access to personal information.	
Brokers should authenticate individuals to a level of assurance commensurate with the sensitivity of the information.	
Brokers should hold other brokers, MLSs and affiliates accountable for the proper handling of consumer personal information and trading partner business information.	
Brokers should disclose a breach of information security to consumers whose information may have been disclosed to unauthorized persons.	

These disclosures should be published on any Web sites that are under the broker's control and include a link to the Realtor® Code of Ethics. Brokers should identify their state of licensure on all Web sites and promotional materials and make certain that all agent Web sites and promotional materials disclose the agent's brokerage affiliation and state of licensure. Affiliate relationships should also be disclosed on all broker and practitioner Web sites.

8. Labeling Sensitive Information

Some forms of broker information are especially sensitive and should always be labeled as confidential and, in some cases, secret.

Some 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, in some cases, addresses should be handled as confidential. Virtual tours and interior pictures should also be regarded as confidential. Any information concerning access, 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 and identifies purchasing interests or other attributes should also be categorized and labeled as confidential. This information may be very valuable and is 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.

Brokers also maintain sensitive customer, employee and business information such as financial records, market research, prospect lists, employee compensation and tax records, sales results and forecasts, contact information, directories, e-mail addresses and access numbers. This information should be categorized and labeled as confidential or secret. If sensitive information is lost or is suspected of being lost or disclosed to unauthorized parties, the information owner and the manager of the affected organization should be notified immediately.

9. Keeping Personal Information Private

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

Some forms of personal information are subject to specific state, national and international regulation. Name, telephone number, street address and e-mail address information of consumers are routinely

captured by practitioners in the course of their business, and brokers should take care to ensure they are not inadvertently disclosed. In some cases, brokers may also create files that describe financial history, Social Security number and purchasing intention. Brokers should employ technical solutions like encryption to ensure that this personal consumer information in the care of the agent and company remains private.

Brokers should have a legitimate business need when capturing information that describes physical characteristics, racial or ethnic origin, marital status, religious or philosophical beliefs, or health conditions.

Personal information should not be removed from a broker's premises without prior approval from the information owner. Confidential or secret information should not be released during a meeting, seminar or lecture without prior authorization of the information owner.

Sensitive company information should be destroyed or disposed of when it is no longer needed for business purposes. Information owners should assess the continued value and usefulness of information on a periodic basis. Brokers should create a data retention plan with legal counsel to determine the appropriate retention periods for information. Brokers and practitioners should not destroy or dispose of potentially important records or information without specific advance management approval. Unauthorized destruction or disposal of broker records or information should result in disciplinary action.

Brokers should ensure that the information exchanged between business partners is adequately protected.

10. Involving Your Trading Partners

Brokers exchange information with a wide variety of business partners including other brokers, MLSs, appraisers, title companies, and loan origination and settlement services firms. Any sensitive information shared between trading partners should be subject to a confidentiality or nondisclosure agreement (NDA). Brokers should institute information exchange practices that ensure that the information exchanged between all parties to a transaction is adequately protected. These practices include the following:

Information Exchange Best Practices	Assessment
Label any information the licensed broker considers confidential or secret.	
Identify what sensitive information the broker receives from trading partners.	
Understand the standards of care your trading partners will apply to your information.	
Enter into confidentiality agreements drafted by legal counsel with any organization that has access to broker information systems.	
Enter into licensing agreements for confidential or personal information about others, drafted by legal counsel, only after specific authorization from the consumer, other licensed brokers or information owners.	
Ensure that current license agreements exist for all software programs installed on brokerage-owned and -operated systems.	
Inspect the security provisions of Internet service providers (ISPs) and other third parties and contractors.	

The rights of trading partners to use or repurpose broker information should be defined at the time the information is created. The rights associated with many forms of broker 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 brokers ensure that they do not violate the copyright protections for any digital information used in the course of their business.

Brokers should contractually specify the rights associated with their digital information. License agreements should define the rights of the recipient to

render the information by printing in hardcopy, viewing on a dynamic display or playing on an audio/video device;

transport information that is copied, moved or loaned; and

derive new information created through manipulation, repurposing, repackaging, extracting, embedding or editing information.

Brokers should consult with legal counsel whenever entering into information-sharing and license agreements or publishing digital

information that might be subject to unauthorized copying or use.

11. Securing All Sensitive Information

Many forms of real estate 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 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. Business-critical information, such as financial records, should be locked away (ideally in a fire-resistant safe or cabinet) when not required, and especially when the office is vacated.

Brokers are responsible for ensuring that sensitive information under their control is not compromised through unauthorized access, editing or manipulation. Confidential documents and sensitive data can be compromised and tampered with during transmission of the information, during exchange of the information on electronic media or through unauthorized access to the information stored in broker files or systems.

All sensitive computer-resident information should be protected via access controls to ensure that it is not improperly disclosed, modified, deleted or rendered unavailable. Access to sensitive information should be provided only after the written authorization of the information owner has been obtained. 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. Brokers should change the user passwords on their systems at least every 90 days, and the password should be a minimum of eight upper- and lowercase characters. Sharing or publishing a password or authentication token should be subject to disciplinary action.

Improperly installed or configured wireless access points are a major security risk, potentially exposing the entirety of the office's communications and information resources to public view. Wireless access points should never be installed on an ad hoc basis, but integrated with the rest of the information security architecture, and only by personnel with the knowledge necessary to properly configure wireless security options. Agents and employees should be instructed

never to install a wireless access point in the broker’s offices without the authorization and assistance of the broker or office security manager.

Agents and employees should be instructed to treat all communication sent through a public wireless access point (“Wi-Fi hot spot”) as visible to the public unless they are using a virtual private network (VPN).

Any attempt by an unauthorized individual to tamper with or gain access to broker systems or information files should be reported immediately to the broker, MLS or third-party service provider and, in severe cases, law enforcement.

12. Technology

Brokers should work to create and maintain an organizational culture that practices and values security and successfully communicates this to employees, contractors, partners and customers. Every individual who is given access to a broker’s information resources holds a position of trust and should be required to preserve security, protect company resources and report violations of policy. Technology and other active measures can help create, enforce and advance this culture.

Brokers should use mature security technologies that are available to reduce the risks to broker information. Brokers should concentrate their efforts on preventing unauthorized access and use by adopting the following practices:

Technology Best Practices	Assessment
Install firewall software on systems and personal computers.	
Install and update virus-scanning and protection software.	
Install monitoring software to audit sensitive transactions.	
Utilize a secure virtual private network (VPN) whenever possible.	
Encrypt sensitive records and files.	
Embed data markers on key files and listings.	
Establish business continuity and contingency plans.	
Assess overall information security effectiveness.	
Implement remediation programs to enhance information security.	

Post privacy policies and other disclosures after completing education, training and assessment programs.	
---	--

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

An independent review of information system controls should be periodically conducted to determine compliance with the organization's security policies and practices. This review should be performed by an external organization not responsible for implementing and maintaining information security controls.

13. Responding to an Event

The effective implementation of best information security practices can prevent or reduce serious business losses or disruption. Despite a company'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 company'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. Copies of applications that have been custom developed or modified should especially be stored off-site and readily available. Business applications utilizing commercial off-the-shelf software can generally be restored quickly once new computing resources have been identified and backup data files obtained.

Emergency response procedures or a "call tree" should be developed to notify key employees and trading partners should a major event occur. Contact law enforcement in any case where you suspect intentional or malicious damage to business information assets.

14. Education and Training

Technology alone is insufficient to protect an organization and its trading partners if employees don't understand their role in information security. Brokers should establish a training and education program for staff that use, administer and maintain sensitive information and systems. These programs should do the following:

Education Best Practices	Assessment
Advise users of the scope of their access privileges to systems and all specific restrictions that apply to their use.	
Require users to acknowledge they have read and understand the organization's requirements and information security policies.	
Ensure that new users attend an approved training class within 60 days of being granted access to any company system or information resource.	
Update all users on the local, state and national policies that may affect the protection of Realtor® information.	

Brokers should ensure that incident response procedures are included in the training program. Procedures should be published, the staff trained and responsibilities delegated. Whether an incident is minor or major, it should be reported to the security manager for appropriate handling.

15. A Community Responsibility

The Internet created a major shift in the way brokers collect and publish listing information to consumers. The next major shift will involve how all forms of company information are protected and controlled. The need for Realtors® to preserve consumer privacy, protect business-critical 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 brokers continue to work to improve the information security procedures and technology protections of their company operations.

Though industry business models, participants, regulation, threats and technology will continue to change, information security will remain 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 more efficient transactions. Greater convenience and service quality must also include preservation of consumer privacy and control of real estate information.

Brokers have a vital role to play in the evolution of the industry's information security policies, 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 brokers 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[®] Information Security Guidelines.