
The Commercial Broker's Guide to Protecting Real Estate Information



Version 1.0

November 2004

Contents

1. Executive Summary	3
2. Protecting Broker Information	5
3. Business Principles	6
4. Information Ownership	7
5. Managing Information Security	8
6. Acceptable Use	9
7. Authenticating Identity	10
8. Disclosing the “Standard of Care”	11
9. Labeling Sensitive Information	12
10. Keeping Personal Information Private	12
11. Involving Trading Partners	13
12. Securing All Sensitive Information	15
13. Technology	16
14. Responding to an Event	17
15. Education and Training	18
16. Community Responsibility	19

The Commercial Broker's Guide to Protecting Real Estate Information

1. Executive Summary

Protecting and controlling commercial real estate information has become critical to the business success of commercial practitioners and the operations of commercial brokerages. To respond to several changing market forces, commercial practitioners should embrace best practices for information security:

Protecting and controlling commercial real estate information has become critical to the business success of agents and brokers

Customer Trust	Consumers have a number of choices to assist them with their real estate needs. Brokers need to improve their information security practices to enhance their traditional position as the first point of consumer contact and the facilitator of the real estate transaction.
Privacy	Identity theft, fraud, unwanted solicitations, malicious viruses, and other highly publicized threats have increased consumer awareness of the need to better protect the privacy of their personal information. Agents and brokers need to improve their information security practices to meet and exceed their business and investment clients' expectations that their sensitive information will be protected.
Regulation	Practitioners are subject to many new information security regulations. They need to improve their information security practices to comply with international, federal, and state privacy and security regulation.
Liability	The widespread sharing of information and the accumulation of sensitive client and transaction information put practitioners at risk. Practitioners need to improve their information security practices to mitigate the liability resulting from any compromise of client and business partner information.
Piracy	Agent- and broker-controlled information, such as client lists, property listings, qualifications, and contract terms, is of tremendous monetary value and may be subject to unauthorized access and uses. Practitioners need to improve information security practices to create a chain of custody that can control the way their information is used.
Rights	Practitioners assume liability, add creative expression, and frequently compile listing and other forms of information. Practitioners should assert their

	ownership through copyright and technology protections of their intellectual property.
Efficiency	The workflow of a commercial real estate transaction is complex and involves many participants. Organizations are pursuing initiatives with the ultimate goal of reducing the costs, complexity, and risks associated with the transaction process. Practitioners need to develop, integrate, and manage new standards for the secure exchange of commercial real estate information.
Costs	The real estate industry can improve information security through the use of new technologies. Commercial practitioners should use proven nonproprietary technologies to lower the cost of implementing information security.

Commercial brokers should implement the following essential information security support programs and practices to help practitioners reduce the growing risks of liability and business disruption from growing internal and external threats.

Commercial Brokers Essential Information Security Practices	
1	Enter into confidentiality and intellectual property agreements that specify broker ownership, rights, and consideration for the intellectual property of the brokerage.
2	Apply copyright protections for all information collected, 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 on the basis of the sensitivity of the information that the person will have access to or potential business risk to clients, employees, and contractors.
5	Establish the company's "Standard of Care" to be applied to all client personal, business 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

	members who use, administer, and maintain sensitive information and systems.
9	Establish company procedures, such as encryption, to protect company and client information from unauthorized access, alteration, destruction, 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 commercial brokers assess their information security readiness, better secure sensitive information, reduce costs, and improve the effectiveness of their business operations. Commercial brokerages will also be contributing to industry efforts to control the activities of third parties who attempt to acquire information for unauthorized commercial purposes.

2. Protecting Broker Information

Trust is based on the expectation of fair and honest dealings between parties. Businesses and investors trust the Realtor® to play a vital role in managing their interests when engaged in complicated commercial transactions. Clients and corporations also trust commercial practitioners with sensitive information about their business and financial strategies that shape their acquisition and leasing intentions. Protecting all forms of commercial broker–controlled 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. Commercial brokers need new management tools, technologies, and business processes to protect the content they create, publish, and increasingly exchange through commercial information exchanges (CIEs).

Commercial Brokers need new management tools, technologies, and business processes to protect the content they create, publish, and exchange electronically through CIEs.

Client and corporate expectations concerning the protection of their sensitive business information are high and rapidly escalating. Clients have relied on Realtors® to protect transactional information that includes sensitive proprietary information about their business and strategic intentions. Many corporate clients and transaction partners have made significant investments in strong information security

practices and technologies. They expect their confidential information to be handled by agents and brokers with the same care they exercise themselves. Business partners understand that the careless handling of business information can harm individuals and corporate operations. Furthermore, new and proposed government regulations impose penalties on organizations that don't secure or that improperly use the personal information in their care. Commercial practitioners are accountable to clients, business partners and, increasingly, regulators for the protection of personal and business information.

These guidelines will help commercial brokers reduce the growing risks of liability and business disruption from increasing internal and external threats. Commercial brokers will be better able to assess their information security readiness, 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 content for unauthorized purposes.

3. Business Principles

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

Business Principles

Customer Trust	Customer trust is critical to Realtors [®] success. A Realtor [®] should inform customers how the information they provide will be used and protected.
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.
	The broad adoption of information and transaction

Standards	standards will improve the service, quality, and efficiency for Realtors [®] customers.
Infrastructure	Creating an industry infrastructure to protect information will enable a more efficient market and better protect the privacy of customers and the rights of Realtors [®] .
Consideration	Brokers should work together to protect the information they create, to add value to it, and to receive consideration when it is used for commercial purposes.

Commercial brokers should become familiar with these principles and educate their employees and contractors on the importance of protecting the information they create. Brokers who are members of NAR have a vital role to play in implementing effective programs to improve information security for all Realtors[®] and their clients.

4. Information Ownership

Third parties may use Realtor[®]-controlled information to encroach on the position of commercial agents and brokers, capture market share, and erode broker profitability. The ability of brokers to operate in a secure manner, preserving their rights to information and serving client privacy interests, is fundamental to retaining their competitive advantage in a rapidly changing market.

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

Real estate content has monetary value to many inside and outside the real estate industry. Brokers should assert their ownership of the information they create, and control the content “chain of custody” that extends from the agent to third-party information aggregators, such as CIEs and commercial information providers. Brokers should take several actions to assert ownership of 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 CIE or MLS. Identify the information to which the	

organization adds creative expression, analysis, and interpretative comments (e.g., remarks and descriptions created by an agent).	
Consider copyright protections for all information created, captured, compiled, and published by the brokerage.	

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

5. Managing Information Security

Responsibility for information security on a daily basis rests with every Realtor[®]. 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. Depending on the size of the brokerage, 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.

Commercial brokers, the designated security manager, or both 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.

6. Acceptable Use

Information should be treated and managed as a valuable business resource. Brokers provide information and access to information systems to employees, contractors, business 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 adhere to the following acceptable use best practices:

Acceptable Use Best Practices	Assessment
Do not attempt to access any data, documents, e-mail correspondence, or programs contained on any systems for which authorization is not granted.	
Do not share account(s), passwords, personal identification numbers (PIN), security tokens (i.e., Smartcards), 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 to be 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 as well as the storage of personal e-mail messages, voice messages, files, and documents.

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

7. Authenticating Identity

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

Ensuring the security of company information starts with establishing the identity (authentication) of the individuals and businesses the company is dealing with. Commercial practitioners understand the importance of vetting the entities they interact with by reviewing corporate information that establishes the entities' legitimacy before the transaction process begins. Similarly, in an online interaction it is important to establish the identity of any individual or organization before exchanging digital information.

Commercial brokers should consider screening the background of a prospective employee before 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 to which the prospective employee or contractor will have access.

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 to which that person will have access. This process may involve inspection of government documents and establishing a password or PIN or simply a destination (address or e-mail). Commercial brokers should take extra care in safeguarding information about identity and the credentials that are used to access information and systems.

Commercial practitioners, other employees, and contractors should be instructed to avoid downloading any files or opening any e-mail attachments they are not expecting. 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 listings or other information is exchanged.

8. Disclosing the “Standard of Care”

Commercial agents and brokers are involved with many disclosures in their business. Brokers and agents should disclose the standard of care they will apply to protecting a client’s sensitive information.

Disclosure Best Practices	Assessment
Brokers should not collect or store any information that is not directly related to a real property transaction unless authorized by the client.	
Brokers should inform clients when their personal or company information may be used for statistical analysis or marketing purposes beyond their specific transaction.	
Brokers should obtain permission (opt-in) before initiating e-mail or telephone communications and collecting information from a prospect.	
Brokers should offer clients 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 client information from unauthorized access, alteration, destruction, or disclosure.	
Brokers should ensure that personal or company information is protected in transit over the Internet and that physical and technical safeguards are in place to permit only authorized access to personal and company information.	
Brokers should authenticate individuals and companies to a level of assurance commensurate with the sensitivity of the information.	
Brokers should hold other brokers, CIEs, MLSs, and affiliates accountable for the proper handling of client and commercial broker personal and business information.	
Brokers should disclose a breach of information security to clients whose information may have been disclosed to unauthorized persons.	

These disclosures should be published on the broker’s Web sites and should include a link to the Realtor® Code of Ethics. Commercial

brokers should identify their state of licensure on all Web sites and promotional materials and make certain that all agent Web sites and promotional material disclose the agent's brokerage affiliation and state of licensure. Affiliate relationships with business partners should also be disclosed by the broker and agents.

9. Labeling Sensitive Information

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

Some forms of commercial broker 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, financial terms, client contact information and, in some cases, addresses should be handled as confidential. Property pictures should also be regarded as confidential. Passwords to information systems and any information concerning access, such as pass codes or building security codes, should always be labeled and handled as secret.

Customer information that identifies a buyer or seller and specifies purchasing interests or other attributes should also be categorized and labeled as confidential. This information may be very valuable to marketers and is subject to theft. Social Security numbers, financial qualifications, credit information, business and financing strategies, and data related to a client transaction should always be regarded as secret and subject to the highest level of protection.

Commercial brokers also maintain 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.

10. Keeping Personal Information Private

The National Association of Realtors[®] Code of Ethics states that "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. Clients' names, telephone numbers, addresses, and e-mail addresses are routinely captured by commercial practitioners in the course of their business; brokers should take care to ensure that this information is 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 such as encryption to ensure that this personal client or business information in the agent's and company's care 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 broker 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 periodically. Brokers should create a data retention plan with legal counsel to determine the appropriate retention periods for information. Commercial 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.

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

11. Involving Trading Partners

Commercial brokers exchange information with a wide variety of business partners, including other brokers, CIEs, appraisers, and attorneys. Any sensitive information shared between business 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 business partners.	
Understand the standards of care business partners will apply to the broker's information.	
Disclose the standard of care to business partners.	
Enter into confidentiality agreements drafted by legal counsel with any organization that has access to broker information systems.	
Enter into licensing agreements for sensitive or confidential information about others, drafted by legal counsel, only after specific authorization from the client, 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 services 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 commercial brokers ensure that they do not violate the copyright protections for any digital information used in the course of their business.

Commercial 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 hard copy, viewing on a dynamic display, or playing on an audio or video device.

transport information that is, copied, moved, or loaned.

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

Commercial 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.

12. Securing All Sensitive Information

Many forms of commercial information continue to exist on paper that must be physically secured. Access to prospect and client lists, research, client requirements, 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.

Commercial brokers are responsible for ensuring that sensitive information under their control is not compromised through unauthorized access or manipulation. Confidential documents and sensitive data can be compromised and tampered with when information is being transmitted, when information on electronic media is exchanged, or when information stored in broker's files or systems is accessed without authorization.

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

13. Technology

Commercial brokers should work to create and maintain an organizational culture that practices and values security and successfully communicates that attitude to employees, contractors, partners, and clients. 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 adhering to the following technology best practices:

Technology Best Practices	Assessment
Install firewall software on systems and personal computers.	
Install and updating virus scanning and protection software.	
Install monitoring software to audit sensitive transactions.	
Use a secure virtual private network (VPN)	

whenever possible.	
Encrypting sensitive records and files.	
Embedding data markers on key files and listings.	
Establishing business continuity and contingency plans.	
Assessing overall information security effectiveness.	
Implementing remediation programs to enhance information security.	
Posting 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 services providers to meet these needs. Through the Realtor[®] Secure Program, data systems can be tested for vulnerabilities. These are just some of the services available to help commercial brokers and other commercial Realtor[®] organizations reduce liability and sustain a high level of client 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.

14. 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 the place of business.

Copies of applications that have been custom developed or modified should, in particular, be stored off-site and readily available. Generally, business applications using commercial off-the-shelf software can 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 business partners should a major event occur. Contact law enforcement in any case in which intentional or malicious damage to business information assets is suspected.

15. Education and Training

Technology alone is insufficient to protect an organization and its business partners if employees don’t understand their role in information security. Commercial brokers should establish a training and education program for staff members who use, administer, and maintain sensitive information and systems. These programs should include the following best practices:

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 that 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 commercial broker's system or information resource.	
Update all users on the local, state, and national policies that may affect the protection of commercial broker's information.	

Commercial 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.

16. Community Responsibility

The Internet created a major shift in the way commercial practitioners are able to collect, publish, and exchange information with clients. The next major shift will involve the way all forms of commercial broker information are protected and maintained. The need for practitioners to preserve client confidentiality and protect business critical information will continue to grow. Supporting industry efforts to remain as the “trusted” point of client contact requires that commercial 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 commercial transaction process. Sensitive information will be shared electronically between an ever-growing set of devices and organizations. Commercial brokers will invest in technologies that provide more efficient transactions. Improved service quality must also include preservation of client confidentiality and information integrity as well as control of company information.

Brokers have a vital role to play in the evolution of the industry’s information security policies, practices, and protection infrastructure. Commercial brokers increasingly operate in an interconnected industry in which the security of all systems 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 clients’ trusted advisers in an increasingly competitive and complex marketplace.

For more information on these or any information security topic refer to the Realtor® Information Security Guidelines.